INFORMATICA GIURIDICA
collana del CIRSFID

8

Direttori

Monica Palmirani
Alma Mater Studiorum – Università di Bologna

Giovanni Sartor
Alma Mater Studiorum – Università di Bologna

Comitato scientifico

Agata Cecilia Amato Mangiameli
Università degli Studi di Roma "Tor Vergata"

Alberto Artosi
Alma Mater Studiorum – Università di Bologna

Luisa Avitabile
"Sapienza" Università di Roma

Raffaella Brighi
Alma Mater Studiorum – Università di Bologna

Donato Limone
Università Telematica Unitelma Sapienza

Ugo Pagallo
Università degli Studi di Torino

Francesco Romeo
Università degli Studi di Napoli "Federico II"

Antonino Rotolo
Alma Mater Studiorum – Università di Bologna

Giovanni Ziccardi
Università degli Studi di Milano

INFORMATICA GIURIDICA
collana del CIRSFID

La collana ha l'obiettivo di accogliere scritti scientifici che affrontino temi di informatica giuridica con originalità, innovazione, interdisciplinarietà. Ospiterà lavori dedicati ai diversi aspetti del rapporto tra discipline informatiche e diritto, spaziando dalle tecnologie informatiche per il diritto, alla logica giuridica e al diritto dell'informatica. I lavori possono comprendere riflessioni — di teoria del diritto e dell'argomentazione, bioetica, sociologia e filosofia del diritto — sugli impatti delle tecnologie dell'informazione sul sistema giuridico e sull'attività del giurista.

CIRSFID
Alma Mater Studiorum – Università di Bologna

NUOVE QUESTIONI DI INFORMATICA FORENSE

a cura di

RAFFAELLA BRIGHI

Prefazione di

CESARE MAIOLI

Contributi di

LAURA BARTOLI, ULRICO BARDARI, SEBASTIANO BATTIATO, MARIA ANGELA BIASIOTTI, RAFFAELLA BRIGHI, ALFONSO BUCCINI, DONATO E. CACCAVELLA, ILARIA CAPRILLI, PIER GIORGIO CHIARA, VINCENZO COLAROCCO, SARA CONTI, GIUSEPPE CONTISSA, FEDERICO COSTANTINI, GIOVANNA DE RUGERIIS, MARCO ALVISE DE STEFANI, ROSA DOMINA, CORRADO FEDERICI, MICHELE FERRAZZANO, FEDERICO GALLI, FAUSTO GALVAN, ANTONIO GAMMAROTA, OLIVER GIUDICE, FRANCESCO GODANO, SILVIA GOLIN, LUCA GUARNERA, GIULIA LASAGNI, SILVIA MOFFA, ISADORA NERONI REZENDE, ANDREA PASELLI, ANTONIO PUGLIESE, PASQUALE SAMMARIO, GALILEO SARTOR, SILVIA SIGNORATO, LEONARDO SUMMA

aracne

aracne

©

ISBN
979–12–5994–643–0

PRIMA EDIZIONE
ROMA 5 GENNAIO 2022

Indice

11 Prefazione
Cesare Maioli

17 Sfide recenti e nuovi paradigmi dell'Informatica forense
Raffaella Brighi

Parte I
Sistematica evolutiva delle nuove tecnologie forensi. Riflessioni metodologiche e giuridiche

43 Questioni aperte sull'acquisizione probatoria di dati informatici
Silvia Golin

61 La selezione di dati informatici in ambito giudiziario: prassi e modalità operative
Michele Ferrazzano, Leonardo Summa

83 Parità delle armi e *e-discovery* nel processo penale: quali indicazioni da Strasburgo*?*
Laura Bartoli

101 *Data retention*, tra diritto alla protezione dei dati personali ed esigenze di accertamento dei reati
Silvia Signorato

115 Sull'analisi forense dei tabulati di traffico: aspetti giuridici, metodologici e tecnici
Ilaria Caprilli, Raffaella Brighi

137 Il captatore che non c'è: ovvero perché il captatore potrebbe non entrare più nelle aule di un tribunale
Alfonso Buccini, Donato E. Caccavella

Parte II
IoT, *Crypto* e Social Media: nuove sfide per la *forensics*

159 La "Qualità dell'Informazione" nella IoT Forensics: dal modello IQA all'ontologia forense
F. Galvan, F.Costantini, M. A. De Stefani, S. Battiato

187 *Cyberlaundering* e *Blockchain Forensics*: aspetti giuridici e tecnici del riciclaggio di criptovalute
Pasquale Sammario, Raffaella Brighi

207 DarkNet, DarkMarkets e criptovalute: attività investigativa di contrasto
Andrea Paselli

227 Dal *Phishing* allo *SMiShing*. Strumenti di prevenzione e repressione delle frodi informatiche
Ulrico Bardari

245 Indagini digitali forensi sui Social Network. Nuovi orizzonti investigativi
Antonio Pugliese

261 Tecniche di digital forensics nelle pratiche di concorrenza sleale su piattaforme di *advertising online*: il caso di *Google AdWords*
Vincenzo Colarocco, Michele Ferrazzano

281 Un modello per la gestione del trattamento dei dati prodotti e raccolti dall'Internet of Things (IoT) nell'e-Health
Rosa Domina

Parte III
Prospettive della *Artificial Intelligence Forensics*

303 *Policing* via *Multi-Agent Systems*: un nuovo volto per la digital forensics (e non solo)?
Giulia Lasagni

323 *Deep Learning* per l'analisi del *sentiment*
Corrado Federici

343 L'IA applicata all'analisi dei metadati: un'alternativa alla rottura della crittografia per le autorità di contrasto alla criminalità
Isadora Neroni Rezende, Pier Giorgio Chiara

363 Fenomenologia dei *DeepFake*: aspetti teorici e operativi per la detection di volti umani "artificiali"
L. Guarnera, O. Giudice, S. Battiato

387 La nuova Proposta di Regolamento europeo sull'intelligenza artificiale: questioni giuridiche e approcci regolatori
G. Contissa, F. Galli, F. Godano, G. Sartor

Parte IV
Modelli ibridi di cooperazione giudiziaria

413 Aspetti di Informatica forense nel Regolamento della Procura europea
Antonio Gammarota

431 La gestione delle prove digitali in ambito europeo: un necessario connubio tra la tecnologia e la legge
Maria Angela Biasiotti, Sara Conti

449 Sulla Procura Europea. Profili di Informatica giudiziaria
Silvia Moffa

469 Il Processo Penale Telematico tra emergenza COVID e riforme
Giovanna De Rugeriis

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464301
pp. 11-16 (gennaio 2022)

Prefazione

CESARE MAIOLI

L'Informatica forense (internazionalmente nota come *Digital forensics*) ha assunto negli ultimi lustri una propria maturità e completezza tale da poterle riconoscere autonomia scientifica nel più ampio ambito dell'Informatica giuridica[1].

Il riconoscimento teorico e pratico deriva non solo dallo studio e attività che a livello internazionale le vengono dedicate, ma anche, per quanto riguarda l'Europa e l'Italia, dalla formazione di un ampio *corpus* normativo omogeneo che, per quanto connesso al diritto processuale penale da un lato e all'informatica dall'altro, ne travalica i limiti essendo i suoi principi caratterizzati da peculiarità di oggetto, finalità e metodo che la differenziano dalle sue componenti e la rendono indispensabile e trasversale a tutte le altre branche dell'ordinamento giuridico.

A ciò si aggiunga la formalizzazione del suo insegnamento in corsi di studi universitari stabilmente strutturati e ampiamente diffusi in tutto il mondo, che trovano riscontro a livello europeo e, da alcuni anni, anche in Italia. Ricordo le prime versioni nel 2003 del Corso di Informatica Forense – tenute con Antonio Gammarota – al Corso di Laurea triennale in Operatore Informatico Giuridico dell'Università di Bologna allora coordinato da Monica Palmirani che assieme a Giovanni Sartor dirige ora la collana che ospita questo libro. Il Corso è successivamente proseguito nel Corso di Laurea Magistrale a ciclo unico in Giurisprudenza – dal 2017 con titolarità a Raffaella Brighi – senza soluzione di continuità anche con parti seminariali dedicate ad avvocati e cultori della materia.

Lo scopo e l'oggetto di studio dell'Informatica forense sono oggi ben delineati sulla base sia di una propria metodologia interdisciplinare fondata su quella delle scienze afferenti (diritto processuale penale e

[1] C. MAIOLI, C. ORTOLANI, *La cyber law non è la horse law. L'informatica giuridica nelle Facoltà di Giurisprudenza*, Gedit, 2007, pp. 185-186.

informatica), sia di un *corpus* normativo ampio e articolato, sia di un vasto riconoscimento dottrinale che si traduce in una letteratura ricca e con posizioni strutturate, spesso divergenti, oltre a una importante letteratura tecnica. Pertanto, l'Informatica forense ha acquisito autonomia scientifica al pari delle altre scienze forensi di più antica tradizione quali ad esempio la medicina legale, la chimica forense e la balistica forense.

Dato che in Italia, come in altri Paesi, le prime esperienze teoriche e applicative dei principi e delle tecniche della *Digital forensics* si sono sviluppate in ambito penalistico, l'Informatica forense appare naturalmente inquadrabile tra le scienze ausiliare all'applicazione del diritto penale e processuale penale, secondo la tradizione classificatoria dei più importanti Autori di tali discipline[2].

Tuttavia, sin dalle prime esperienze teoriche, si è posta la questione di delimitare l'area di studio e l'operatività dell'Informatica forense rispetto alle altre discipline dell'area tecnico-giuridica come la Giuscibernetica[3], l'Informatica giuridica[4] (insegnamento obbligatorio nel Corso di laurea quinquennale a Giurisprudenza dell'Università di Bologna fin dal 2007 su sollecitazione e per merito di Enrico Pattaro[5]), il Diritto dell'informatica[6], l'Informatica documentaria.

La trasversalità delle problematiche studiate dall'Informatica forense rispetto a molti altri ambiti diversi dal diritto penale e processuale penale, è resa attuale dalla pervasività dei cambiamenti tecnologici e sociali e dalle recenti riforme legislative verificatesi in vari settori del diritto processuale che hanno toccato gli ambiti del processo tributario, amministrativo e civile.

Per questo motivo, le riflessioni e le tecniche maturate nell'ambito dell'Informatica forense si prestano, previ opportuni adattamenti, a poter essere mutuate in altri settori della scienza giuridica stante proprio il carattere trasversale dei presupposti comuni a qualsiasi ambito nel quale si renda necessario trattare dati digitalizzati a fini processuali.

[2] *Ex multis:* F. ANTOLISEI, *Manuale di diritto penale, Parte generale*, Giuffrè, 1987, p. 26.; F. MANTOVANI, *Diritto Penale, Parte generale*, Cedam, 1992, p. 10.

[3] M. LOSANO, *Informatica per le scienze sociali*, Einaudi, 1985, pp. 45-53.

[4] G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli, 2012, p. 11 e ss.

[5] E. PATTARO, (a cura di), *Manuale di diritto dell'informatica e delle nuove tecnologie*, Cedam, 2000.

[6] E. GIANNANTONIO, *Manuale di diritto dell'informatica*, II ed., Cedam, 1997; V. FROSINI, *Informatica diritto e società*, Giuffrè, 1992, p. 229 e ss.

Secondo i principi sistematizzati dalla materia, i dati digitali sono di per sé neutri e per mantenere integre le informazioni che se ne possono trarre, devono essere trattati secondo le modalità introdotte dalla L. 48/2008, con le tecniche scientifiche che ne rispettano le caratteristiche fisiche a vantaggio di tutte le parti del processo e nel quadro di procedure che riconoscano alle stesse il diritto a partecipare sin dal primo momento alle operazioni tecniche che li riguardano. Solo l'adozione delle opportune metodologie tecnico-scientifiche, nel quadro di procedure che impediscano la strumentalizzazione degli accertamenti per fini di parte, assicura infatti il maggior grado possibile di oggettività e certezza dei dati, nonché garantisce a tutte le parti coinvolte nel procedimento – giudice incluso – lo svolgimento delle rispettive attività.

Al contrario, i dati assunti al di fuori di tali criteri, sotto il profilo giuridico prestano il fianco al rischio di inutilizzabilità o invalidità mentre sotto il profilo del merito legittimano informazioni erronee o inattendibili, in ogni caso inidonee a costituire la base di sentenze capaci di superare il limite minimo "al di là di ogni ragionevole dubbio".

Nonostante tali assunti, la disamina della giurisprudenza di merito e di legittimità ha dimostrato la progressiva riduzione della portata delle innovazioni della L. 48/2008 e quindi la difficoltà che emergano orientamenti che inquadrino correttamente i fatti digitali nella cornice delle norme giuridiche e tecniche che sovrintendono alle operazioni di trattamento dei dati digitali a fini probatori. Ove tale tendenza dovesse consolidarsi, si assisterebbe a un anacronistico immobilismo dello sforzo riformatore e interpretativo teso ad assicurare che i dati digitali siano trattati in modo tale da garantire a tutte le parti del processo il corretto esercizio delle proprie prerogative processuali, alla luce delle norme costituzionali in punto di Giusto Processo.

Sul piano dei correttivi, l'ideale sarebbe quello di evitare l'interpolazione del modello pre-informatico riproducendo quindi in formato digitale le dinamiche analogiche, con il risultato di amplificare le incertezze e, per molti aspetti, le inefficienze del sistema preesistente. Al contrario, la descrizione dei procedimenti (i sistemi informativi) che danno forma alle sequenze processuali dovrebbero esser riformulati *ex novo* secondo logiche digitali native.

Tuttavia, con gradualità, sul piano dei correttivi praticabili, la tendenza in atto potrebbe essere rettificata intraprendendo decise iniziative

di aggiornamento normativo come[7]: il riconoscimento al dato informatico della dignità e tutela di autonomo bene giuridico; l'aggiornamento delle norme in punto di Giusto Processo, riconoscendo la necessità di adeguare modi, tempi e condizioni per la preparazione della difesa alle peculiarità imposte dalle innovazioni tecnologiche; la rivisitazione del sistema processuale per valorizzare il ruolo, ormai preponderante, della tecnologia digitale e della prova documentale informatica; la caratterizzazione del *thema probandum* a oggetto informatico come soggetto alla formazione in contraddittorio sin dal momento dell'acquisizione dei dati; il riconoscimento della centralità del metodo scientifico e tecnico che garantisce il corretto trattamento dei dati e della prova documentale informatica, secondo gli standard internazionali; l'adozione della sanzione di inutilizzabilità o della nullità alle prove acquisite in violazione delle norme introdotte dalla L. 48/2008.

Le tendenze significative nell'ultimo decennio sono state[8]: (1) l'armonizzazione degli standard tecnici e giuridici, (2) l'istituzione di centri specializzati per la gestione dei reperti digitali, (3) l'approfondimento della cornice epistemologica di riferimento per le scienze forensi. Per i punti (1) e (2) vanno segnalate le numerose iniziative ISO per la standardizzazione delle modalità di indagine e mantenimento degli elementi di prova digitali e il recente Regolamento (EU) 2019/881 (*Cybersecurity Act*) che, potenziando i compiti dell'ENISA, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, confermano la centralità della qualità dell'informazione e della sicurezza come prerequisito indefettibile del corretto utilizzo delle tecnologie informatiche e telematiche[9]. Tuttavia, l'Informatica forense stenta ancora a raggiungere, oggi, una maggiore centralità nelle aule di giustizia e recenti sentenze confermano come la rilevanza degli standard sia an-

[7] A. Gammarota, *Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali*, su ams.dottorato.unibo.it, 2016, p. 206.

[8] R. Brighi, C. Maioli, *Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologica*, Informatica e Diritto, Informatica e Diritto, Vol. XXIV, 2016, n. 1-2, pp. 217-234.

[9] Si rimarca come ENISA si rivolga ai Paesi membri per elevare i livelli di sicurezza, abbia una base per lo più tecnica, e attivi processi tecnici a monte delle violazioni che possono perfino assumere dimensioni belliche e quindi non affrontabili giudiziariamente; mentre l'Informatica forense è indirizzata agli operatori forensi, ha base tecnico-giuridica e si colloca a valle delle violazioni.

cora negletta o quantomeno ignorata dalla maggior parte della giurisprudenza di merito e di legittimità.

Per il punto (3) al giudice non si può più chiedere di improvvisarsi "tecnico" – secondo il mito del *judex peritus peritorum* –, ma si dovrebbe pretendere lo svolgimento del ruolo di *gatekeeper*, ossia di valutare a quali condizioni una tecnica investigativa possa essere ritenuta dotata di validità scientifica, e di informarsi sui presupposti di validità del metodo o prova scientifici utilizzati nel processo e dunque, su queste basi, di formulare la propria decisione autonoma. Il principio fondamentale – sviluppato e consolidato a partire da Daubert[10] – che le prove fornite dall'esperto non siano vincolanti per il giudice e che, per quanto esse siano complesse, il giudice abbia l'onere di interpretarne e rielaborarne i contenuti informativi in modo autonomo, è ormai da tempo alla base di tutti gli ordinamenti processuali. In particolare, nel contesto europeo, soprattutto in ambito penale, importanti basi normative per la disciplina della prova scientifica nei distinti momenti della ammissione, dell'assunzione e dell'utilizzazione dell'elemento di prova contribuiscono a definire il ruolo della scienza nel processo; inoltre, diverse sentenze fissano criteri per la validazione del sapere scientifico non consolidato.

L'interpretazione giuridica, l'arte dell'interpretazione, quasi sempre ammette una pluralità di risultati alternativi plausibili, razionalmente fondati, tra i quali è necessario individuarne uno esplicitando le ragioni di questa scelta; il giudice, quindi, mantiene il controllo del sistema informativo. Giovanni Canzio recentemente ha scritto[11] «D'altra parte, è cresciuta nella società la legittima pretesa che il giudice, nell'esercizio dell'arte del giudicare e nella pratica giudiziaria, sia un buon ragionatore e un decisore di qualità. Sicché la professionalità, l'etica e l'implementazione del grado di *expertise* accumulata dal giudice nell'utilizzo delle tecniche inferenziali del ragionamento e nella verifica degli schemi statistico-probabilistici, acquisiti con l'ausilio della tecnologia digitale, di software informatici» e dei più recenti prodotti dell'informatica «potrebbero certamente contribuire a restituire al funzionamento della giustizia penale una più adeguata immagine di efficacia e qualità».

[10] Nel 1993, la Corte Suprema degli Stati Uniti ridefinì il ruolo del giudice nell'ammissione e valutazione della prova scientifica nel famoso caso Daubert vs. Merrel Dow Pharmaceutical relativo a malformazione di feti connesse all'utilizzo di alcuni farmaci.

[11] G. Canzio, Sistema Penale, 2021.

Le innovazioni dell'informatica e dei sistemi informativi si riflettono sul piano giuridico e il processo penale è un importante specchio della società e dei tempi. Allo stato, le questioni affrontate riguardano ancora poche norme tra quelle che compongono l'edificio processuale. Tuttavia, a fianco dei molti dubbi riguardanti l'esito di tali innovazioni, permane la visione sul futuro del sistema processuale penale nel quale la dimensione digitale sarà forma e contenuto dell'intero procedimento, cosicché gli istituti estranei alla digitalizzazione e alle regole dell'Informatica forense diverranno residuali.

In questa prospettiva ho curato nel 2015 il volume *Questioni di Informatica Forense* e sei anni più tardi ho visto nascere il presente *Nuove Questioni di Informatica Forense* che Raffaella Brighi ha curato con perizia, competenza e signorilità.

A ciascuna delle Autrici e degli Autori dei contributi va il mio sincero e profondo apprezzamento per il loro lavoro.

Dicembre 2021

Cesare Maioli
Alma Mater Studiorum – Università di Bologna

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464302
pp. 17-39 (gennaio 2022)

Sfide recenti e nuovi paradigmi dell'Informatica forense

RAFFAELLA BRIGHI

1. Introduzione

A partire dalla prima definizione di cui si ha traccia nella letteratura italiana[1] che qualificava l'Informatica forense (IF) come «la disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova»[2], i confini della materia si sono prepotentemente dilatati, spinti dalla sempre crescente dipendenza della società moderna dalle tecnologie informatiche. Le attività commerciali, le transazioni d'affari e i servizi governativi traggono indubbi benefici dalle sempre nuove funzionalità delle ICT, quali reti di comunicazione, dispositivi mobili, soluzioni *Internet of Things* (IoT) e servizi basati sul *Cloud*; e con essi

[1] La definizione che si attribuisce a Cesare Maioli è precedente al 2004. C. MAIOLI, *Dar voce alle prove: elementi di informatica forense,* in P. Pozzi (a cura di) *Crimine virtuale, minaccia reale*, Franco Angeli, 2004.

[2] Per una introduzione di ruolo, principi e metodi della informatica forense si veda G. Ziccardi, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. Lupária (a cura di), *Sistema penale e criminalità informatica,* Giuffrè, Milano, 2009; P. Perri, voce *Computer forensics (indagini informatiche)*, in Digesto delle discipline penalistiche, Utet, Torino, 2011; G. FAGIOLI, A. GHIRARDINI, *Digital forensics,* Apogeo, 2020 e S. ATERNO, F. CAJANI, G. COSTABILE, D. CURTOTTI (a cura di), *Cyber Forensics e indagini digital*i, Giappichelli, 2021. Inoltre, E. CASEY *Foundations of digital forensics*, in ID. (ed.) *Digital evidence and computer crime*, 3rd ed. Academic, Waltham, 2011; L. DANIEL, *Digital forensics for legal professionals. Understanding digital evidence from the warrant to the courtroom*, Syngress, Amsterdam, 2012; J. HENSELER, *Computer crime and computer forensics*, in The Encyclopaedia of Forensic Science, Academic, London, 2000; S. MASON, *Electronic evidence*, 3rd ed., Lexis Nexis Butterworths, London, 2012. Si v. anche M. POLLIT, *A History of Digital Forensics*, in K.P. Chow-S. Shenoi (eds.), *Advances in Digital Forensics* VI, Boston, Springer, 2010, pp. 3-15.

anche i comportamenti e le abitudini degli individui. Ciò ha creato sfide e prospettive inedite per le attività di indagine.

Qualsiasi evento, fenomeno o cosa – film, libri, messaggi vocali, spostamenti, finanche relazioni e sentimenti – transita convertito in formato digitale in dispositivi informatici che possono essere tecnicamente esaminati a supporto dell'attività investigativa. Gli esperti informatici forensi si trovano a dover cercare traccia di accadimenti in "luoghi" che fino a poco tempo fa era impensabile potessero contenere dati rilevanti per l'accertamento di un fatto: telecamere di sorveglianza, stampanti 3D, apparecchiature biomedicali e autoveicoli[3].

Il ricorso a informazioni desunte dai dati digitali conservati in supporti informatici o trasmessi attraverso le reti non riguarda solo il procedimento penale ma si estende a qualsiasi contesto in cui diventi necessario produrre, a sostengo della propria tesi, quelle che sono "rappresentazioni informatiche" di fatti (ad esempio e-mail, messaggi, post su piattaforme web)[4]. Tali elementi, tuttavia, implicano una maggiore difficoltà nella loro produzione rispetto all'epoca analogica; è noto, infatti, come venga attribuita alla prova informatica qualità di intrinseca oggettività, senza considerarne le caratteristiche di alterabilità, volatilità e intangibilità.

L'espressione *Computer forensics*, utilizzata per riferirsi alla disciplina sin dalle sue origini, è stata soppiantata dalla più ampia espressione *Digital forensics* (DF)[5] che, secondo le classificazioni generalmente proposte[6], comprende molteplici ambiti a seconda delle caratteristiche dei dispositivi oggetto di analisi o delle modalità di raccolta dei

[3] M. Ferrazzano, *Dai veicoli a guida umana alle autonomous car. Aspetti tecnici e giuridici, questioni etiche e prospettive per l'informatica forense*, Giappichelli, 2018.

[4] Nel processo civile, in ambito giuslavorista, in materia di diritto amministrativo, ma anche nelle investigazioni aziendali (*Corporate Digital forensics*), allo scopo di individuare eventuali attacchi informatici provenienti dall'esterno, scoprire dipendenti infedeli, attività di spionaggio, furto o danneggiamento dei dati, violazione delle policy aziendali e in ambito sanitario per la gestione del rischio clinico (informatica forense sanitaria). Gli esempi sono molteplici. Tra tutti si vedano: A. Gammarota, D. Caccavella, *L'informatica forense per l'E-Health*, in C. Faralli, R. Brighi, M. Martoni (a cura di) *Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth*, Giappichelli, 2015, pp. 205-220; U. Bardari, *L'esperimento giudiziale su posizionamento GPS e scatole nere per automobili,* in R. Brighi, M. Palmirani, E. Sánchez Jordán (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza*, Aracne, 2018, pp. 241-254.

[5] Le espressioni *Digital forensics* e informatica forense sono qui utilizzate indistintamente. Sul punto A. Gammarota, *Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali*, 2016, su Amsdottorato.unibo.it.

[6] V. nota 2.

dati: dall'esame di supporti di memorizzazione (*Disk forensics*), ai sistemi di rete (*Network forensics*) e ai dispositivi mobili (*Mobile forensics*), fino a nuovi ambiti e paradigmi tra cui, per citare i più dibattuti oggi, *Multimedia forensics*, *Embedded forensics*, *IOT forensics* e *Crypto forensics*.

Le nuove competenze nell'intelligenza artificiale e nella *data science* si stanno, inoltre, unendo al campo della *Digital forensics* a supporto dell'analisi delle attività criminali e, più in generale, delle attività di *intelligence*[7]. La raccolta di informazioni provenienti da fonti diverse, tra cui sorgenti aperte, e la conseguente esplorazione con metodi e tecniche che mirano a identificare *regolarità* e relazioni all'interno di grandi *dataset* dove la capacità analitica umana sarebbe insufficiente[8], fornisce un aiuto alla comprensione generale dei fenomeni e può guidare le strategie investigative[9].

Allo stesso tempo, si registra un progressivo aumento quantitativo e qualitativo di minacce e attacchi informatici che hanno impatti significativi su comunità, istituzioni e imprese[10]. L'informatica ha offerto nuove opportunità anche alle organizzazioni criminali che, a fronte di eterogeneità di target e motivazioni (finanziaria, terroristica, predatoria) sfruttano la complessità delle infrastrutture informatiche e di rete, complicando le indagini e le attività relative alla *Digital forensics* (DF)[11]. Sorgenti di dati sempre più ampie ed eterogenee, architetture distribuite, ubiquità degli spazi di archiviazione, tecniche anti-forensi, crittografia, virtualizzazione e la diffusione dei meccanismi di anonimato sono alcuni dei numerosi ostacoli che rendono difficile sia individuare l'azione criminosa e chi l'ha compiuta sia successivamente provare il suo accadimento. Peraltro, frequentemente l'esame dei supporti digitali si basa sul presupposto che le informazioni rilevanti saranno trovate in "luoghi" simili a quelli in cui sono state individuate in casi

[7] E. Casey, *The value of forensic preparedness and digital-identification expertise in smart society*, in *Digital investigation*, 2017, 22, pp.1-2.

[8] Molteplici sono le tecniche utilizzate in tale ambito, tra le più note: il *data mining*, il *datawarehouse,* il *machine learning*, il *clustering*.

[9] È questo il dominio della c.d. *Cyber Intelligence*. In argomento G. Costabile, *Indagini ditigali*, in S. Aterno, F. Cajani, G. Costabile, D. Curtotti (a cura di), *Cyberforensics e indagini digitali*, Giappichelli, 2021, pp.77 e ss.

[10] Numerosi rapporti di agenzie pubbliche, organismi e aziende registrano incidenti informatici, attacchi e minacce. Tra tutti si veda *ENISA Threat Landscape 2021*, su enisa.europa.eu.

[11] Sul punto si v. il Rapporto quadriennale di Europol SOCTA 2021 (*Serious and Organised Crime Threat Assessment)*.

precedenti, senza tenere conto della velocità con cui le nuove tecnologie appaiono sul mercato e che queste vengano adottate *in primis* dai criminali stessi. Di conseguenza, gli elementi di prova conservati in "luoghi" precedentemente sconosciuti o in quelli nuovi saranno ignorati dando luogo a un problema tipico delle scienze forensi che è quello dei *bias* cognitivi.

Pur in assenza di adeguati riferimenti normativi, la necessità di trovare soluzioni tecniche efficaci alle sfide contemporanee non deve indurre a intraprendere facili scorciatoie che prescindano dall'intersecarsi con le garanzie proprie del giusto processo. La prospettiva dell'attività tecnica resta quella della *utilizzabilità* in dibattimento delle informazioni raccolte, messe a disposizione di tutte le parti processuali per la valutazione di ogni aspetto rilevante e ciò a garanzia dell'esercizio del diritto di difesa e a salvaguardia dei diritti fondamentali dei soggetti coinvolti. Inoltre, ciò che si vuole evitare è che le indagini si trasformino in «vere e proprie incursioni investigative nel nucleo più intimo dell'individuo»[12], con un ruolo spesso attivo e decisivo di attori privati, tra cui i *provider* di servizi informatici la cui intermediazione per accedere ai dati oggetto di indagine è inevitabile.

Quel necessario connubio tra tecnica e diritto – esito della costruzione di una cornice epistemologica per le scienze forensi di riferimento con l'adozione di standard metodologici e strumenti tecnici adatti a garantire la certezza procedurale e la trasparenza[13] – si è consolidato in una maggior sensibilità al tema della prova informatica. Per assicurare l'opportuna flessibilità del sistema processuale con l'apporto della scienza nella ricerca della verità, i criteri della sentenza Daubert del 1993, accolti nel nostro Paese dalla sentenza della Cassazione penale n. 47789 del 2010, insieme all'art. 189 c.p.p. – che porta a vagliare criticamente gli elementi di prova per «assicurare l'accertamento dei fatti» senza che venga pregiudicata «la libertà morale delle persone» – stabiliscono come il giudice debba valutare l'indipendenza e la affidabilità dell'esperto, il rigore che ha accompagnato l'individuazione del sistema tecnologico utilizzato come strumento di prova, le finalità e gli

[12] Così si esprime R. Orlandi in *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma,* Riv. it. dir. proc. pen., 2018, 2, p. 539.

[13] Sul punto sia consentito il rimando a R. Brighi, C. Maioli, *Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologia*, in Informatica e diritto, 2015, XXIV, pp. 217-234; R. Brighi, M. Ferrazzano, *Digital forensics: best practices and perspective*, in Caianiello M., Camon A. (a cura di), *Digital forensics evidence. Towards common european standards in antifraud administrative and criminal investigations*, Wolters Kluwer, 2021, pp. 13-48.

studi che ne hanno permesso l'implementazione e, infine, l'attitudine esplicativa dei fondamenti scientifici delle teorie sottostanti.

Il confronto con tecnologie diverse, come quelle relative all'*Internet of Things* (IoT), al *Cloud computing*, ai dispositivi mobili, alla *blockchain* e alle criptovalute, nonché agli edifici intelligenti e persino alle *smart cities*, costringe gli scienziati forensi e i giuristi ad aggiornare e ripensare l'approccio all'informatica forense. Il tema centrale resta la prova informatica, in particolare la sua modalità di formazione, di acquisizione, di conservazione e di valutazione- e, con essa, il processo investigativo in cui si raccolgono gli elementi probatori mediante tecniche informatiche; tuttavia, ogni caso presenta nuove sfide e il futuro *Digital forensics expert* (DFE) dovrà essere equipaggiato con le conoscenze e le abilità per affrontare le molteplici questioni forensi nel caso presentato[14].

2. La "cassetta degli attrezzi": standard per le operazioni informatico forensi. Analisi dello stato dell'arte

Gli strumenti standard utilizzati nelle procedure di IF coprono tutti i diversi aspetti delle fasi di indagine informatica e seguono il dato nel suo ciclo di vita completo: dall'individuazione e acquisizione delle potenziali prove digitali, alla loro analisi, valutazione e conservazione, fino alla chiusura dell'indagine[15]. Ogni operazione manuale o automatizzata è condotta salvaguardando i requisiti tecnici di verificabilità, ripetibilità, riproducibilità e giustificabilità secondo il paradigma dalla catena di custodia[16]. Più nello specifico, le procedure tipiche di IF secondo un autorevole studio recente[17] possono essere ricondotte a tre principali ambiti: (1) analisi di dati archiviati e *file system*, (2) analisi

[14] E. Casey, c*it.*, pp. 1-2.

[15] I passaggi di cui si compone *la Digital investigation* sono descritti in particolare, nella norma tecnica ISO/IEC 27043 «*Information technology – Security techniques – Incident investigation principle and processes*».

[16] Requisiti fissati dalle norme tecniche di riferimento e in particolare dalla ISO/IEC 27037. Sulla catena di custodia L. Bartoli, C. Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in M. A. Biasiotti, M. Epifani, F. Turchi (a cura di*), Trattamento e scambio della prova digitale in Europa*, Edizioni Scientifiche Italiane, 2016, pp. 139-151.

[17] L. Caviglione, S. Wendzel, W. Mazurczyk, *The Future of Digital Forensics: Challenges and the Road Ahead,* in IEEE Security & Privacy, 2017, 15(6), pp. 12-17.

del traffico di rete e (3) *reverse engineering*, ciascuno dei quali si scontra con ostacoli e limiti dovuti all'evoluzione delle ICT.

Al primo ambito (1) si riferiscono tutte le attività legate all'estrazione di informazioni rilevanti dai supporti digitali oggetto di indagine: si tratta di analisi statiche se il dispositivo è spento (*post-mortem*), oppure *live* se il sistema è attivo. Nelle analisi statiche il rispetto dei principi di integrità, immodificabilità ed inalterabilità dei dati viene assicurato dall'impiego di strumenti che consentono l'accesso al dispositivo in modalità di sola lettura e creano copie forensi (o *bit-stream imagine*, o immagine bit a bit), duplicati delle sorgenti originali come le migliori pratiche suggeriscono e che possono essere utilizzati per analizzare file e applicazioni installate o per ispezionare lo spazio inutilizzato alla ricerca di frammenti di file cancellati. L'attenzione è posta non solo ai file e al loro contenuto ma anche a metadati, file temporanei, porzioni di file, *slack space*. Particolarmente importante, allo stato attuale della tecnica, è la valutazione dei sistemi *live* che consente ai DFE di esaminare prove potenzialmente nascoste in artefatti digitali quali i contenuti delle memorie volatili (RAM), l'elenco dei file aperti, i processi in esecuzione, le connessioni di rete e le unità esterne mappate[18]. L'analisi *live* è strategica per evitare la perdita di dati temporanei e l'inaccessibilità a dati protetti da cifratura al riavvio del dispositivo. L'uso di *filesystem* cifrati (specie nei dispositivi mobili, quali *smartphone* e *tablet*, oggetto della *Mobile forensics*) con procedimenti sempre più semplici da applicare per gli utenti finali è, infatti, in significativo aumento a seguito anche dell'impatto del Regolamento Generale per la Protezione dei Dati Personali (Regolamento UE 679/2016) e si pensa che possa diventare a lungo termine lo scenario predefinito. L'analisi dei dati archiviati si scontra, inoltre, con il volume delle informazioni disponibili che rende le operazioni di acquisizione lunghe e dispendiose, in termini di tempo e di risorse informatiche necessarie, e con la difficoltà di accesso a grandi *datacenter* tipici delle architetture *Cloud*. Il volume dei dati rappresenta un limite anche per le fasi di analisi e valutazione delle potenziali prove digitali, dove la selezione delle informazioni pertinenti all'accertamento richiede l'impiego di strumenti dedicati all'indicizzazione, ricerca e consultazione dei dati acquisiti.

[18] B. Nelson, A. Phillips, C. Steuart, *Guide to Computer Forensics and Investigation*s, Cengage, 2018, pp. 415 e ss.

Il secondo ambito (2) – l'analisi del traffico di rete – attiene alla *Network forensics* che si occupa dell'acquisizione e dell'analisi del traffico di dati tra più sistemi informatici collegati in rete (un *host*, un nodo intermedio, una intera porzione di rete) per accertare come è stato condotto un attacco, oppure come si è realizzato un certo evento sulla rete. In questo caso i DFE sfruttano sia la acquisizione diretta del traffico di rete sia i *file di log* dei servizi di rete, inclusi i *router*, i server DHCP, i *firewall*, i *proxy web*, e le informazioni raccolte da strumenti impiegati per la sicurezza informatica come i sistemi per il rilevamento delle intrusioni. Le tecniche più raffinate comprendono l'ispezione di ogni pacchetto per identificare la minaccia analizzando i campi di intestazione (*header*) oppure gli indirizzi IP. Anche in questo ambito, le operazioni forensi si scontrano con l'impossibilità tecnica di raccogliere, archiviare e analizzare l'enorme volume di traffico, con l'eterogeneità delle tecnologie utilizzate, con la crittografia delle comunicazioni e con i meccanismi di anonimizzazione in grado di nascondere l'IP del dispositivo da cui proviene l'azione[19].

Nella cassetta degli attrezzi del DFE si trovano, infine, (3) metodologie e strumenti per il *reverse engineering*. Nella raccolta delle prove, capire come è stato effettuato un attacco può richiedere un esame approfondito del software utilizzato e del suo funzionamento. Capire questo può aiutare ad arrestare l'attacco, e fornire riscontri o interpretazioni di prove già scoperte. La tecnica del *reverse engineering* è utile quando si tratta di esaminare codici non *open source*[20]; si esegue su codici binari di programmi informatici, sulle registrazione del traffico di rete o di altri dati dinamici per capire come funziona il software in assenza di documentazione e per interpretare i dati grezzi acquisiti in artefatti di livello superiore. È una tecnica che richiede tempo e non esiste un insieme standard di strumenti e procedure.

[19] A. Jayakrishnan, V. Vasanthi, *Empirical survey on advances of network forensics in the emerging networks*, International Journal of Cyber-Security and Digital Forensics, 2018, 7(1), pp. 38-46.

[20] I diritti di proprietà intellettuale e alcuni sistemi software di intelligenza Artificiale (IA) come il *machine learning* possono rendere difficile il controllo e la verifica del *modus operandi* degli strumenti forensi che dovrebbero supportare il processo decisionale umano.

Al fine di garantire i requisiti di integrità, autenticità e disponibilità delle informazioni che la legge pone nel disciplinare le modalità di esecuzione delle operazioni di DF[21], i paradigmi dell'agire tecnico si fondano su due elementi. Da una parte un elemento oggettivo, consistente nell'adesione agli standard e alle linee guida di settore che sono indipendenti da specifiche scelte tecnologiche e al contempo individuano una base condivisibile di procedure operative e modalità di indagini per gli informatici forensi; dall'altro un elemento soggettivo che consiste nel set di competenze che l'esperto forense applica ai dati informatici dal momento in cui la prova digitale in questione viene rilevata.

Gli esperti di DF seguono diverse linee guida, internazionali e di settore[22], ognuna delle quali stabilisce principi e metodi per la corretta gestione delle prove digitali. Si osserva come il contenuto delle norme tecniche negli anni sia cambiato, passando da un primo approccio molto dettagliato e proceduralizzato a un approccio che attribuisce maggior rilievo alla definizione della metodologia, alla formazione in Informatica giuridica e ai principi etici.

3. Le sfide e gli ostacoli principali

Rispetto alle prime applicazioni, è oggi molto più difficile ottenere progressi nella informatica forense per la rapida evoluzione e per la complessità degli scenari tecnologici moderni. *Review* della letteratura scientifica sul punto concordano nell'individuare quelle di seguito richiamate come le sfide più significative che devono essere affrontate sul piano tecnico e sul piano giuridico e metodologico[23].

[21] F. Costantini, M.A. De Stefani, *Il "controllo" della prova digitale. Questioni teoretiche, organizzative e operative*, in M.A. Biasiotti, M. Epifani, F. Turchi (a cura di), *op. cit*., pp. 105-119.

[22] Nel nostro Paese significativa in tal senso è la Circolare 1/2018 della Guardia di finanza che ha introdotto la figura professionale qualificata di Computer Forensics and Data Analysis (CFDA) responsabile dell'identificazione, raccolta e acquisizione di prove digitali.

[23] In particolare, L. Caviglione et al., *The Future of Digital Forensics*, cit.; R. Montasari, R. Hill, *Next-Generation Digital Forensics: Challenges and Future Paradigms*, IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019, pp. 205-212; E. O. Edward, J. A. Ojeniyi, *A Systematic Literature Review On Digital Evidence Admissibility: Methodologies, Challenges and Research Directions*, 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019; B. K. Sharma, M. A. Joseph, B. Jacob e B. Miranda, *Emerging trends in Digital Forensic and Cyber security - An Overview*, Sixth HCT Information Technology Trends (ITT), 2019; H. Majed, H. N. Noura e A.

- *Alte velocità e grandi volumi*. L'incessante crescita del volume di dati da acquisire, archiviare ed esaminare, conseguenza del continuo progresso della tecnologia di archiviazione nei dispositivi e nei servizi di *cloud* e dell'aumento del numero di dispositivi sequestrati per ogni caso, è un problema con cui gli investigatori si confrontano da tempo, tanto che oltre dieci anni fa è stato censito come uno dei principali motivi di crisi della *Digital forensics*[24]. Il tempo e le risorse *hardware* per la creazione della copia forense e per elaborare tutti i dati è spesso insufficiente.
- *Eterogeneità di piattaforme hardware e software e dei formati dati*. La presenza di numerose tecnologie nell'ambiente da indagare aumenta la complessità e impedisce lo sviluppo di standard e strumenti unificati. I dati, raccolti da sorgenti eterogenee quali *devices*, reti, spazi *cloud*, *social media*, sono caratterizzati da una ampia varietà di formati. Da segnalare è il grande aumento del numero e delle dimensioni di immagini digitali e video che vengono riscontrati nei dati oggetto di indagini. Questo, in parte, è dovuto al fatto che la presenza di fotocamere è una caratteristica ormai comune degli smartphone e alla maggiore penetrazione delle CCTV[25] che sono presenti nei veicoli, nei droni e in altri dispositivi. Frequentemente in questa "giungla"[26] diventa necessario sviluppare appositi programmi per l'identificazione della fotocamera che ha scattato le immagini o per capire se immagini diverse provengano dalla stessa sorgente. Analoghe problematiche si riscontrano nell'estrazione e interpretazione di informazioni mediante tecniche di *automatic speech recognition*, per esempio dagli ormai diffusissimi assistenti virtuali digitali.
- *Complessità dei sistemi e architetture distribuite.* Gli artefatti probatori sono spesso distribuiti su luoghi diversi, fisici e virtuali, conservati in *datacenter* dislocati su tutto il territorio, mediante i servizi di *cloud computing* con meccanismi di replicazione e

CHEHAB, *Overview of Digital Forensics and Anti-Forensics Techniques*, 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-5; P. REEDY, *Interpol review of digital evidence* 2016 - 2019, Forensic Science International, Synergy, 2020, 2, pp. 489-520.

[24] S.L. GARFINKEL, *Digital forensics research. The next 10 years*, Digital Investigation, 2010, 7, pp. S64-S73.

[25] Per *Closed circuit television* (CCTV) si intende l'uso di telecamere che trasmettono il segnale verso specifici o limitati set di monitor o supporti di registrazione.

[26] B. VAN WERKHOVEN, *et al*. *A Jungle Computing approach to common image source identification in large collections of images*, Digital Investigation, 2018, 27, pp. 3-16.

ridondanza (*multi-tenancy*); frammenti di informazioni possono trovarsi, oltre che nei singoli dispositivi, nei sistemi di comunicazione tra dispositivi "intelligenti" e mondo esterno (computer, smartphone) e anche in sistemi che sono al di fuori della rete oggetto di indagine (come *cloud*, social network, *internet service provider*, fornitori di reti mobili, identità virtuali online, portafogli virtuali di criptovalute). Determinare dove risiedano i dati e come acquisirli può porre molti ostacoli ai DFE che devono confrontarsi, non solo con sistemi complessi, tecnologie miste, interfacce e livelli di sicurezza differenti (piano tecnico), ma anche con giurisdizioni diverse (piano legale) e con la mancanza di collaborazione dei *provider* dei servizi (piano organizzativo).

– *Crittografia.* Se da un lato lo sviluppo, l'attuazione e l'utilizzo della crittografia forte è uno «strumento necessario per tutelare i diritti fondamentali e la sicurezza digitale dei governi, dell'industria e della società»[27], riconosciuto dalle autorità dell'Unione Europea responsabili della protezione dei dati e della cibersicurezza, nel contempo essa è una delle maggiori sfide che le autorità competenti devono affrontare per poter avere accesso agli elementi di prova che consentono di contrastare terrorismo, criminalità organizzata e altre forme di cibercriminalità. La crittografia è utilizzata in tutti i settori della vita pubblica e privata. Non solo le applicazioni e i dispositivi elettronici sono programmati per crittografare per *default* i dati archiviati degli utenti, ma sempre più canali di comunicazione e servizi di archiviazione dei dati sono anche protetti dalla crittografia *end-to-end*. La crittografia può essere applicata su una cartella, su un servizio *cloud*, sui dispositivi mobili e sui dati memorizzati in un *database* o trasmessi tramite e-mail. Tali tecnologie richiedono una grande quantità di risorse informatiche per essere aggirate. A tal fine, le opzioni possibili vanno dall'utilizzo di *exploit*, ovvero programmi che sfruttano debolezze note dei sistemi per raggirare la crittografia, all'acquisizione (*dump*) e analisi del contenuto della memoria RAM[28] per cercare la password di decrittazione nei casi in cui sia

[27] Consiglio dell'Unione Europea, *La sicurezza attraverso la crittografia e nonostante la crittografia,* 13084/1/20, 2020.

[28] Questa attività è particolarmente complessa per l'assenza di documentazione pubblica della struttura dei software e spesso richiede il *reverse engineering* dei programmi per comprendere come sono create le strutture dati.

possibile accedere al dispositivo acceso; fino a condurre attacchi a forza bruta o a dizionario per indovinare la password di cifratura. Se i dati sono cifrati utilizzando moderne tecniche diventa molto difficile recuperare il contenuto senza disporre della chiave di cifratura[29].

– *Nuove minacce e criminalità informatica*. Anche se le prove digitali sono ormai presenti in qualsiasi indagine penale, alcuni crimini sono più di altri legati all'uso della tecnologia e, dunque, per essi un buon risultato investigativo dipenderà maggiormente dalla abilità nell'uso delle stesse tecnologie. Il Rapporto quadriennale di Europol SOCTA 2021 registra come praticamente tutte le attività criminali organizzate abbiano una componente online o abbiano effettuato una transizione definitiva sulla rete. I criminali sfruttano le comunicazioni criptate per collegarsi in rete tra di loro, usano i social media e i servizi di messaggistica istantanea per raggiungere un pubblico più ampio con lo scopo di pubblicizzare beni illegali o diffondere disinformazione. L'ambiente online e il commercio online forniscono l'accesso a competenze e strumenti sofisticati anche ai gruppi privi di competenze tecnologiche, secondo un nuovo modello criminale noto come *Crime As a Service*.
– *Tecniche anti-forensics.* Man mano che le misure difensive diventano sempre più efficienti è possibile prevedere un dispiegamento più aggressivo di metodi antiforensi che impediscono le operazioni forensi con vari mezzi, alcuni dei quali sono oggetto di ricerca. L'*Interpol review of digital evidenc*e 2016-2019 evidenzia come la ricerca nell'ambito dell' *anti-forensics* rappresenti solo il 2% del totale della ricerca in DF. Le tecniche *anti-forensics*, generalmente, si riconducono a quattro categorie[30]: (1) occultamento dei dati che avviene mediante la crittografia, la steganografia impiegata perché non solleva il sospetto di uno scambio di informazioni, e sistemi specifici per i dati in transito quali *Virtual Private Network* (VPN); (2) cancellazione degli artefatti, ovvero distruzione permanente (*wiping*) di file, partizioni o dischi, smagnetizzazione/distruzione di supporti di memorizzazioni, cancellazione delle informazioni presenti sui registri di

[29] H. MAJED *et al*., cit.
[30] *Idibem.*

sistema, manipolazione dei metadati; (3) offuscamento delle tracce, tra cui manipolazione dei file di log, *spoofing* degli indirizzi IP, sfruttamento di reti P2P e di *server proxy* e infine (4) attacchi contro strumenti forensi e processi, quali metodi che contrastano il *reverse engineering* o attacchi all'integrità degli *hash*.

Le nuove sfide connesse alla complessità degli scenari attuali non riguardano la sola dimensione tecnologica bensì si riflettono sulla dimensione legale e su quella metodologico-organizzativa con riferimento, in particolare, alla legittimità delle operazioni di informatica forense, al rispetto dei diritti fondamentali, tra cui il diritto alla riservatezza e alla protezione dei dati personali, e alla definizione di nuovi standard e percorsi formativi.

Il perimetro transnazionale delle indagini e la necessità di delegare a soggetti terzi (i *provider* dei servizi) alcune attività tecniche sono tra le più importanti sfide sul piano delle legittimità della DF, che deve confrontarsi con legislazioni e procedure differenti. Come illustrato poc'anzi, gli strumenti di indagine tradizionali sono diventati meno efficaci a causa delle misure tecniche di protezione dei dati e dei supporti e, dunque, l'uso di strumenti di *hacking* da parte degli investigatori delle Forze dell'Ordine, finalizzati a superare le misure di protezione del sistema informatico e a prenderne il controllo – tra cui il dibattuto "captatore informatico"[31] – sembra l'alternativa maggiormente efficace per rispondere alle esigenze di accertamento[32]. I rischi non sono tuttavia trascurabili, sia per la conseguente compromissione della sicurezza dei sistemi *hackered* sia perché le nuove potenzialità intrusive possono

[31] Un software che fornisce una serie di possibilità operative molto efficaci in quanto permette all'investigatore di assumere, da remoto, il controllo totale del dispositivo c.d. *target* o bersaglio. L'uso dello strumento per le intercettazioni ambientali è stato oggetto di recente regolazione a partire dalla c.d. "Riforma Orlando". Per tutti si veda S. SIGNORATO, *Rimodulazioni normative dell'uso investigativo del captatore informatico,* in G. Giostra, R. Orlandi (a cura di) *Revisioni normative in tema di intercettazioni*, Giappichelli, 2021.

[32] Con riferimento all'esigenza di recuperare l'efficacia dello strumento delle intercettazioni, Cajani osserva che «a fronte dell'esistenza di un rimedio più agevole (se pur più costoso) quale quello del trojan, gli investigatori hanno fatto la loro scelta di campo». Cfr. F. CAJANI, *The song remains the same: riflessione sul tempo che passa e sulla necessità di macchine utile per una effettiva tutela delle vittime di reati*, In F. Cajani, G. Cernuto, G. Costabile, F. D'Arcangelo (a cura di), *Le nuove frontiere dell'acquisizione degli elementi di prova nel cyberspace*, e-book IISFA, 2017.

andare a limitare le garanzie della persona e le libertà costituzionali[33]. Il modo in cui tali tecniche vengono utilizzate determina il livello di tutela dei diritti degli individui coinvolti.

A prescindere dall'attuale contesto tecnologico, risulta pertanto fondamentale da un lato preservare i poteri delle autorità competenti nel settore della sicurezza e della giustizia penale attraverso un accesso legittimo che consenta loro lo svolgimento dei compiti secondo quanto prescritto e autorizzato dalla legge, d'altro lato le previsioni di tali poteri esecutivi devono sempre rispettare il giusto processo e altre garanzie processuali, nonché i diritti fondamentali, in particolare il diritto al rispetto della vita privata e del carattere privato delle comunicazioni e il diritto alla protezione dei dati personali.

Sono potenzialmente oggetto di analisi tutti quei dati che costituiscono il patrimonio informativo della persona e che coesistono in modo promiscuo negli spazi digitali. Occorre, perciò, definire procedure sul piano giuridico, organizzativo e tecnico che consentano un accesso selettivo ai dati in modo da trovare un giusto bilanciamento tra l'esigenza di acquisire informazioni pertinenti e puntuali per l'accertamento di specie secondo gli standard della informatica forense e il diritto alla riservatezza, alla protezione dei dati di terzi e anche diritto alla protezione di dati classificati come segreti industriali.

La definizione di metodi e linee guida standardizzate per rilevare, acquisire, conservare, analizzare e presentare le prove digitali, sempre al centro dell'attenzione della comunità dei DFE, stenta a tenere il passo con le tecnologie emergenti. In particolare, la cooperazione in indagini trasnazionali richiede la capacità di elaborare informazioni in modo collaborativo o l'utilizzo di risorse di archiviazione e computazione condivise in laboratori centralizzati. Pertanto, di fondamentale importanza è concordare, unitamente a modelli formali del processo di investigazione forense, formati standard, schemi e ontologie efficaci per gli artefatti di DF.

Trasversale alle linee tracciate è una attenzione crescente alla gestione della qualità, alla mitigazione degli errori, ai test degli strumenti e alle metodologie di verifica. Il *Scientific Working Group on Digital*

[33] Una ricognizione a livello europeo di strumenti e pratiche è tracciata nel documento della Commissione Libertà civili, giustizia e affari interni (LIBE) del Parlamento europeo, *Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* (2017). In argomento G. Ziccardi, *Parlamento Europeo, captatore e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in Arch. Pen., 2017, 1.

Evidence (SWDGE)[34] ha proposto, a riguardo, un *framework* di base[35], che si interseca alle norme ISO 17020 e 17025, su cui sviluppare sistemi per la gestione della qualità con un approccio di mitigazione degli errori basato su test e convalida degli strumenti forensi digitali che, tuttavia, non si occupa della valutazione delle prove e della mitigazione dei *bias*.

Nella valutazione dell'errore umano devono essere considerati anche i fattori cognitivi e il loro impatto sul processo decisionale[36], sui quali incidono molti aspetti, tra cui la formazione e la motivazione, le aspettative di base, l'organizzazione e dunque le pressioni per le riduzioni dei costi, le informazioni non rilevanti sul caso. La fallibilità del ragionamento umano è un forte incentivo a seguire il metodo scientifico nelle analisi delle *digital evidence* per mitigare i rischi di errore. Anche nella DF vale il principio fondamentale delle scienze forensi, ossia che le opinioni degli esperti non dovrebbero essere espresse come fatti ma che sia necessario considerare più ipotesi alternative e che i risultati delle analisi dovrebbero essere espressi in termini di probabilità, evitando una terminologia che includa pregiudizi[37].

4. Aree emergenti e linee di ricerca

Davanti alle sfide e alle opportunità sollevate dall'incessante progresso tecnologico degli strumenti informatici e dalla loro diffusione capillare ed eterogenea tra gli utilizzatori, emergono nel perimetro dell'informatica forense nuove aree e linee di ricerca; su alcune di esse la comunità scientifica e gli operatori di IF si confrontano da qualche tempo[38], altre sono al centro del dibattito più recente.

Tra queste, *in primis*, la *Cloud Forensics,* area che si discosta sensibilmente dal paradigma tradizionale client-centrico dove l'investigatore ha accesso diretto ai supporti fisici. Negli ambienti virtualizzati del

[34] Autorevole gruppo di lavoro scientifico statunitense che riunisce le organizzazioni impegnate nel campo delle prove digitali con lo scopo di rafforzare la cooperazione tra gli enti e garantire la qualità e coerenza delle attività svolte dalla comunità forense.

[35] *SWGDE Establishing a Quality Management System for a Digital and Multimedia Organization under ISO-IEC 17025 or 17020*, Version: 2.0 (June 17, 2021) e *SWGDE Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers* Version: 1.0 (September 25, 2017).

[36] Sul punto P. Reedy, *op. cit.*, pp. 496-497.

[37] Ad esempio, l'*UK Forensics Science Regulato*r ha stabilito che frasi come "nelle vicinanze di" e "corente con" devono essere utilizzate solo con *caveat*. *Ibidem* p. 497.

[38] Cfr. in particolare C. Maioli (a cura di*), Questioni di Informatica forense,* Aracne, 2015.

cloud, soprattutto nel modello di *Software As a Service*, l'accesso alle informazioni può essere minimo e gli artefatti probatori tradizionali sul dispositivo dell'utente (voci di registro, file temporanei, log) estremamente volatili. Tuttavia, molte funzioni utili alla investigazione possono essere già presenti ed acquisite direttamente dalla piattaforma *cloud* comunicando con le API pubbliche[39] dei moduli del servizio con vantaggi legati all'immutabilità dei dati[40]. Diversi strumenti e metodologie sono oggetto di studio e valutazione[41]: (1) strumenti che esaminano i dati direttamente sul *cloud* per risolvere il problema della copia e trasferimento di dati molto voluminosi; (2) modelli di *forensics readiness,* basati su agenti, per registrate eventuali elementi utili alle indagini in via preventiva; (3) ontologie computazionali che collegano i dati del web con i dati di provenienza e dunque con i dati dell'utente per scoprire eventuali manomissioni delle informazioni. Come anticipato *supra* §3, le sfide non sono solo tecniche, ma riguardano anche il piano organizzativo e il piano legale. La catena di soggetti che devono comunicare e collaborare per facilitare le attività forensi sul *cloud* è ben individuata nei seguenti attori[42]: *Investigators*, IT *professionals*, *Legal advisors*, *Law enforcement*, *Third parties* e Università. Queste ultime hanno il compito di favorire lo sviluppo della ricerca scientifica, di proporre nuovi percorsi multidisciplinari per l'istruzione e per la formazione in ambito informatico forense e di contribuire alla nascita di *startup* e studi legali specializzati.

Collegate strettamente alla *Cloud Forensics,* emergono la *IOT Forensics* e la *Big Data Forensiscs.*

La *IOT Forensics* rileva sia in termini delle molte opportunità per le investigazioni – dalla identificazione del sospetto grazie alle informazioni biometriche e identità personali conservate nei dispositivi alla possibilità di capire esattamente cosa è accaduto in un certo ambiente – sia in termini di criticità legate alla durata di vita molto breve dei dati conservati localmente nei dispositivi, alla vulnerabilità degli stessi, alle interfacce proprietarie, alla cifratura e allo spostamento dei dati su altri dispositivi e nel *cloud* con conseguenze sulla ricostruzione della

[39] Le API (Application Programming Interface) sono interfacce di programmazione basate su servizi web.

[40] Sul punto si veda, in particolare, C. FEDERICI, *Nuovi orizzonti per l'acquisizione remota di Personal Cloud Storage*, in *Questioni di Informatica forense*, cit., pp. 113-132.

[41] P. REEDY, *op. cit*., pp. 499 e ss.

[42] G. COSTABILE, *Indagini digitali*, cit., pp.71-72.

timeline degli eventi. La ricerca in questo ambito si rivolge anche, ma non solo, (1) allo sviluppo di modelli per ricostruire gli eventi fisici sulla base di dispositivi disomogenei negli ambienti, ad incentivare la condivisione di informazioni sulle proprietà dei dispostivi utili per le indagini forensi in modo che l'investigatore possa effettuare preliminarmente un'analisi costi-benefici; (2) allo sviluppo di *tool* di *forensics readiness* per il recupero automatico della cronologia di registrazione delle informazioni e della corretta collocazione temporale; (3) alla definizione di meta-interfacce unificate per l'IOT forense che copra un ampio spettro di dispositivi e interfacce di basso livello di diversi fornitori[43]. L'attenzione va inoltre posta alle questioni legate alla privacy degli individui per consentire di mantenere il controllo delle informazioni sensibili memorizzate nei dispositivi IOT personali.

La *Big Data Forensics*[44] affronta invece il problema dell'aumento della dimensione quantitativa e qualitativa dei dati oggetto delle attività forensi. Negli ultimi anni sono stati proposti strumenti basati sul *data mining* o più in generale su tecniche avanzate di *Business analitycs* in grado di elaborare i dati con modelli statistici senza alcuna predeterminazione degli obiettivi per cercare correlazioni non immediatamente visibili. A queste tecniche si affiancano: (1) soluzioni su sistemi distribuiti che offrono una maggior potenza di elaborazione; (2) strategie di *data reduction*[45]; (3) tecniche di *Natural Language Processing* (NLP) per il *clustering* e la categorizzazione dei dati non strutturati; (4) l'adattamento di algoritmi di apprendimento automatico (MLA) per un uso specifico nel contesto unico del DF. Al di là delle soluzioni tecniche, sembra comunque imprescindibile nel contesto Big Data ripensare alle fasi tradizionali della DF prevedendo una fase di *triage*[46], compatibile con le garanzie processuali, in cui gli investigatori possano estrarre e acquisire solo le informazioni rilevanti per l'indagine di specie.

Ulteriori aree emergenti, connesse tra loro, sono la già citata *Cyber Intelligence* che si avvale di tecniche per incrociare dati di natura diversa – tra cui, informazioni desunte mediante OSINT (*Open source*

[43] L. Caviglione et al., *op. cit*., p. 15.

[44] R. Montasari *et al*., *op. cit*., p. 209-210.

[45] La strategia di riduzione dei dati impiegata può variare a seconda della natura dell'indagine, ma c'è una certa prevedibilità basata sul tipo di crimine. Per esempio, un'indagine sulla droga è di solito principalmente interessata alle comunicazioni, mentre un'indagine sulla pedopornografia è di solito interessata alle immagini.

[46] *Ibidem*. Sull'importanza di potenziare la fase di *triage* E. Casey, *The chequered past and risky future of digital forensics,* Australian Journal of Forensic Sciences, 2019, 51:6, 649-664.

intelligence) da fonti eterogenee aperte (pagine web, social network[47], ecc.) – come supporto decisionale alle attività di prevenzione o repressione a integrazione del livello cognitivo umano, la *Dark Web Intelligence* e la *Crypto Forensics*[48].

Trasversalmente alle aree introdotte, per far fronte alle molteplici sfide, è diventato prioritario lo sviluppo di sistemi che automatizzino le fasi di raccolta e acquisizione delle potenziali prove digitali in una ottica di *forensics readiness.* In questa linea evolutiva si colloca la *Digital Forensics as a Service* (DFaaS)[49], nuovo paradigma in cui sono fornite *utility* per le operazioni di DF, come l'analisi dei log, l'indicizzazione dei dati e l'elaborazione multimediale, sfruttando il modello del *cloud computin*g. Le soluzioni DFaaS facilitano la gestione efficiente delle risorse e permettono agli investigatori di condividere le conoscenze e cooperare. Altre ricerche propongono lo sviluppo di sistemi per una gestione robusta delle prove digitali che, sfruttando il protocollo *blockchain*, sono in grado rappresentare in modo immutabile la *chain of custody* delle prove, di ordinarle nella linea del tempo e di esprimere, per ognuna di esse, con una metrica pesata, il livello di fiducia dell'esperto[50]. A completamento del quadro, si aggiunge anche la promozione di metodologie che utilizzando la *Computer vision* per migliorare la comprensione dei fenomeni in esame, sia durante l'analisi dei dati raccolti sia durante la presentazione delle risultanze dell'esperto DF nella fase dibattimentale.

Inevitabilmente, infine, l'informatica forense, come tutti gli altri ambiti della moderna società tecnologica, deve e dovrà confrontarsi con l'intelligenza artificiale (IA), sotto un duplice profilo: (1) l'IA come ostacolo per le attività di indagine forense, a causa di sofisticate forme di falsificazioni delle prove quali i *deepfake*, i sistemi perturbativi, il *machine learning* avverso e le molte criticità legate alla ispezionabilità dei programmi e (2), l'IA come supporto alle attività di *digital forensics*.

[47] I principi della *Digital forensics* sono applicati anche alla *Social Network Analysis* con lo scopo di raccogliere dati e informazioni in modo rigoroso e scientifico al fine di comprendere la vera portata di un evento.

[48] G. Costabile, *Indagini digitali,* cit, pp. 76 e ss.

[49] H.M.A. van Beek et al., *Digital forensics as a service: Stepping up the game*, Forensic Science International: Digital Investigation, 2020, 35.

[50] D. Billard, *Weighted Forensics Evidence Using Blockchain*, in International Conference on Computing and Data Engineering - ICCDE 2018, 2018, pp. 57–61.

Le direttrici per l'applicazione di tecniche di IA a supporto dell'informatica forense, tracciate dalle ricerche più recenti, sono sostanzialmente due[51]. La prima linea riguarda l'automazione delle diverse fasi di trattamento delle potenziali prove informatiche, dall'individuazione all'analisi dei dati, tra cui: algoritmi per estrarre informazioni da set di dati complessi, identificazione e individuazione di elementi (persone, oggetti, volti) in immagini e video, estrazione di segnali da tracce audio, analisi del linguaggio naturale e classificazione dei contenuti crittografati[52]. La seconda linea ha l'obiettivo di guidare l'esperto nelle fasi di valutazione dei potenziali elementi di prova attraverso l'interpretazione di fatti noti integrando e correlando le diverse tracce trovate, riguarda quindi sistemi di supporto alle decisioni per formare ipotesi o confrontare ipotesi alternative e sistemi per la condivisione delle informazioni sulle prove e sulle operazioni svolte (*chain of custody*).

Elemento dibattuto delle applicazioni della IA in ambito legale-giudiziario[53] è la *spiegabilità* perché una eventuale mancanza di controllo e trasparenza si sconterebbe con i requisiti che devono essere garantiti nel trattamento della prova informatica e precluderebbe la possibilità di verificare se ci siano state alterazioni nei dati.

Il tema è affrontato anche dal recente Regolamento sull'Intelligenza Artificiale della Commissione Europea del 21 aprile 2021 che, più in generale, ha l'obiettivo di delineare un quadro giuridico comune, in grado di valutare il livello di rischio associato ad ogni possibile ambito applicativo[54]. La proposta di Regolamento classifica i prodotti che utilizzano completamente o parzialmente il software di IA in base al rischio di impatto negativo su diritti fondamentali quali la dignità umana, la libertà, l'uguaglianza, la democrazia, il diritto alla non discrimina-

[51] S. Costantini, G. De Gasperis, R. Olivieri, *Digital forensics and investigations meet artificial intelligence. Annals of Mathematics and Artificial Intelligence*, 2019, 86, pp. 193–229.

[52] Diversi prodotti professionali propongono per tali operazioni, già oggi, soluzioni basate su IA.

[53] Opinione generalmente riconosciuta tra gli studiosi di intelligenza artificiale per il diritto (G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione*. Giappichelli, 2016) è che, per avere soluzioni efficaci nel dominio giuridico, si debbano combinare tecniche per la modellazione logica esplicita della conoscenza e del ragionamento con tecniche di apprendimento automatico, orientandosi verso uno standard debole di IA che consenta all'essere umano di mantenere il controllo della macchina. Si veda anche G. Canzio, *Intelligenza artificiale, algoritmi e giustizia penale*. Sistema Penale (sistemapenale.it), 2021.

[54] La proposta si inserisce nella più ampia strategia dell'Unione europea che, a partire dalla Comunicazione "Intelligenza artificiale per l'Europa" COM(2018) 237, ha riconosciuto l'importanza strategica dell'IA per lo sviluppo del futuro dell'Unione ad ogni possibile ambito applicativo di questa tecnologia.

zione, la protezione dei dati in particolare per la salute e la sicurezza; più il prodotto è suscettibile di mettere in pericolo questi diritti, più severe sono le misure adottate per eliminare o mitigare l'impatto negativo sui diritti fondamentali, fino a vietare quei prodotti che sono completamente incompatibili con questi diritti.

In linea con la proposta di Regolamento e con il "Piano coordinato sull'intelligenza artificiale" – COM(2018)795 della Commissione europea, l'Italia ha presentato nel novembre di quest'anno il proprio "Programma Strategico per l'Intelligenza Artificiale per il 2022-2024"[55] che comprende, tra le sue ventiquattro politiche, anche la definizione di un sistema di governance nazionale a supporto della certificazione dei prodotti di IA immessi sul mercato (con profili di rischio più elevati, in particolare per la salute, la sicurezza o i diritti) con la definizione di chiari strumenti armonizzati con la proposta europea di Regolamento. Certamente, lo sviluppo di nuovi prodotti industriali per la DF basati sull'IA dovrà avvenire nel perimetro di certificazioni, tracciabilità, documentazione, supervisione umana così come delineato dal quadro delle iniziative europee.

Ogniqualvolta si introduce un nuovo strumento occorre domandarsi se i potenziali elementi di prova raccolti con queste tecniche investigative rispondano o meno ai requisiti di verificabilità, ripetibilità, riproducibilità, giustificabilità: requisiti alla base delle linee guida e degli standard tecnici che definiscono un sistema forte di garanzie in tema di acquisizione e analisi dei dati, in una prospettiva di bilanciamento delle opposte esigenze.

Il campo dell'informatica forense sta affrontando sfide che sono spesso difficili da superare. La definizione di un quadro giuridico comune e armonizzato, la condivisione di protocolli operativi aggiornati e testati, di standard metodologici rigorosi in tutte le fasi del processo sono elementi essenziali per un approccio comune di cooperazione, unitamente a un continuo aggiornamento delle competenze, degli strumenti e alla formazione interdisciplinare.

Pare che la comunità scientifica e la pratica aziendale stiano lavorando esclusivamente sul piano del contenimento delle sfide portate dal cybercrimine e che via sia la tendenza a considerare endemici i problemi di "insicurezza" informatica che danno origine al lavoro della

[55] Il Programma è consultabile in https://assets.innovazione.gov.it/1637937177-programma-strategico-iaweb-2.pdf.

DF. Servirebbe un approccio sistemico e unitario per affrontare compiutamente le violazioni dei sistemi informativi e più in generale la gestione della sicurezza. Crediamo che le ricadute organizzative e tecnico-professionali della recente istituzione della Agenzia per la cybersicurezza Nazionale (legge n. 109 del 4 agosto 2021) saranno di grande aiuto alla diffusione e consolidamento della DF soprattutto per gli aspetti che riguardano: il raccordo unitario per lo sviluppo di capacità nazionali per il rilevamento di incidenti informatici, la certificazione nazionale di metodi e strumenti per la cybersicurezza, l'innalzamento della sicurezza dei sistemi ICT inclusi nel perimetro nazionale dei collegamenti delle reti e dei sistemi informativi, il supporto allo sviluppo di competenze scientifiche, di progetti per l'innovazione e di qualificata formazione nel campo della sicurezza informatica.

Si auspica dunque un potenziamento della collaborazione tra tutti gli attori del campo, *law enforcement*, istituzioni accademiche e aziende, per mantenere un dialogo costante sul futuro della DF e su come affrontarne gli aspetti più impegnativi.

***

Pochi anni sono trascorsi dalla pubblicazione delle "prime" *Questioni di Informatica forense* (a cura di Cesare Maioli, Aracne Editrice, 2015). Da allora, la riflessione giuridica e filosofica sulle innovazioni tecnologiche, metodologiche e scientifiche non si è arrestata.

Il volume *Nuove questioni di Informatica forense* nasce con l'obbiettivo ambizioso di tenere alta l'attenzione sulle sfide contemporanee dell'Informatica forense e di creare uno spazio aperto per lo scambio di idee e opinioni tra studiose e studiosi, operatori del diritto e professionisti del settore in una dimensione interdisciplinare e da diversi angoli prospettici, fotografia del dialogo costante alimentato dagli incontri seminariali del corso di Informatica forense che ho il privilegio di tenere all'Università di Bologna dal 2017.

Il Volume è organizzato in quattro parti.

La prima parte delinea *la sistematica evolutiva delle nuove tecnologie forensi* sul profilo giuridico e metodologico. Il contributo di Silvia Golin, sulla acquisizione in sede investigativa e utilizzabilità dibattimentale della prova digitale, in raccordo con il Volume "Questioni di

informatica forense" del 2015, presenta – dalla prospettiva del magistrato – un tema classico dell'Informatica forense da cui si diramano molteplici questioni. Sulla *discovery* della prova digitale, alla ricerca di un difficile equilibrio tra esigenze investigative e prerogative processuali da tutelare, si interrogano Michele Ferrazzano e Leonardo Summa, che avanzano una proposta metodologia per la selezione dei dati informatici, e Laura Bartoli che, partendo dalle indicazioni della Corte europea dei diritti dell'uomo, riflette criticamente sul diritto di accesso e sul principio di parità delle armi. Il delicato equilibrio tra diritto alla protezione dei dati personali e esigenze di accertamento dei reati – oggetto di recenti modifiche dell'assetto normativo in tema di *data retention* – viene affrontato, sul piano giuridico, nel contributo di Silvia Signorato e sul piano metodologico e tecnico da Ilaria Caprilli e Raffaella Brighi. L'analisi dello sviluppo delle tecnologie di intercettazione, nello specifico del captatore informatico e dei suoi usi insidiosi, condotta da Alfonso Buccini e Donato Eugenio Caccavella, chiude la parte sistematica per la lasciar spazio alle nuove sfide.

La seconda e la terza parte del Volume sono dedicate alle frontiere della IF che si espandono, sollevando questioni giuridiche e tecnologiche ancora inesplorate e rinnovando le tradizionali criticità insite nella natura della prova digitale.

I contributi raccolti nella seconda parte affrontano, nello specifico, aspetti della *forensics* nei contesti dell'IOT, nei contesti di anonimato tipici del *darkweb* e, più in generale, nelle indagini digitali sui Social media e piattaforme online. Fausto Galvan, Federico Costantini, Marco Alvise De Stefani e Sebastiano Battiato trattano il problema della 'Qualità dell'informazione' nell'ecosistema IOT proponendo un modello teorico per la valutazione della prova informatica estratta in tale contesto, mentre Rosa Domina affronta i profili di rischio legati al trattamento dei dati personali raccolti dall'IOT per le applicazioni di eHealth. Le problematiche relative all'identificazione del soggetto e all'acquisizione delle informazioni utili alla ricostruzione delle azioni criminose e la conseguente necessità di normare e regolare i poteri e gli strumenti di indagine in tali contesti sono affrontate, dal punto di vista dei *law enforcement*, nei contributi di Andrea Paselli e di Ulrico Bardari, mentre Pasquale Sammario e Raffaella Brighi affrontano nello specifico il riciclaggio di criptovalute. Ai quesiti in merito all'acquisizione e utilizzazione processuale dei dati digitali prodotti dall'utilizzo dei social network e di messaggistica istantanea si rivolge il contributo

di Antonio Pugliese, mentre Vincenzo Colarocco e Michele Ferrazzano affrontano le questioni giuridiche e tecniche legate alle pratiche di concorrenza sleale nelle piattaforme di *advertising online*.

Nella terza parte del Volume ci si interroga sulla complessa e promettente dialettica tra Intelligenza Artificiale e Informatica forense. I contributi di Giulia Lasagni, di Corrado Federici, di Pier Giorgio Chiara e Isadora Neroni Rezende esplorano le potenzialità dell'intelligenza artificiale alla ricerca di nuovi paradigmi investigativi; con riferimento, rispettivamente: (1) all'impiego di taluni sistemi IA noti come *Multi-Agent Systems* (MAS) presentati dall'autrice come strumento per ampliare la nozione di *fairness,* e quindi la tutela dei diritti di difesa, già nella fase delle indagini, (2) alle tecniche di *deep learning* per l'analisi del *sentiment* su corposi insiemi di testi per ricavare l'andamento nel tempo dell'umore di un individuo o di un gruppo ed apprezzarne immediatamente gli eventuali repentini mutamenti, e (3) allo studio della disciplina normativa, unitamente a un'analisi tecnica, per chiarire se l'impiego di modelli di IA nell'analisi dei metadati del traffico telematico criptato possa essere d'aiuto per ridurre l'invasività delle operazioni di sorveglianza delle forze dell'ordine. Luca Guarnera, Oliver Giudice e Sebastiano Battiato affrontano, invece, gli ostacoli posti alle attività tipiche della *Multimedia Forensics* da sofisticate forme di falsificazioni delle prove, basati su IA, quali sono i *deepfake*. Il contributo di Giuseppe Contissa, Federico Galli, Francesco Godano e Galileo Sartor chiude questa terza parte con la presentazione della nuova Proposta di Regolamento europeo, proposta che, tra le possibili applicazioni della IA, classifica come sistemi ad "alto rischio" quei sistemi rientranti nella categoria attività di contrasto (Allegato III, n. 6, let. d) quali sistemi «per la valutazione dell'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati», «per individuare i deep-fake» e «per l'analisi criminale riguardo alle persone fisiche, che consentono alle autorità di contrasto di eseguire ricerche in set di dati complessi, correlati e non correlati».

Il Volume si chiude con una raccolta di contributi che studiano nuovi modelli per la cooperazione giudiziaria e per l'integrazione degli strumenti investigativi dell'Unione, a fronte della circolazione transnazionale della prova digitale. Antonio Gammarota apre la quarta sezione con l'analisi delle norme del Regolamento della Procura Europea (EPPO) – Regolamento (UE) 2017/1939 – che rientrano nel perimetro

di interesse dell'Informatica forense, con l'intento di individuare eventuali intersezioni con i principi e la disciplina interna. Il contributo di Maria Angela Biasiotti e Sara Conti si focalizza sul cammino della prova digitale in Europa tracciando il percorso fatto, fino agli attuali strumenti che le autorità giudiziarie degli Stati membri hanno a loro disposizione per scambiarsi le prove stesse utilizzando la tecnologia. Infine, i contributi di Silvia Moffa e di Giovanna De Rugeriis, entrambi in tema di informatica giudiziaria, si soffermano il primo sull'analisi della gestione dei flussi documentali digitali di competenza della Procura Europea, e il secondo sulle innovazioni nel processo penale telematico a seguito dell'emergenza COVID e delle recenti riforme, auspicando una visione sul futuro del sistema processuale penale nel quale la dimensione digitale sarà «forma e contenuto dell'intero procedimento».

Desidero ringraziare tutte le Autrici e gli Autori che hanno partecipato al Volume con esperienza, rigore scientifico e passione.

Un ringraziamento sincero va a Monica Palmirani per il sostegno alla pubblicazione e a Pasquale Sammario e Leonardo Summa che hanno contribuito alla cura editoriale.

A Cesare Maioli la mia profonda gratitudine.

PARTE I

SISTEMATICA EVOLUTIVA DELLE NUOVE TECNOLOGIE FORENSI

Riflessioni metodologiche e giuridiche

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464303
pp. 43-60 (gennaio 2022)

Questioni aperte sull'acquisizione probatoria di dati informatici

SILVIA GOLIN[1]

1. L'invasione del mondo digitale nella realtà analogica

L'inarrestabile processo di digitalizzazione che coinvolge la società moderna costringe il giurista ad un particolare sforzo interpretativo nell'adeguamento delle norme processuali al mondo digitale che presenta caratteristiche assolutamente peculiari rispetto al mondo fenomenico.

Le difficoltà sono evidenti considerato che in precedenza il processo penale ha sempre vissuto di elementi materiali, tangibili, come ad esempio la testimonianza resa in dibattimento, l'esame del reperto sequestrato, la visione delle fotografie o delle videoriprese, beni che si potevano percepire direttamente, toccare, guardare, analizzare.

Balza agli occhi la profonda differenza con il dato digitale che ha caratteristiche di immaterialità, fragilità, aterritorialità[2].

Lo sguardo del giurista passa, quindi, dalla realtà fenomenica all'analisi e comprensione dei dati codificati digitali che solo a seguito di decodifica diventano comprensibili all'uomo.

Inoltre, nella c.d. realtà digitale il contenuto rilevante per il processo (la prova costituita dal dato informatico) è sempre più indipendente dal suo contenitore (il dispositivo elettronico in cui sono memorizzati i dati informatici rilevanti o per mezzo del quale si accede ai dati rilevanti che si trovano memorizzati altrove).

[1] Sostituto Procuratore della Repubblica in servizio alla Procura di Padova nominata con D.M. 19.10.2004, nonché Referente Informatico Distrettuale per il distretto di Venezia su nomina del C.S.M.

[2] L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato fra progresso scientifico e garanzie fondamentali*, Giuffrè, 2007, pp. 128 e ss.

È di tutta evidenza come le caratteristiche del dato digitale incidano sulla corretta acquisizione e conservazione del dato informatico che abbia rilevanza investigativa, al fine di acquisire una prova spendibile nel dibattimento penale.

Così, sin dagli anni ’80 negli Stati Uniti e in seguito in altri Paesi, l’attenzione degli operatori si catalizzava verso le tematiche della *computer forensics* e della *digital evidence*[3], fino a giungere, nel nostro ordinamento, all'adozione della legge n. 48 del 2008 attuativa della convenzione di Budapest del 23 novembre 2001 del Consiglio d’Europa che ha imposto – nell’acquisizione della c.d. prova digitale – l’adozione di cautele non tipizzate[4] che assicurino la conservazione e non alterazione del dato informatico, lasciando libero l’operatore di polizia giudiziaria e il magistrato inquirente nel determinare quale strumento tecnologico e quale strumento giuridico utilizzare.

Pertanto, l’acquisizione di una prova digitale nel corso delle indagini preliminari impone una duplice valutazione: la valutazione tecnica relativa a quale metodo scientifico adottare per la ricerca e l’estrazione di determinati dati da un dispositivo e la valutazione giuridica relativa a quale strumento giuridico utilizzare per acquisire quella prova nel processo penale.

La prima valutazione è evidentemente scientifica e concerne le modalità tecniche per la ricerca di un determinato file di interesse investigativo e, in caso positivo, alle tecniche di estrazione e copiatura del dato individuato. Si tratta di valutazione da concordare con personale tecnico competente.

La seconda valutazione riguarda la natura giuridica delle operazioni di ricerca, individuazione e copiatura di un dispositivo digitale in cui è

[3] F. M. Molinari, *Le attività investigative inerenti alla prova di natura digitale,* Cassazione Penale, 2013, pag. 1259B.

[4] Principio ribadito da Cass. Sez. 3 n. 3744 del 28/05/2015 Rv. 265180: «in tema di perquisizione di sistema informatico o telematico, sia l’art. 247, comma 1-bis, che l’art. 260, comma secondo, cod. proc. pen., si limitano a richiedere l’adozione di misure tecniche e di procedure idonee a garantire la conservazione dei dati informatici originali e la conformità ed immodificabilità delle copie estratte per evitare il rischio di alterazioni, senza imporre misure e procedure tipizzate. (Fattispecie in cui la Corte ha rigettato il motivo di ricorso genericamente fondato sulla mancata indicazione, da parte del consulente tecnico del PM, del cd. valore “hash” dei files ottenuti dai supporti informatici, in assenza peraltro di contestazione circa la mancata corrispondenza fra le copie estratte e i dati originariamente presenti sui supporti informatici nella disponibilità dell’imputato)».

contenuto il dato rilevante ai fini probatori[5] al fine di utilizzare il corretto strumento giuridico per l'ingresso della prova nel procedimento penale.

Nel nostro ordinamento, in attuazione dei principi affermati nella Convenzione di Budapest, è stato introdotto il comma 1 bis dell'art. 247 c.p.p. che consente la perquisizione informatica di un dispositivo elettronico quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, mediante l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Tuttavia, il codice di rito nulla prevede nel caso in cui, per varie ragioni, il dispositivo elettronico non fosse stato oggetto di perquisizione, ma sottoposto a sequestro senza prima averne esaminato il contenuto.

Secondo le norme del codice di procedura penale, si prospettano diverse possibilità: copiatura forense e successiva analisi dei dati contenuti nel dispositivo sequestrato da parte di polizia giudiziaria delegata, oppure copiatura e analisi effettuata dal consulente nominato dal pubblico ministero con accertamento tecnico irripetibile ai sensi dell'articolo 360 c.p.p. o con accertamento tecnico ripetibile ai sensi dell'articolo 359 c.p.p.

La scelta di quale strumento giuridico adottare coinvolge anche l'opportunità o meno di dissequestrare i dispositivi dopo le operazioni di copiatura. Lo svincolo dei reperti potrebbe infatti pregiudicare la corretta formazione della prova in dibattimento, sottraendo il materiale ad un eventuale esame da parte di un perito nominato dal giudice, in presenza di contestazioni sulle operazioni di estrazione forense, ad esempio, in relazione al software utilizzato o alle procedure seguite.

Inoltre, si è accennato come il progresso tecnologico sta spostando sempre di più i dati dal contenitore collocato vicino all'utente (il pc, il cellulare, il server di una società) a luoghi virtuali di immediato accesso per l'utente ma collocati altrove (si pensi agli spazi virtuali in *cloud* con server collocati in paesi UE, extra UE, ma anche al sorgere spazi virtuali collocati fuori dallo spazio terrestre in satelliti in orbita[6]).

[5] E. Lorenzetto, *Utilizzabilità dei dati informatici incorporati su computer in sequestro; dal contenitore al contenuto passando per la copia*, Cassazione penale, 2010 p. 1522 ss.; P. Tonini, *Documento informatico e giusto processo, Dir. Pen. e Proc., 2009*, p. 404.

[6] Esempi di *cloud* nello spazio: SpaceX (la società di Elon Musk) e SES in partnership con Microsoft hanno creato Azure Space per dar vita a servizi di connettività satellitare sicuri e

I milioni di *gigabyte* condivisi nei social network, in servizi come *Facebook*, hanno fatto sorgere la necessità di costruire data center dove allocare e rendere fruibili dati nella continua e costante necessità di fornire una velocissima e continua interconnessione di utenti[7].

Ecco lo scarto che si è creato tra informazione e il luogo dove quell'informazione risulta collocata, pur essendo l'informazione immediatamente accessibile all'utente[8].

Questo progresso inarrestabile costituisce un evidente enorme limite per l'inquirente, con evidenti problemi di cooperazione giudiziaria con tra Stati quando il dato sia memorizzato in server posti al di fuori del territorio italiano.

Per rispondere alle domande sopra riportate appare necessario interrogarsi in primo luogo sulle caratteristiche tecniche della prova digitale, successivamente percorrere la disciplina legislativa vigente, analizzare il panorama giurisprudenziale e – considerato che il nostro ordinamento non è vincolato al precedente giurisprudenziale di *common law* – verificare se le conclusioni cui giunge la giurisprudenza siano coerenti con i principi giuridici del nostro ordinamento[9].

accessibili da qualunque parte del mondo. Si tratta di un cloud integrato con satelliti per rispondere alle esigenze della comunità spaziale e per connettere pressoché ogni dispositivo ovunque si trovi. Ancora, la start-up Cloud Constellation Corporation e Telespazio (joint venture Leonardo-Thales) hanno costituito nel 2019 una impresa per fornire un servizio basato su una costellazione di dieci satelliti in orbita bassa con l'obiettivo di proteggere le risorse costituite da banche dati di alto valore, di importanza critica per attività altamente sensibili, fornendo l'archiviazione di tali dati nello spazio e servizi di rete globali gestiti in massima sicurezza.

[7] Facebook genera in questi mesi quattro petabyte di dati al giorno (un petabyte è circaun milione di gigabyte). Tutti questi dati sono memorizzati in quello che viene chiamato The Hive (l'alveare), che contiene circa 300 petabyte di dati. Per poter allocare tali quantità di informazioni sono sorti i data center, enormi stabili che hanno un'immensa memoria di dati con una grande capacità di archiviazione. Curiosi gli investimenti nel data center di Facebook sito a Luleå, cittadina della Lapponia svedese, popolata da 45 mila abitanti. Lo stabile di 300 metri per 100 è posizionato nel bel mezzo della vegetazione tra abeti e betulle e sfrutta la naturale necessità di raffreddamento collocando i server in un luogo in cui le temperature d'inverno raggiungono i -20 gradi, mentre d'estate non arrivano mai sopra i 20°C. In questo modo la struttura può raffreddare le proprie macchine a costo zero. Cfr. https://www.ultimavoce.it/data-center-facebook-svezia/.

[8] Per i riflessi culturali e sociali della rivoluzione digitale si rimanda all'interessante The Game di Alessandro Baricco (Einaudi, 2018).

[9] F.M. MOLINARI, *cit.,* p. 1259B.

2. Conseguenze della Legge 48/2008 di attuazione della convenzione di Budapest

Come noto, la convenzione di Budapest[10], recepita in Italia con L. 48/2008 ha introdotto numerose modifiche nel codice di procedura penale e nel codice penale, dettando regole cautelari nell'acquisizione della prova digitale, indicando le esigenze che debbono essere soddisfatte, ma lasciando l'operatore libero nell'individuazione degli strumenti tecnici da utilizzare[11].

Si rimanda alla lettura degli articoli del codice di procedura penale, novellati dalla L. 48/2008, in tema di ispezioni (art. 244 c.p.p.[12]) e perquisizioni (art. 247 c.p.p.[13]), osservando come la regola cautelare di acquisizione della prova sia sempre la conservazione dell'integrità del dato informatico e la sua non alterazione.

Rilevato che l'adozione di misure tecniche tese alla conservazione del dato ed alla sua non alterazione è una scelta tecnologica, è necessario interrogarsi sulle conseguenze della violazione delle regole cautelari introdotte con la convenzione di Budapest[14].

Nessuna norma della Convenzione di Budapest, né la normativa introdotta con la legge 48/2008 indica le conseguenze della violazione delle suddette regole cautelari.

Rifacendosi ai principi generali, si conviene che la violazione non può essere ricondotta ad una nullità, non essendo stato introdotto alcun richiamo all'art. 178 c.p.p. e vigendo il principio di tassatività delle nullità.

[10] La Convenzione di Budapest del 23.11.2001 del Consiglio d'Europa sulla criminalità informatica è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche. Importante notare che tra i firmatari troviamo sia stati membri UE che stati non membri UE; sul tema, tra gli altri: L. PICOTTI, *Ratifica alla Convenzione cybercrime e nuovi strumenti di contrasto alla criminalità informatica e non solo*, in *Diritto dell'internet n. 5, 2008*; C. MAIOLI e E. SANGUEDOLCE, *I nuovi mezzi di ricerca della prova fra informatica forense e L. 48/2008*, Altalex, 7/5/2012.

[11] Principio ribadito da Cass. Sez. 3 n. 3744 del 28/05/2015 Rv. 265180, cit.

[12] Art. 244 comma 2 c.p.p.: L'A.G. può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica anche in relazione a sistemi informatici o telematici, adottando le misure tecniche dirette ad assicurare la conservazione dei dati e ad impedirne l'alterazione.

[13] Art. 247 comma 1 bis c.p.p.: Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

[14] F. CAJANI, *Il vaglio dibattimentale della digital evidence,* Archivio Penale, 2013, 3, p. 837 ss.

Si potrebbe affermare che l'acquisizione della copia forense possa essere dichiarata inutilizzabile nell'ordinanza di ammissione delle prove ex art. 190 c.p.p., lamentando la violazione di un divieto di legge. Tuttavia, la normativa introdotta dalla L. 48/2008 non stabilisce divieti di utilizzabilità, ma sancisce le esigenze cautelari da adottare per non alterare il dato e conservarne l'integrità.

L'inutilizzabilità di una prova presuppone la presenza di una prova vietata per la sua intrinseca illegittimità oggettiva ovvero per effetto di un procedimento acquisitivo la cui manifesta illegittimità lo pone completamente al di fuori del sistema processuale.

Pertanto, l'inutilizzabilità non pare la soluzione giuridica corretta, appunto per la generica formulazione della norma che non stabilisce dei divieti, ma generiche cautele e rimette la scelta all'inquirente/operatore di polizia giudiziaria/consulente su quali regole tecniche seguire per effettuare correttamente la copiatura forense.

È evidente che, vigendo nel nostro ordinamento il principio del libero convincimento del giudice nella valutazione delle prove, la valutazione è rimessa al Giudicante.

A tali conclusioni è pervenuta la Corte di Cassazione Sez. 2 con la sentenza n. 29061 del 01/07/2015[15] in cui ribadisce che la mancata adozione di modalità (tese a non alterare il dato e a preservarne l'integrità) non comporta l'inutilizzabilità dei risultati probatori acquisiti, ma la necessità di valutare, in concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti.

Guardando al mondo fenomenico facciamo l'esempio della manipolazione erronea dell'arma del delitto. Un errore nell'acquisizione e nella conservazione del reperto, toccato a mani nude dall'operatore di polizia giudiziaria o da un terzo estraneo al delitto che imprima accidentalmente le sue impronte, non inficia automaticamente la prova in dibattimento. Nell'esempio citato, il rilievo delle impronte esalterà anche le impronte del terzo estraneo oltre che l'impronta del presunto

[15] Si cita la massima ella Corte di Cassazione Sez. 2 con la sentenza n. 29061 del 01/07/2015: «L' estrazione di dati archiviati in un computer non costituisce accertamento tecnico irripetibile anche dopo l'entrata in vigore della legge 18 marzo 2008, n. 48, che ha introdotto unicamente l'obbligo di adottare modalità acquisitive idonee a garantire la conformità dei dati informatici acquisiti a quelli originali; ne deriva che la mancata adozione di tali modalità non comporta l'inutilizzabilità dei risultati probatori acquisiti, ma la necessità di valutare, in concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti». (In motivazione, la Suprema Corte ha chiarito che i dati di carattere informatico rientrano in ogni caso nel novero delle prove documentali).

assassino e/o della vittima. L'analisi delle impronte esaltate (procedimento valutativo), unita all'annotazione in cui viene dato atto della manipolazione del coltello senza cautele ed alla comparazione del rilievo con l'impronta del terzo, convincerà – se del caso – il Giudicante circa l'individuazione dell'omicida, escludendo l'inesperto operatore di polizia giudiziaria o il terzo estraneo che avessero toccato l'arma del delitto. Tale prova non appare per nulla inficiata da nullità, tanto meno da inutilizzabilità. Nonostante siano state utilizzate modalità errate e non tese alla conservazione e alla non alterazione del reperto, il vaglio dibattimentale restituirà il giusto valore alla prova raccolta.

Analogamente in relazione alla prova digitale: il principio del libero convincimento del giudice consentirà al Giudicante di motivare la rilevanza probatoria del dato digitale estratto nelle operazioni di copiatura forense anche in violazione delle regole cautelari di conservazione dell'integrità del dato informatico e della sua non alterazione.

3. La copia forense

Per sua propria caratteristica, il dato informatico di un *device* comprende sia l'insieme di file visibili all'utente (documenti, fotografie, messaggistica, note, ecc.), che tutta una serie di metadati relativi alle proprietà e caratteristiche dei file, delle applicazioni, delle connessioni, dati spesso utilissimi dal punto di vista investigativo.

Una fotografia digitale non contiene soltanto l'immagine che vediamo, ma conserva i metadati relativi al giorno ed ora in cui è stata scattata, i dati del dispositivo utilizzato per scattare quella fotografia, le coordinate geografiche del luogo ove è stata scattata. Analogamente, una email non è composta solo dal contenuto visibile (che scriviamo o scriviamo), ma contiene i metadati relativi a mittente, ip del percorso nei differenti server che hanno gestito la trasmissione della mail (c.d. header).

L'informatica ci insegna che i dati digitali, per loro caratteristica, possono essere copiati 'bit to bit', cosicché si può ottenere una copia identica dell'originale (c.d. copia-clone o bitstream): tant'è che dal punto di vista informatico la copia originale e la copia-clone non sono differenziabili.

L'operazione di copiatura forense consente di avere a disposizione l'esatta copiatura di tutto il contenuto di un determinato dispositivo

elettronico, quindi la copiatura di tutti i dati, anche quelli non visibili o cancellati, duplicando tutti i bit ivi contenuti nel dispositivo in questione.

Come è noto, la *computer forensics* nel corso degli anni ha individuato una serie di strumenti volti ad assicurare l'integrità del dato informatico, di modo che nelle operazioni di copiatura si potesse avere la garanzia di integrità del dato e della sua non alterazione. Sul punto si sono consolidate diverse prassi riconosciute a livello internazionale[16].

È evidente che la copiatura forense sia una prova scientifica, la cui caratteristica essenziale risiede nel momento acquisitivo caratterizzato dall'ausilio di conoscenze e metodologie attinenti a sapere scientifico e tecnico[17] .

Solitamente si procede alla copiatura bit to bit del contenuto di un dispositivo elettronico per poi proseguire nelle operazioni di ricerca di dati informatici rilevanti lavorando sulla copia clone così da non alterare i dati originali.

Ci si è chiesti quale sia la natura giuridica dell'operazione di copiatura del contenuto di un dispositivo elettronico.

La giurisprudenza di legittimità ha spesso ripetuto che la copiatura di dati informatici è un accertamento ripetibile per un numero infinito di volte, escludendo la necessità che si debba procedere nel contraddittorio della difesa.

In sintesi, il panorama giurisprudenziale di legittimità non ritiene necessaria la presenza dell'indagato alle operazioni di copiatura, perché non considera le operazioni di copiatura forense quale accertamento tecnico irripetibile, nemmeno dopo l'entrata in vigore della L. 48/2008.

Si precisa che la giurisprudenza di legittimità analizzata si occupa di estrazione forense del contenuto di un hard disk di un pc. Attualmente non risultano depositate sentenze di legittimità che riguardino la copiatura di dispositivi c.d. mobili (come smarphone o tablet) né di *cloud.*

[16] Tra le varie possibilità offerte dall'informatica, si indica il *write blocker*, come uno strumento hardware che garantisce la sola lettura del supporto oggetto di investigazione, impedendo qualsivoglia scrittura, anche inavvertita, su di esso. Inoltre, il calcolo del valore di *hash è* una funzione univoca che calcola mediante un algoritmo il valore di un file in un numero prefissato di bit. Ad ogni *file* corrisponde infatti un solo determinato valore di hash che lo contraddistingue; se il file viene modificato, ricalcolando l'hash, il valore sarà diverso. Inoltre, come detto, l'hash è univoco, nel senso che non è possibile da esso ricostruire il file sottostante, il che garantisce un ottimo livello di sicurezza ed integrità del dato analizzato. Possiamo dire che questa è una buona prassi informatica per far sì che si possa estrarre il contenuto di un determinato dispositivo, che sia un personal computer, lo smartphone, un tablet, un qualunque device esterno.

[17] O. DOMINIONI, *La prova penale scientifica,* Giuffrè, 2005.

Nella sentenza n. 29061 del 01/07/2015 della seconda sezione (analoga motivazione nella sentenza sempre della seconda sezione n. 24998 del 04/06/2015), la Cassazione[18] precisa che i dati di carattere informatico rientrano nel novero delle prove documentali. Tuttavia, la sentenza non si addentra in precise motivazioni nell'affermare che la copiatura sia attività non irripetibile, indicando l'assunto secondo il quale la copiatura sia un'operazione meramente meccanica riproducibile per un numero indefinito di volte (argomentazione valida, si badi bene, solamente finché il dispositivo in questione rimanga in sequestro); la sentenza sul punto motivazionale rinvia al precedente della prima Sezione, sentenza n. 23035 del 30/04/2009.

Nella motivazione della citata sentenza n. 23035 del 30/04/2009 i giudici di legittimità ritengono che la copiatura sia un accertamento di fatto che consiste nello stabilire se i dati informatici siano o meno stati alterati e in caso affermativo, stabilire in cosa consista l'alterazione e, quindi, se il dato informatico possa o meno continuare ad essere utilizzabile nonostante l'alterazione. I giudici precisano che tale accertamento è una prova scientifica.

È necessario precisare che la sentenza n. 23035 tratta il ricorso in Cassazione sul riesame cautelare dell'ordinanza del Tribunale di Napoli di conferma dell'ordinanza di custodia cautelare in carcere per il reato di cui all'art. 416 bis c.p., per avere partecipato all'associazione per delinquere di stampo mafioso detta 'clan dei Casalesi'. Si tratta di una sentenza di legittimità sul giudicato cautelare, che non affronta pertanto alcuna questione giuridica legata alla formazione e valutazione della prova in dibattimento.

Nel caso esaminato, il ricorrente lamentava la violazione dell'art.360 c.p.p. assumendo l'inutilizzabilità dei dati estratti dal computer del coindagato, che assertivamente consistevano invece in operazioni irripetibili, per le quali avrebbero dovuto dare avviso alla difesa.

Il Collegio rigettava il motivo di ricorso (sull'inutilizzabilità dei dati estratti dal computer dell'indagato, dai quali emergevano le prove dell'appartenenza all'associazione per delinquere di stampo mafioso) ritenendolo assolutamente generico. Secondo i giudici, l'affermazione che l'operazione di estrazione degli appunti del coindagato archiviati

[18] Anche in tale sentenza la Corte si richiama alle precedenti pronunce: Cass. Sez. 1^, Sentenza n. 23035 del 30/04/2009 dep. 04/06/2009 Rv. 24445. Che l'estrazione dei dati archiviati in un computer non sia un accertamento tecnico irripetibile si legge anche in Cass. Sez. 2, Sentenza n. 8607 del 19/02/2015.

nel computer costituisse attività irripetibile, è stata considerata priva d'ogni riferimento che consenta di apprezzarne la plausibilità. Mentre, osservano, è dato di comune esperienza che la stampa di un qualsiasi documento redatto su supporto informatico sia operazione meramente meccanica: riproducibile, teoricamente, all'infinito (cfr. nello stesso senso, Cass. Sez. I, n. 12472 del 11.3.2009; e ancora Cass. n. 11503 del 25.2.2009, Cass. 14511/20019). I Supremi Giudici inoltre hanno precisato che la sanzione della inutilizzabilità espressamente prevista dall'art. 360 c.p.p., comma 5, riguardando il dibattimento, è evidentemente limitata all'ipotesi in cui il pubblico ministero, malgrado l'espressa riserva di promuovere incidente probatorio formulata nel contesto di un conferimento incarico ai sensi dell'art. 360 c.p.p. e pur potendo gli accertamenti irripetibili essere differiti, ha ugualmente disposto di procedere a detti accertamenti.

Altra sentenza di legittimità che si è occupata incidentalmente della natura giuridica della copia forense è la n.11503 del 25/02/2009. In tale pronuncia gli ermellini osservano che non dà luogo ad accertamento tecnico irripetibile la lettura dell'hard disk di un computer sequestrato, trattandosi di attività di polizia giudiziaria volta, anche con urgenza, all'assicurazione delle fonti di prova[19].

Si sottolinea che anche tale pronuncia afferisce non al procedimento di merito ma al giudicato cautelare, non entrando di conseguenza nelle valutazioni giuridiche relative alla formazione della prova in dibattimento.

A ben vedere, la giurisprudenza citata non si è occupata della natura giuridica della copia forense, ma si è interrogata sulla lesione o meno del diritto della difesa per la mancata partecipazione alle operazioni di copiatura, sul presupposto che si tratti di operazione meccanica ripetibile per un numero indefinito di volte.

Si noti bene che tale assunto è condivisibile laddove il dispositivo permanga in sequestro. Se il dispositivo venisse dissequestrato, l'operazione di copiatura non sarebbe più ripetibile un numero indefinito di volte.

Pertanto, in tale sede, ci si chiede se la copiatura bit to bit di un contenuto informatico costituisca, dal punto di vista giuridico procedurale, un accertamento.

[19] Nel caso di specie, *l'hard disk* era stato rimosso dal pc sequestrato e letto senza la presenza dei difensori, né di loro consulenti, né di avviso a presenziare alle operazioni.

Secondo chi scrive, una volta compresa la natura del dato informatico e la natura della copia-clone, non si può non convenire che l'attività di copiatura altro non sia che un rilievo e non un accertamento tecnico.

Secondo i principi generali, il rilievo tecnico si differenza dall'accertamento tecnico vero e proprio, in quanto si esaurisce in una mera attività di osservazione e di descrizione senza implicare alcuna valutazione critica del dato raccolto, e perciò può essere eseguito dall'autorità di polizia, mentre l'accertamento tecnico non può mai eseguirsi senza l'osservanza delle garanzie difensive (cfr. Cass. Sez. 2, Sentenza n. 2611 del 18/01/1993)[20].

Effettuare una copia-clone del contenuto di un dispositivo elettronico è rilevare l'esatto contenuto di quel dispositivo nel momento in cui avvengono le operazioni di copiatura.

Analizzare il contenuto di quel dispositivo è, invece, attività valutativa.

La maggior parte dei tecnici informatici nulla obietta sulla copiatura digitale del contenuto di un hard disk in assenza di garanzie difensive, mentre suggerisce di coinvolgere la difesa nella attività di copiatura del contenuto di uno smartphone o un tablet.

Tale conclusione è legata alle differenti caratteristiche tecniche dei dispositivi c.d. fissi rispetto a quelli c.d. mobili. Infatti, i tecnici riferiscono che per copiare il contenuto di un PC[21] è possibile farlo con dispositivo spento, mentre per la copiatura dei dati di uno smartphone o tablet è necessario che il dispositivo sia acceso.

Si tratta, a ben vedere, di una differente modalità di esecuzione delle operazioni di copiatura legata alle differenti caratteristiche tecniche di hard disk e dispositivi c.d. mobili, quest'ultimi con caratteristiche costruttive diverse, legate principalmente al minore spazio di memoria che devono avere i dispositivi portatili, sempre più piccoli e leggeri.

[20] Ancora, sui rilievi tecnici si cita la Sentenza della Cass. Sez. 1, n.18246 del 25/02/2015: «Il prelievo del d.n.a. della persona, attraverso il sequestro di oggetti contenenti residui organici alla stessa attribuibili, è qualificabile come rilievo tecnico e, in quanto tale, è delegabile ai sensi dell'art. 370 cod. proc. pen., senza la necessità per il suo espletamento dell'osservanza delle garanzie difensive, che vanno, invece, assicurate nella distinta e successiva operazione di identificazione del d.n.a. della persona, attraverso l'utilizzo del materiale genetico repertato, la quale costituisce accertamento tecnico, da qualificarsi ripetibile o meno in base ad una valutazione tecnico-fattuale in ordine alla possibile conservazione dei reperti».

[21] Ci si riferisce al PC di vecchia generazione con hard disk perché questo non vale per gli innovativi SSD – Solid State Drive. Gli SSD presentano una tecnologia che utilizza le memorie flash rispetto ai classici dischi rigidi. Non hanno parti meccaniche.

La conseguenza è che quando la polizia giudiziaria sequestra un pc lo spegne e le operazioni di copiatura possono avvenire a dispositivo spento, che rimane nella medesima condizione del momento in cui è stato sequestrato e non subirà alcuna modifica dei dati rispetto al momento del sequestro (ovviamente se il personale adotterà le cautele ed effettuerà le operazioni secondo le buone prassi condivise).

Diversamente, in caso di smartphone, tablet o altro dispositivo mobile per la copiatura dei dati è necessario che il device sia acceso. Di conseguenza, la polizia giudiziaria spegnerà il dispositivo al momento del sequestro e lo riaccenderà in modalità aereo (quindi scollegato dalla rete internet) per le operazioni di copiatura. Operazione, quella di accensione in un momento successivo al sequestro, che potrebbe influire sul contenuto del dispositivo per l'attivarsi di una serie di caratteristiche costruttive dello stesso. Vari tecnici rappresentano, ad esempio, che al momento dell'accensione del dispositivo varia la data e l'ora di ultima accensione, con ciò modificando (seppur di poco) il contenuto totale del dispositivo sequestrato[22]. Così come possono variare una serie di altri piccoli elementi, come ad esempio l'eliminazione automatica delle fotografie presenti nel cestino[23], che giacciono in un limbo prima di essere eliminate automaticamente dal sistema al trascorrere di un determinato intervallo temporale.

Il dispositivo mobile riacceso e non connesso ad alcuna rete internet non aggiornerà ulteriori dati delle applicazioni preservando il contenuto.

È questa la motivazione per la quale spesso le operazioni di copiatura forense sono eseguite seguendo le disposizioni di cui all'art. 360 c.p.p., con il contraddittorio delle parti e la possibilità per gli indagati di esprimere riserva di incidente probatorio. A rigore, infatti, l'accensione del dispositivo per le operazioni di copiatura modifica il contenuto dell'intero device rispetto a quello che aveva nel momento in cui era stato sottoposto a sequestro.

A parere della scrivente, tale caratteristica (ovvero le piccole modifiche legate all'accensione del dispositivo mobile) non incide sulla natura

[22] Di conseguenza, il calcolo del valore di hash dell'intero contenuto di un dispositivo sarà diverso se effettuato in due momenti diversi, proprio per la variazione di alcuni dati, come quelli indicati.

[23] L'esempio si riferisce alla giacenza automatica delle fotografie eliminate dai dispositivi Iphone IOS ed eliminazione definitiva al trentesimo giorno https://support.apple.com/it-it/HT205856.

giuridica delle operazioni di copiatura del dato informatico, che ricordiamo essere la creazione di un clone rispetto all'originale. Si tratta di una caratteristica di modificabilità dell'intero contenuto del device in questione, caratteristica legata alle caratteristiche costruttive del dispositivo nonché alle modalità tecniche attraverso le quali l'operazione di copiatura è realizzata.

Si ritiene che la circostanza in base alla quale alcune parti dell'intero contenuto di un device di cui si effettua copia forense si possano modificare non incida sui paradigmi di non alterazione e immodificabilità del dato informatico richiesti dalla Convenzione di Budapest, paradigmi che si rivolgono allo specifico dato informatico (il file di interesse) che costituisce la prova rilevante trovata analizzando tutta la massa di dati contenuti nella copia forense. È quello il dato che si deve conservare nelle sue caratteristiche originali e che non si deve alterare, non l'intera massa dei dati analizzati.

Sarebbe pertanto opportuno chiedere al consulente di indicare, in relazione allo specifico tipo e modello di device da analizzare, quali siano i contenuti oggetto di modifica al momento di accensione del dispositivo in epoca successiva al sequestro, oltre ai dati relativi all'ora di ultima accensione ed alla eventuale perdita di fotografie.

Conosciute tali caratteristiche, sarebbe più semplice per l'interprete comprendere se e in quale maniera queste piccole modifiche (legate appunto al momento dell'accensione del dispositivo) possano incidere nella ricerca delle prove per il reato per cui si procede, o possano compromettere la valutazione della prova perché violano (seppur in minima parte) la regola cautelare di non alterazione e di conservazione dell'integrità del dato.

Si tratta di questione che sarà valutata liberamente dal giudice, il quale dovrà verificare se i dati informatici estratti da quel dispositivo mobile e ritenuti rilevanti ai fini probatori siano o meno stati compromessi o alterati dalle operazioni di copiatura.

È interessante conoscere quindi, in base alle caratteristiche tecniche del device, se le operazioni di accensione vadano a modificare alcuni determinati contenuti individuabili a priori; e altresì conoscere se tali modifiche incidano sui dati che nel concreto vi è interesse a cercare (ad esempio si cercano nel concreto determinati contenuti di quel *device* che rimarrebbero comunque immutati con la successiva accensione del dispositivo finalizzata alla copiatura del suo contenuto). Ciò a ben vedere non implicherebbe la partecipazione della difesa alle operazioni.

Si ricorda infatti che la partecipazione della difesa ai sensi dell'art. 360 c.p.p. è legata alla irripetibilità delle operazioni. È evidente che fino a quando il *device* sia mantenuto in sequestro l'operazione sia ripetibile in un numero infinito di volte. Chiaramente, diverse copiature del medesimo dispositivo mobile in giorni diversi darebbero luogo a copie diverse, posto che nei termini sopra indicati il dispositivo subisce alcune piccole modifiche a causa dell'accensione. Tuttavia, l'analisi delle diverse copie forensi così ottenute consentirebbe sempre di trovare quel determinato file di interesse investigativo.

Se, invece, l'interesse investigativo fosse rivolto ad uno di quei contenuti che si modificano dal momento dello spegnimento alla successiva riaccensione del dispositivo, è evidente che le operazioni di copiatura dovrebbero essere fatte immediatamente, sul posto, con il dispositivo acceso e mai spento.

Si tratta di un'evidente scelta investigativa rimessa all'attenzione del pubblico ministero e della polizia giudiziaria, legata alla prova che si sta cercando e quindi alle specificità del caso concreto.

Riprendendo la questione relativa alla natura giuridica delle operazioni di copiatura forense di un dispositivo elettronico, si ricorda che il rilievo tecnico si differenza dall'accertamento tecnico, in quanto si esaurisce in una mera attività di osservazione e di descrizione senza implicare alcuna valutazione critica del dato raccolto. Nel caso di copiatura forense del contenuto di un pc, di smartphone, tablet o altro dispositivo elettronico, l'attività di copiatura bit to bit è il clone del contenuto di quel dispositivo al momento in cui si eseguono le operazioni. Come detto contenuto originale e contenuto copiato in *bitstream* sono identici, tant'è che non è possibile distinguerli.

La copiatura forense potrebbe qualificarsi come attività di rilievo tecnico. Si tratta di un rilievo anche se sia intervenuta una naturale modifica del bene.

Facciamo un esempio legato al mondo fenomenico: in un'abitazione si rinviene un corpo esamine, circondato da una pozza di sangue, con accanto un coltello e molte impronte di scarpe intrise di sangue. Al fine di far intervenire personale altamente specializzato, viene rimosso il corpo (che sarà sottoposto ad autopsia, attività valutativa e non di mera osservazione) ma si decide di non toccare il coltello, le macchie di sangue e gli altri oggetti presenti, sequestrando l'intera abitazione.

Quando il giorno seguente, polizia giudiziaria e personale tecnico delegato tornano nel luogo dei fatti la situazione è mutata: il sangue si è rappreso, ha cambiato colore, perché lo scorrere delle ore, l'ossida-

zione ed altri processi biologici hanno prodotto reazioni chimiche che hanno variato il materiale, sia nella sua forma visiva che biologica. Ma nessun operatore penserebbe che l'acquisizione delle fotografie che rappresentano la scena del crimine (tra l'altro senza clonarla) in un momento successivo al sequestro sia un accertamento e non un rilievo.

Medesime considerazioni per il coltello sequestrato e riposto in un sacchetto di plastica. Il sequestro del coltello è necessario per compiere dei rilievi finalizzati all'estrazione di dati utili (come la rilevazione di impronte). Quando esso sarà esaminato per verificare la presenza di impronte si compiranno rilievi e non accertamenti, anche se il sangue sul coltello sarà diverso dal modo in cui si presentava al momento del sequestro ed anche se si compiranno operazioni che andranno a modificare l'aspetto di quel coltello. Così come l'attività di acquisizione del campione di sangue è pacificamente attività di rilievo e non valutativa. L'attività valutativa è la analisi di quel sangue.

La rilevazione delle impronte altro non è che la copiatura della traccia biologica lasciata da mano umana sul reperto.

La copiatura forense di un dispositivo elettronico altro non è che il rilievo (la fotografia) del suo contenuto nel preciso momento in cui sono poste in essere le operazioni di copiatura.

In particolare, la copiatura forense di un dispositivo mobile, il cui contenuto, come detto, sarà lievemente diverso nel contenuto rispetto a quello che sarebbe stato se la copiatura fosse avvenuta il giorno del sequestro, è il rilievo del contenuto di quel device nel momento in cui sono effettuate le operazioni di copiatura.

La differente natura accordata ha un importante riflesso: i rilievi (e non gli accertamenti) entrano nel fascicolo per il dibattimento. Anche la copia forense effettuata ai sensi dell'art. 360 c.p.p. entra nel fascicolo per il dibattimento, tuttavia in questo caso le parti hanno facoltà di chiedere l'incidente probatorio.

È evidente che la scelta dell'organo inquirente sarà intimamente legata alla necessità o meno di procedere nel segreto istruttorio oppure coinvolgendo la difesa, qualora si opti per la procedura di cui all'art. 360 c.p.p. Tale scelta è legata alle peculiarità investigative del caso concreto.

In conclusione, a parere della scrivente, la copiatura forense costituisce attività di rilievo tecnico del contenuto di un dispositivo elettronico nel momento in cui viene effettuata.

La successiva attività di analisi della copia forense estratta, consistente nella ricerca dei dati di interesse investigativo e, in caso positivo,

dell'analisi del loro contenuto e dei relativi metadati, è attività valutativa.

4. Il domicilio informatico

Dottrina e giurisprudenza anche internazionali si chiedono se il domicilio informatico sia un luogo, seppur virtuale, al quale riconoscere la tutela della *privacy* delle informazioni ivi memorizzate, ma anche la tutela di un diritto costituzionale dell'individuo (art. 14 e 15 Cost., art. 8 CEDU, art. 7 della Carta dei diritti Fondamentali dell'Unione Europea)[24].

Tale principio che al momento non trova un esplicito riconoscimento costituzionale e legislativo[25]; pare riconosciuto indirettamente in alcune pronunce della giurisprudenza.

Vi è un diretto riferimento al domicilio informatico nel codice penale, dal momento in cui il legislatore ha introdotto il delitto di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. collocandolo nella sezione IV "Dei delitti contro l'inviolabilità del domicilio" all'interno del titolo XII "Dei delitti contro la persona" del libro II del c.p.

La giurisprudenza di legittimità ha affermato che l'art. 615-ter c.p. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti[26], ma offre una tutela più ampia che si concreta nello *jus excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello *jus excludendi* sia persona fisica, persona giuridica, privata o pubblica, o altro ente.

La giurisprudenza della Cassazione pare occuparsi indirettamente della tutela del domicilio informatico nei giudizi di legittimità sui riesami reali. In coerenza con la giurisprudenza in tema di sequestri

[24] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 104 ss.

[25] F. Iovene, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, Diritto Penale contemporaneo, 2014, 3, p. 329 ss.

[26] Con la sentenza n. 13057 del 31 marzo 2016 i giudici della Cassazione hanno precisato che costituisce un sistema informatico tutelato dall'art. 615 ter c.p. anche la casella di posta elettronica protetta da password.

probatori, i giudici di legittimità ritengono necessario un vincolo di pertinenzialità tra il reato per cui si procede e il dispositivo elettronico oggetto di sequestro.

Si cita sul punto la sentenza della Cassazione Sez. 6, n. 24617 del 24/02/2015 in cui gli ermellini hanno ritenuto illegittimo, per violazione del principio di proporzionalità ed adeguatezza, il sequestro a fini probatori di un sistema informatico, qual è un personal computer, che conduca, in difetto di specifiche ragioni, ad una indiscriminata apprensione di tutte le informazioni ivi contenute[27].

Nella sentenza n. 12107 del 18/11/2008 la III Sezione della Cassazione afferma che il giudice del riesame di un sequestro probatorio deve accertare l'esistenza del vincolo di pertinenzialità tra il reato ipotizzato ed i diversi beni o le diverse categorie di beni oggetto del provvedimento di sequestro. (Fattispecie nella quale è stato ritenuto illegittimo il sequestro di un intero server aziendale disposto in relazione al reato di turbata libertà dell'industria o del commercio).

In realtà, al fine di comprendere se vi sia una tutela costituzionale del domicilio informatico, occorre verificare se, e in che senso, un sistema possa essere considerato un luogo.

Al fine di evitare confusioni, difatti, bisogna preliminarmente distinguere tra il luogo ove è collocato il sistema informatico e l'ipotesi del sistema quale luogo o comunque proiezione di luogo (come nel cloud in cui il luogo è slegato dal dispositivo elettronico o sistema informatico attraverso al quale si accede allo spazio virtuale).

Nel primo caso sarebbe possibile arrivare ad una tutela del sistema attraverso un'interpretazione estensiva del concetto di privata dimora (si vedano recenti decisioni giurisprudenziali che ammettono l'operatività dell'art. 614 c.p. anche rispetto agli impianti industriali: Cass., sez. V, n. 85 del 17/10/90).

[27] Nella sentenza citata n. 24617/2015 si legge la seguente massima: «in tema di mezzi di ricerca della prova, costituisce sequestro probatorio l'acquisizione, mediante estrazione di copia informatica o riproduzione su supporto cartaceo, dei dati contenuti in un archivio informatico visionato nel corso di una perquisizione legittimamente eseguita ai sensi dell'art. 247 cod. proc. pen., quando il trattenimento della copia determina la sottrazione all'interessato della esclusiva disponibilità dell'informazione». (In motivazione, la Corte ha osservato che le disposizioni introdotte dalla legge 48/2008 riconoscono al "dato informatico", in quanto tale, la caratteristica di oggetto del sequestro, di modo che la restituzione, previo trattenimento di copia, del supporto fisico di memorizzazione, non comporta il venir meno del sequestro quando permane, sul piano del diritto sostanziale, una perdita autonomamente valutabile per il titolare del dato).

Nel secondo caso, ci si trova di fronte ad una situazione nuova, di vero e proprio spazio virtuale, totalmente slegato al territorio. Infatti, come accennato, gli informatici riferiscono che il *cloud* può avere la caratteristica della c.d. ridondanza ovvero i dati sono continuamente spostati da un server all'altro. Ci si chiede se tale caratteristica incida sulla possibilità di qualificare tali spazi virtuali quali luoghi e, quindi, estendere la tutela accordata al domicilio.

Ci si chiede, in conclusione, se la tutela accordata al domicilio (quello fenomenico, non virtuale) sia legata alla presenza di un luogo fisico o alla sostanza delle informazioni in esso contenute che essendo espressione della personalità dell'individuo meritino la tutela costituzionale accordata dall'art. 14 della costituzione.

E, quindi, se al *cloud* (come ad ogni altro spazio virtuale in uso esclusivo ad una persona fisica e contenente dati esplicativi della sua personalità) fosse riconosciuta la tutela del domicilio si dovrebbero applicare tutte le tutele riconosciute dalla costituzione e dalla legge, con la conseguenza che per accedere a quello spazio è necessario un decreto di perquisizione. E con conseguente illegittimità della possibilità di effettuare una c.d. perquisizione on line utilizzando degli strumenti, come ad esempio i captatori informatici, inoculati in segreto sul bersaglio da copiare regola che consente da remoto la copia dei file esistenti su un computer.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464304
pp. 61-82 (gennaio 2022)

La selezione dei dati informatici in ambito giudiziario: prassi e modalità operative

Michele Ferrazzano[1], Leonardo Summa[2]

1. Introduzione

L'utilità probatoria delle informazioni memorizzate all'interno dei supporti digitali di uso quotidiano è ormai questione di informatica forense non più trascurabile per gli operatori del diritto. La rapida diffusione di dispositivi capaci di immagazzinare, con estrema facilità, una quantità considerevole di dati ed informazioni potenzialmente rilevanti nel corso di un accertamento giudiziario contribuisce ad aumentare significativamente la quantità di dati che entrano in gioco in un procedimento giudiziario allorquando un dispositivo viene raccolto.

La produzione individuale di una sempre più crescente mole di informazioni native digitali, il rapido sviluppo di soluzioni tecnologiche differenti, l'aumento della complessità delle infrastrutture tecnologiche di utilizzo quotidiano, unitamente alle caratteristiche già note del dato informatico, richiedono un elevato grado di competenze tecniche specialistiche per l'acquisizione dei dati di interesse per un determinato accertamento.

Sin dal suo ingresso, il trattamento della prova informatica nell'ordinamento giuridico italiano ha sollevato questioni di estremo interesse, pratico e scientifico, alle quali la giurisprudenza ha tentato di offrire una soluzione adeguata alla tutela delle differenti esigenze processuali. In tale solco si collocano le recenti attestazioni della Corte di Cassazione in tema di sequestro di dati informatici, testimoni di una consapevolezza più matura degli interessi in gioco e del potenziale profondamente invasivo dei mezzi istruttori a vocazione informatica nel godi-

[1] Professore a contratto di Computer forensics, Università Statale di Milano, e di Informatica, Università degli Studi di Modena e Reggio Emilia; *Digital Forensics Expert*.
[2] Cultore della materia di Informatica Giuridica e Informatica forense, Università di Bologna.

mento di diritti umani fondamentali, quali il diritto ad avere un equo processo e i corollari da esso derivati.

La spinta innovativa degli orientamenti in commento risiede nella comprensione della funzione e del reale ruolo dell'acquisizione forense di un supporto informatico negli accertamenti tecnici in ambito giudiziario, individuando la copia forense quale mezzo per la selezione, estrazione e successivo sequestro del solo materiale pertinente e rilevante con la finalità probatoria perseguita.

Nel dare attuazione agli orientamenti richiamati, l'Autorità Giudiziaria procedente deve far ricorso alle competenze specialistiche degli esperti di informatica forense e avere a disposizione gli strumenti tecnici adeguati all'esecuzione di accertamenti a carattere informatico nel rispetto delle garanzie processuali riconosciute dall'ordinamento.

In quest'ottica le modalità di selezione dei dati informatici in ambito giudiziario assumono le vesti delle nuove questioni di informatica forense, con le quali confrontarsi quotidianamente alla ricerca di un difficile punto di equilibrio tra esigenze investigative e prerogative processuali da tutelare ancora da codificare.

2. Le evoluzioni interpretative giurisprudenziali nella selezione dei dati informatici

Dal riconoscimento dell'utilità di tali strumenti informatici per la conoscenza processuale avvenuto per mano del legislatore nella l. 48/2008, la dottrina e la giurisprudenza hanno tentato di dirimere le questioni sollevate dalla crescente necessità di far ricorso all'acquisizione di elementi probatori memorizzati all'interno di supporti informatici e di offrire un tracciato da seguire nella declinazione degli strumenti investigativi a vocazione informatica[3] presente nell'impianto processuale italiano.

Nel corso evolutivo dell'interpretazione giurisprudenziale alla fenomenologia informatico-giuridica si rinvengono attestazioni di indiscusso interesse e meritevoli di approfondimento, dalla lettura delle

[3] Si fa riferimento alle interpolazioni subite dalle disposizioni del codice di procedura penale in materia di ispezioni e rilievi tecnici (art. 244, c. 2 c.p.p.), l'esame di atti, documenti e corrispondenza presso banche (art. 248, c. 2 c.p.p.), i doveri di esibizione e consegna (art. 256, c. 1 c.p.p.), gli obblighi e le modalità di custodia (art. 259, c. 2 c.p.p.), i sigilli e i vincoli delle cose sequestrate (art. 260, c. 1 e 2 c.p.p.), l'acquisizione di plichi e corrispondenza (art. 353, c. 1 e 2 c.p.p.) e, infine, gli accertamenti urgenti e il sequestro (art. 354, c. 2 c.p.p.).

quali si evince una diversa maturità di comprensione delle questioni di informatica forense, vecchie e nuove.

Si pensi agli orientamenti che hanno riconosciuto una rilevanza autonoma dell'interesse ad impugnare il sequestro della copia forense effettuata su dispositivi informatici successivamente restituiti, nei quali si valorizza – perché ben compresa – la peculiare ontologia dei dati informatici superando la tradizionale inammissibilità per sopravvenuta carenza di interesse determinata dalla restituzione del bene sottoposto a sequestro[4].

In questa direzione, per quanto di interesse nella presente trattazione, si collocano le pronunce della Cassazione che affrontano il tema della legittimità del sequestro indiscriminato di dati informatici, nelle quali viene ribadito il necessario superamento del vaglio di proporzionalità e adeguatezza della misura ablativa adottata in relazione alle esigenze probatorie, non potendosi conferire un inutile sacrificio di diritti[5].

Nello svolgimento di accertamenti a carattere informatico, in qualsiasi cornice processuale essi trovino la loro ragion d'essere, il rispetto delle migliori pratiche adoperate a livello internazionale nel trattamento della prova digitale[6] è canone ormai consolidato e riconosciuto anche dalla giurisprudenza di legittimità[7].

[4] Il richiamo è alla sentenza Cass., Sez. U., n. 40963 del 20/07/2017, Rv. 270497, che ha affermato la legittimità dell'impugnazione dell'ordinanza di conferma del sequestro probatorio di supporti informatici, restituiti previa estrazione di copia forense dei dati contenuti, qualora sia dedotto l'interesse concreto e attuale all'esclusiva disponibilità dei dati, definendo l'estensione della sussistenza del sequestro sulla copia forense estratta dal dispositivo. In tal senso, e*x multis*, le pronunce *cfr.* Cass., Sez. 5, n. 13694 del 15/02/2019, Rv. 274975; Cass., Sez. 6, n. 13306 del 22/02/2018, Rv. 272904.

[5] Sempre in tema di violazione del principio di proporzionalità e adeguatezza del sequestro probatorio di supporti informatici, nel caso specifico eseguito nei confronti di dispositivi in uso ad un giornalista, si richiama la pronuncia della Cass., Sez. 6, n. 24617/2015, che ha dichiarato l'illegittimità del sequestro indiscriminato di un sistema informatico in difetto di specifiche ragioni per l'apprensione indiscriminata dei contenuti memorizzati all'interno. Di orientamento confermativo le più recenti pronunce Cass., Sez. 6, n. 9989/2018; Cass., Sez. 6, n. 43556/2019; Cass., Sez. 6, n. 3794/2020; Cass., Sez. 6, n. 30225/2020; Cass., Sez. 6, n. 10815/2021.

[6] In particolare, si richiamano le linee guida dello Standard ISO/IEC 27037 sul trattamento della prova informatica nelle prime fasi di identificazione, raccolta e acquisizione del reperto informatico, che prescrivono la documentazione di tutte le attività eseguite, gli strumenti utilizzati e gli eventi modificativi intervenuti sul reperto al fine di garantire l'integrità e l'autenticità del contenuto acquisito con il contenuto originale disponibile. Per maggiori approfondimenti, *cfr*. *Annex* B ISO/IEC 27037 su requisiti minimi di documentazione per il trasferimento di evidenze.

[7] Ci si riferisce alla pronuncia della Cass., sez. 5, n. 49016/2017 che, qualificando i dati informatici quale prova documentale ex. 234 c.p.p., ha sancito la necessarietà dell'acquisizione forense del supporto al fine di verificare l'attendibilità e paternità del contenuto informatico riprodotto, condizionando l'utilizzabilità della trascrizione di messaggi WhatsApp all'acquisizione forense del dispositivo.

L'importanza del rispetto delle tecniche disponibili nel campo dell'informatica forense, idonee a garantire la conformità all'originale e l'inalterabilità del dato informatico acquisito, è questione di informatica forense di antico fascino e rinnovato splendore, alla luce della maggiore comprensione della realtà informatica da parte degli operatori del diritto.

Le considerazioni che derivano dall'esigenza di acquisire il dato informatico nella sua integrità sono molteplici e di trasversale interesse. In una controversia in materia di proprietà intellettuale, la tutela degli interessi della controparte (quali, ad esempio, segreti e brevetti) impone l'individuazione di criteri di analisi dei dati acquisiti che la soddisfino senza comprimere le esigenze di accertamento della parte istante.

In un accertamento tecnico in ambito penale, le considerazioni da sviluppare si moltiplicano ed investono diverse prerogative processuali. Consideriamo, ad esempio, la difficoltà di individuare i dati informatici di interesse investigativo senza ispezionarne i supporti e di bilanciare un'apprensione onnivora dei dispositivi con i vincoli di proporzionalità, adeguatezza e pertinenza imposti alle misure cautelari. Senza dimenticare come un dato informatico apparentemente non rilevante da parte di chi lo sta valutando può essere di estrema importanza per un'altra parte, sia essa già coinvolta o ancora fuori dal procedimento.

Nel tentativo di distendere una simile tensione, la giurisprudenza di legittimità ha condannato i sequestri eseguiti in maniera indiscriminata in assenza di specifiche esigenze investigative[8] che ne giustifichino l'apprensione massiva; dall'altro subordina la validità degli stessi alla difficoltà di esecuzione della selezione del solo materiale pertinente e rilevante.

La selezione del materiale pertinente è una importantissima attività che richiede agli operatori del settore un impegno significativo sotto il profilo temporale, in termini di ore-uomo e ore-macchina necessari alla selezione, ed economico, in strumenti hardware e software dedicati all'indicizzazione, ricerca e consultazione dei dati acquisiti, oltre che profonda competenza nel settore applicativo (capacità di comprendere il significato dei dati in esame) e nello specifico procedimento nel quale si opera (capacità di comprendere le pertinenza del dato in esame).

Oltre la complessità naturale delle operazioni tecniche da espletarsi nel rispetto dei principi di integrità, immodificabilità ed inalterabilità del dato acquisito deve considerarsi l'ingresso di nuovi fattori di com-

[8] Il richiamo, ancora una volta, alle pronunce citate in precedenza, specificatamente le sentenze Cass., Sez. 6, n. 43556/2019 e Cass., Sez. 6, n. 24617/2015.

plessità determinati dall'aumento delle capacità di memorizzazione, che dilatano i tempi di analisi; dalla diffusione di più dispositivi differenti per ciascun soggetto, che richiedono specifici strumenti di acquisizione; dall'evoluzione delle misure tecniche di protezione e cifratura delle informazioni, che sollecita un costante aggiornamento delle competenze necessarie.

La crescente necessità processuale del fabbisogno informativo contenuto nei supporti informatici raccomanda lo sviluppo di procedure definite e modalità operative specifiche per bilanciare le diverse esigenze contrapposte nelle singole fattispecie processuali. Nelle pagine che seguono si proporrà una possibile soluzione alle problematiche sollevate alla luce delle più recenti attestazioni della Corte di Cassazione.

3. La rivoluzione della copia-mezzo

Nel confronto quotidiano con i profili di complessità fin qui esposti, la giurisprudenza di legittimità ha offerto differenti interpretazioni della *ratio* sottesa alle novelle della l. 48/2008, nel tentativo di definire prassi e modalità operative omogenee e idonee al raggiungimento di un bilanciamento in concreto degli interessi in gioco.

In tale direzione si collocano alcune recenti attestazioni della Corte di Cassazione in tema di perquisizione e sequestro di dati informatici, che manifestano l'esigenza di procedere alla loro acquisizione nel rispetto delle *best practices* di settore e delle garanzie processuali previste, salvaguardando la tutela dei diritti fondamentali coinvolti.

Di particolare interesse è la pronuncia della Corte di Cassazione, Sez. VI Pen., n. 12904/2020, che conferma il *modus procedendi* adottato negli accertamenti informatici svolti nel caso all'esame della Corte e prefigura una modalità operativa, accolta e arricchita da successivi orientamenti, da adottare per la selezione del materiale informatico pertinente e rilevante.

> L'operazione culminata nei sequestri, secondo quanto rilevato dal Tribunale, risulta essersi svolta per gradi, dapprima essendosi individuati i dispositivi informatici e di seguito essendosi proceduto all'estrazione di copie forensi, sulla base di specifici canoni selettivi, e quanto al personal computer del ricorrente, essendosi proceduto all'estrazione di copia forense immediatamente seguita dalla fissazione, a distanza di sette giorni, della data in cui un consulente tecnico avrebbe proceduto alla selezione dei soli documenti informatici rilevanti

> sulla base delle medesime parole chiave, con immediata restituzione del resto. Si tratta di *modus procedendi* specificamente conforme a quanto in generale previsto dall'art. 247 cod. proc. pen., in funzione dell'individuazione ed estrapolazione del materiale informativo pertinente[9].

Nello specifico, il provvedimento illustra le ragioni per le quali le modalità esecutive degli accertamenti risultino conforme al dettato normativo e rendano i provvedimenti legittimi, non rilevando una violazione dei canoni di pertinenzialità, proporzionalità e adeguatezza lamentate dal ricorrente.

Come correttamente ricostruito dalla Corte, il sequestro era stato eseguito previa estrazione di copia forense da sottoporre a successiva selezione mediante criteri definiti (parole chiave, delimitazione temporale; comparazione dei digest), con restituzione del dispositivo, da effettuarsi entro un intervallo di tempo ragionevole.

Nel merito della pronuncia in commento, si confermava la proporzionalità del sequestro di materiale informatico in virtù della natura graduale della procedura adottata per l'esecuzione dello stesso.

Meritevole di approfondimento è la metodica utilizzata per l'acquisizione e la selezione degli elementi probatori di interesse: da un lato, si procedeva all'esecuzione immediata di copia forense dei dispositivi mobili sulla base di specifiche parole chiave; dall'altro, si procedeva all'acquisizione forense dell'intero contenuto di un computer con successiva nomina di un consulente tecnico incaricato per l'estrazione dei soli documenti informatici rilevanti, provvedendo alla restituzione della copia forense al termine delle operazioni.

La procedura descritta supera, a parere della Corte, il vaglio di proporzionalità richiesto per l'esecuzione della misura cautelare del sequestro e vincola l'apprensione indiscriminata del contenuto dei dispositivi informatici alla successiva selezione, realizzando un adeguato bilanciamento tra le finalità investigative e le tutele processuali previste.

Testimone del crescente fermento nella definizione di procedure adeguate al soddisfacimento delle diverse esigenze in gioco, è la pronuncia della Cassazione, Sez. VI, n. 13165/2020 che conforta la modalità operativa sin qui descritta e specifica i profili di maggior interesse nella valutazione della proporzionalità della misura adottata.

[9] *Cfr.* Corte di Cassazione, Sez. VI Pen., n. 12904/2020

> Si tratta di modalità che, riflettendo i contenuti della disciplina dettata dall'art. 247 c.p.p., comma 1 *bis*, è volta per gradi a consentire l'acquisizione di dati contenuti nel sistema informatico e nel contempo ad assicurare la minor invasività dell'operazione a vantaggio della parte interessata: ciò che occorre è tuttavia il rispetto dei menzionati profili qualitativi, quantitativi e temporali. […] Ma se di per sé è garantita la continuità operativa e sono definiti i limiti della ricerca, non può parlarsi di un'invasività non giustificata[10].

Nella fattispecie all'attenzione della Corte, veniva esaminata la legittimità dell'ordinanza del Tribunale che disponeva la distruzione delle copie forensi acquisite e dei dati non pertinenti al *thema probandum*, cogliendo l'occasione per approfondire la proporzionalità della misura adottata e definire i limiti operativi nell'acquisizione di materiale informatico.

La massima espressa dalla pronuncia in commento riconosce come il bilanciamento tra le finalità investigative e le esigenze di tutela coinvolte nell'accertamento richieda un'adeguata valutazione sotto il profilo quantitativo, qualitativo e temporale della proporzionalità della misura adottata.

In altri termini, sotto il profilo quantitativo occorre verificare la sussistenza del nesso di pertinenzialità tra il supporto informatico oggetto di accertamento e il *thema probandum*, specificando l'idoneità probatoria dei dati contenuti e oggetto di interesse investigativo; sotto il profilo qualitativo, invece, è necessario valutare la strumentalità dell'apprensione integrale, mediante copia forense, all'individuazione garantita dei dati rilevanti e pertinenti; infine, sotto il profilo temporale bisogna contemperare la necessità di procedere ad operazioni tecniche in differita con l'interesse a rientrare in possesso dei beni oggetto di accertamento.

Sintetizzando le argomentazioni della Corte, in tema di acquisizione di elementi probatori informatici, la legittimità dell'estrazione mediante copia forense del contenuto integrale di un dispositivo informatico deve essere valutata «sotto il profilo ontologico in rapporto alla fase in cui si inserisce, in funzione della separata estrazione dei soli dati realmente rilevanti»[11], non potendo sindacare un'invasività non giustificata di tale

[10] *Cfr*. Corte di Cassazione, sez. VI penale, sentenza 28 aprile 2020 (ud. 4 marzo 2020), n. 13165/2020

[11] *Cfr*. Corte di Cassazione, sez. VI penale, sentenza 28 aprile 2020 (ud. 4 marzo 2020), n. 13165/2020

acquisizione «se di per sé è garantita la continuità operativa e sono definiti i limiti della ricerca»[12].

Perciò, al termine della selezione ed estrazione dei dati rilevanti, la copia forense acquisita non può che essere restituita all'avente diritto, in luogo della distruzione disposta dal Tribunale, quale forma di reintegro al possesso esclusivo dei dati contenuti nella copia forense.

Il rapporto tra l'utilità processuale delle informazioni contenute nei dispositivi informatici e il cambiamento imposto ai tradizionali modelli investigativi è efficacemente rappresentato nella sentenza della Corte di Cassazione, sez. VI, n. 34265/2020[13].

In prima battuta, la pronuncia in commento ricostruisce i limiti della legittimità del sequestro probatorio segnati dalla verifica, caso per caso, del nesso di pertinenzialità e strumentalità tra la *res* – dispositivo informatico – i fatti contestati e la finalità probatoria da soddisfare. In sede di verifica, quindi, occorrerà valutare la proporzionalità e la ragionevolezza della motivazione posta a fondamento della misura adottata e della sussistenza del nesso di strumentalità funzionale all'accertamento dei fatti[14].

Ciò è vero, a maggior ragione, nel contesto degli accertamenti informatici in cui vi è, da un lato, l'interesse investigativo all'acquisizione dei dati rilevanti nel rispetto delle misure tecniche a garanzia dell'integrità e inalterabilità di quanto acquisito, che richiedono competenze specialistiche di difficile attuazione negli atti a sorpresa; dall'altro, l'esigenza di tutela dei diritti fondamentali del soggetto sottoposto alla misura, evitando un inutile sacrificio dei diritti limitati dalla misura[15].

Addentrandosi nell'esame delle misure tecniche atte a garantire l'acquisizione genuina del dato informatico, caratterizzata dall'inalterabilità e dalla conformità all'originale del contenuto acquisito, la Corte offre una lucida interpretazione del portato normativo introdotto dalle interpolazioni della l. 48/2008 al codice di rito.

[12] *Cfr*. Corte di Cassazione, sez. VI penale, n. 13165/2020, cit.

[13] *Cfr*. Corte di Cassazione, sez. VI penale, sentenza 22 settembre 2020 (dep. 2 dicembre 2020), n. 34265

[14] Si ribadisce l'importanza dell'onere motivazionale in ordine al nesso di strumentalità tra la res informatica rispetto all'accertamento penale e della sua necessaria esplicitazione nel decreto di sequestro, in quanto funzionale a garantire che la misura adottata non arrechi un inutile sacrificio di diritti, il cui esercizio di fatto non pregiudicherebbe la finalità probatoria/cautelare perseguita, richiamando le pronunce SS.UU. n. 36072/2018 e la più nota pronuncia della Corte Cost. n. 85 del 2013.

[15] Per approfondimenti si veda il contributo di L. Bartoli, *Parità delle armi e e-discovery nel processo penale: quali indicazioni da Strasburgo?*

Infatti, richiamati i riferimenti alle varie modalità di acquisizione di dati informatici previsti dal codice di procedura[16], chiarisce come la creazione della copia forense di un dispositivo informatico sia la *procedura più adeguata a garantire l'integrità dei dati*, che richiede, nella prassi quotidiana, il sequestro del dispositivo per l'acquisizione e successiva selezione dei dati pertinenti alle finalità probatorie perseguite.

La portata innovativa della pronuncia in commento risiede nella corretta collocazione, sul piano tecnico-giuridico, del nucleo informativo acquisito mediante la creazione della copia forense che vale la pena di riportare nella sua interezza:

> Non rileva in sé come cosa pertinente al reato in quanto essa contiene un insieme di dati indistinti e magmatici rispetto ai quali nessuna funzione selettiva è stata compiuta al fine di verificare il nesso di strumentalità tra res, reato ed esigenza probatoria. Ne deriva, come è stato specificato dalla Corte di cassazione, che la c.d. copia integrale costituisce solo una copia-mezzo, cioè una copia che consente di restituire il contenitore, ma che non legittima affatto il trattenimento dell'insieme di dati appresi (Sez. 6., n. 13165 del 04/03/2020, Scagliarini). La copia integrale consente di fare, dopo il sequestro, ciò che naturalmente avrebbe dovuto essere fatto prima, cioè la verifica di quali, tra i dati contenuti nel contenitore, siano quelli pertinenti rispetto al reato. La c.d. copia integrale è una copia servente, una copia mezzo, e non una copia fine[17].

Il riconoscimento del carattere servente della copia forense produce un duplice effetto: vincola il trattenimento della copia forense esclusivamente per una cornice temporale definita e strettamente necessaria alla selezione delle sole informazioni conferenti con la funzione probatoria sottesa al sequestro; al termine della selezione degli elementi pertinenti al *thema probandum* si dovrà provvedere alla restituzione della copia integrale agli aventi diritto, non potendosi disporre il sequestro probatorio di res non necessarie per l'accertamento dei fatti.

In conclusione, la Corte definisce i limiti del provvedimento di sequestro probatorio informatico, rilevando che:

[16] Nello specifico le prescrizioni atte a garantire l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, contenute negli articoli in materia di ispezioni (art. 244, c. 2, c.p.p.), perquisizioni (art. 247, c. 1 *bis*, c.p.p.) e sequestro di dati informatici presso fornitori di servizi (art. 254 *bis* c.p.p.), come anche in materia di accertamenti urgenti da parte della polizia giudiziaria (art. 354, c. 2, c.p.p.).

[17] *Cfr*. Cass. pen., Sez. VI, 22 settembre 2020 (dep. 2 dicembre 2020), n. 34265

> Il Pubblico Ministero: a) non può trattenere la c.d. copia integrale dei dati appresi se non per il tempo strettamente necessario alla loro selezione; b) è tenuto a predisporre una adeguata organizzazione per compiere la selezione in questione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano stati sequestrati a persone estranee al reato per cui si procede; c) compiute le operazioni di selezione, la c.d. copia - integrale deve essere restituita agli aventi diritto[18].

La portata innovativa della pronuncia in commento si distingue chiaramente nella definizione di una procedura operativa, descritta nell'elenco richiamato, che realizza lucidamente il difficile bilanciamento dell'interesse investigativo dei dati informatici e le esigenze di tutela processuale della proporzionalità delle misure.

In tema di apprensione di dati informatici, meritevole di approfondimento è la Sentenza della Cassazione penale, sez. II, del 23/09/2020, n. 37941 per la efficace ricostruzione degli orientamenti giurisprudenziali in materia e per le motivazioni esposte a sostegno dell'adesione all'orientamento mediano tra quelli presentati[19].

Nella vicenda in esame, da un lato, veniva eseguito il sequestro probatorio di dispositivi informatici, per i quali si disponeva di procedersi ad accertamento tecnico non ripetibile (art. 360 c.p.p.) per la formazione della copia forense; dall'altro si procedeva al sequestro della sola copia forense e della posta elettronica, per i quali si disponeva un accertamento tecnico finalizzato all'estrazione del materiale rilevante a breve distanza dal sequestro.

I ricorsi esaminati dalla Corte deducevano la violazione di legge in ordine alla mancata identificazione delle finalità probatorie del vincolo imposto e al difetto di proporzionalità del materiale sottoposto a sequestro, acquisito senza eseguire alcuna attività perquirente diretta alla selezione dei dati di interesse da sottoporre a successivo sequestro.

La decisione di rigetto viene motivata sulla scorta di un iter argomentativo di fascinosa linearità che, ricostruendo le attestazioni giurisprudenziali in tema di acquisizione di dati informatici[20], afferma la

[18] *Cfr*. Cass. pen., Sez. VI, sent. n. 34265/2020, cit.

[19] *Cfr*. Cass. pen., Sez. II, 23 settembre 2020 (dep. 31 dicembre 2020), n. 37941.

[20] La pronuncia in commento ricostruisce gli orientamenti in materia di sequestro di dati informatici. Nello specifico richiama: a) le sentenze che hanno affermato la legittimità del sequestro dell'intero supporto informatico piuttosto che l'estrazione dei singoli dati quando la misura sia giustificata dalle difficoltà tecniche di estrapolare con riproduzione mirata i dati contenuti nella memoria informatico (Sez. V, n. 38456 del 17/05/2019 - dep. 17/09/2019, Benigni, Rv. 277343; Sez. V, n. 16622 del 14/03/2017 - dep. 04/04/2017, Storari, Rv. 270018);

funzionalizzazione del sequestro imposto all'intero supporto ad una analisi tecnica diretta all'individuazione dei dati rilevanti per la prosecuzione delle indagini.

Nello specifico, chiarita la funzione proattiva e l'onere motivazionale del sequestro probatorio delle cose pertinenti al reato, la Corte si sofferma nella declinazione dei principi generali, da tempo affermati nella giurisprudenza[21], all'apprensione dei dati contenuti in supporti informatici in quanto, pur non costituendo il corpo del reato, si rendono necessari all'accertamento dei fatti delineati nella notizia di reato.

Secondo l'orientamento della Corte, nella valutazione della proporzionalità del sequestro di dati informatici in qualità di cosa pertinente al reato occorre verificare la sussistenza e la corretta individuazione nel provvedimento genetico dei seguenti elementi:

> (a) deve essere identificato il fumus del reato per cui si procede ed il collegamento tra tale reato e i dati informatici che si intendono vincolare individuando così il nesso di "pertinenza"; (b) deve essere indicata la finalità probatoria che sorregge il vincolo; (c) se non si vincolano i dati, ma l'intero supporto (o tutti

b) le pronunce che hanno dichiarato l'illegittimità, per violazione del principio di proporzionalità e adeguatezza, del sequestro informatico a fini probatori che conduca in assenza di specifiche ragione ad un'indiscriminata apprensione di tutte le informazioni contenute. Tale orientamento ha trovato principale applicazione in fattispecie riguardanti dispositivi sequestrati a giornalisti (Sez. VI, n. 24617 del 24/02/2015 - dep. 10/06/2015, Rizzo, Rv. 264092; Sez. VI, n. 9989 del 19/01/2018 - dep. 05/03/2018, Lillo e altri, Rv. 272538) ma anche in situazioni diverse avente ad oggetto il sequestro dell'intero archivio cartaceo di un'azienda senza indicazione specifica dei documenti funzionali all'accertamento dei fatti (Sez. VI, n. 43556 del 26/09/2019 - dep. 24/10/2019, Scarsini, Rv. 277211); c) l'orientamento mediano che ritiene legittimo il sequestro informatico dai contenuti estesi, perché dati potenzialmente rilevanti per le indagini, purché si provveda, nel rispetto del principio di proporzionalità e adeguatezza, alla immediata restituzione delle cose sottoposte a vincolo, non appena sia decorso il tempo ragionevolmente necessario per gli accertamenti (Sez. VI, n. 53168 del 11/11/2016 - dep. 15/12/2016, Amores, Rv. 268489). Il collegio nel dare continuità all'orientamento mediano, precisa come il sequestro non debba essere necessariamente preceduto dalla perquisizione informatica, che necessita la predisposizione di competenze specialistiche incompatibili con l'effetto a sorpresa della perquisizione stessa. In conclusione, la pronuncia in commento valorizza, nella valutazione di proporzionalità del sequestro di supporti informatici, la variabile "tempo" necessaria per l'estrazione dei dati rilevanti.

[21] Richiamando testualmente l'ultimo capoverso del punto 1.1 del considerato in diritto della pronuncia in commento «il sequestro può ritenersi meramente "esplorativo" e, dunque illegittimo solo quando non si sia in presenza di una notizia di reato sufficientemente delineata e suscettibile di approfondimenti istruttori che legittima il sequestro a fini investigativi delle cose pertinenti al reato» (Sez. 6, n. 3187 del 07/01/2015 - dep. 22/01/2015, Boselli, Rv. 262084; Sez. 3, n. 24561 del 17/05/2012 - dep. 20/06/2012, Vicentini e altro, Rv. 252767).

> i dati in modo indistinto) deve essere, altresì, identificata la ragione della necessità del sequestro "integrale", di regola riconducibile alla impossibilità di effettuare la selezione tecnica preventiva, che richiede la predisposizione di una attività tecnica e competenze specialistiche[22].

Dunque, la legittimità del vincolo imposto ad una massa indistinta di dati potenzialmente rilevante per l'attività investigativa deve essere riconosciuta ogni qualvolta risulti funzionale all'esecuzione di accertamenti tecnici diretti all'identificazione degli elementi utili alla prosecuzione delle indagini e, perciò, sia limitato al tempo strettamente necessario all'esecuzione delle operazioni di acquisizione e selezione dei dati di interesse.

Il solco tracciato dalle sentenze in commento è avamposto alla codificazione di prassi e modalità operative ampiamente in uso nella pratica quotidiana degli accertamenti a carattere informatico, meritevole di trovare adeguato riconoscimento nel codice di rito tramite l'introduzione di una procedura autonoma per la selezione di dati informatici.

Dunque, da un lato viene garantita la legittimità di sequestri indiscriminati di materiale informatico, vincolata temporalmente all'esecuzione delle operazioni tecniche necessarie per l'accertamento richiesto, dall'altra viene sindacata la proporzionalità del provvedimento emesso dall'Autorità Giudiziaria in mancanza di criteri specifici da adottare nella selezione del solo materiale pertinente e rilevante per l'accertamento in parola, da sottoporre a successivo sequestro mediante la formazione di una copia forense del solo materiale selezionato.

La procedura descritta consente di limitare, da un lato, l'invasività del sequestro del dispositivo, provvedendo in tempi brevi all'acquisizione forense integrale e alla restituzione del supporto acquisito; dall'altro permette di circoscrivere il carattere esplorativo della misura eseguita all'acquisizione del solo materiale derivato dalla selezione dei contenuti secondo criteri predefiniti e calibrati sulle esigenze investigative della singola fattispecie.

Tuttavia, nell'adozione di una simile procedura operativa vi sono profili critici meritevoli di essere adeguatamente attenzionati e valutati nella cornice processuale di riferimento. In particolare, in ambito penale il rischio concreto che si profila è quello di aggirare i tradizionali principi processuali che sostengono l'impianto accusatorio del processo penale, lasciando nella piena disponibilità degli organi inquirenti tutto

[22] *Cfr*. Cass. pen., Sez. II, n. 37941/2020, cit.

il materiale acquisito e non ancora vagliato. O, peggio, mettere dati riservati a disposizione di terzi comunque coinvolti nel procedimento, con il rischio di divulgazione di informazioni riservate o sulla vita privata che nulla hanno a che vedere con i procedimenti giudiziari nei quali sono stati raccolti[23].

4. Le modalità operative adottate nella selezione di dati informatici in ambito giudiziario

In qualsiasi ambito di accertamento divenga necessario acquisire le informazioni contenute nei dispositivi di uso quotidiano, occorre far riferimento alle indicazioni fornite dagli standard di settore, spesso condensati nel termine *best practices*[24]. Nel campo dell'informatica forense, le linee guide da adottare nel trattamento della prova digitale sono codificate nello standard internazionale ISO/IEC 27037, che indica i principi e le procedure da rispettare nelle specifiche attività di identificazione, raccolta, acquisizione, conservazione e trasporto di una fonte di prova digitale. Ad esso, si aggiungono le differenti procedure operative pubblicate da organizzazioni internazionali, europei e nazionali[25], nel tentativo di definire modelli operativi applicabili in maniera omogenea alle differenti situazioni in cui risulta necessario assicurare l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Come noto, la definizione di simili procedure e *best practice* nello svolgimento degli accertamenti informatici ha l'obiettivo di garantire

[23] Sul carattere onnivoro degli accertamenti informatici eseguiti senza alcuna previa selezione o indicazione dei criteri selettivi da adottare si veda la recente sentenza Cass. pen., Sez. VI, 28 settembre 2021 (dep. 27 ottobre 2021), n. 38460. Di sicuro interesse è l'esplicitazione dei corollari necessari alla dichiarata illegittimità del provvedimento di sequestro, che comporta l'estensione dell'illegittimità della massa di dati acquisita e la restituzione all'avente diritto di tutte le copie forensi illegittimamente acquisite.

[24] Per una disamina più ampia dello stato attuale delle best practices, si veda R. Brighi, M. Ferrazzano, *Digital forensics: best practices and perspective*, in Caianiello M., Camon A. (a cura di), *Digital forensics evidence. Towards common european standards in antifraud administrative and criminal investigations*, Wolters Kluwer, 2021, pp. 13-48.

[25] Oltre agli standard internazionali, di particolare interesse sono le best practice di settore pubblicate dalle diverse organizzazioni, come American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), Scientific Working Group on Digital Evidence (SWGDE), IOCE (International Organization of Computer Evidence), IACIS (International Association of Computer Investigative Specialist), ACPO (Association of Chief Police Officer).

l'acquisizione di dati in forme tali da assicurarne l'integrità, l'autenticità e l'inalterabilità di quanto acquisito e soddisfare le esigenze di verificabilità delle operazioni eseguite, cercando di uniformare il modo di procedere degli operatori tecnici coinvolti – la cui formazione specifica in materia e quindi competenza tecnica è spesso variegata – che altrimenti potrebbero dare eccessivo sfogo alla propria fantasia (come peraltro comunque capita non essendo tali standard vincolanti).

A tale scopo è opportuno predisporre di un'adeguata conoscenza dei processi e dei requisiti richiesti per assicurare una concreta applicazione dei principi esplicitati dalle linee guida riconosciute a livello internazionale. Di interesse primario sarà individuare le competenze tecniche necessarie all'esecuzione delle attività sui reperti informatici, per il tramite di figure professionali in possesso di adeguate competenze tecniche[26] in grado di garantire la raccolta di tutti gli elementi informatici utili nel rispetto dei requisiti di verificabilità, affidabilità e giustificabilità delle operazioni svolte[27].

La fragilità del dato informatico, per le sue congenite caratteristiche effimere, impone di considerare con particolare attenzione le fasi dell'acquisizione e della conservazione della prova digitale, maggiormente suscettibili di comprometterne l'integrità e l'autenticità del dato informatico acquisito[28].

Un aspetto doveroso da chiarire riguarda la motivazione per la quale si esegue copia forense dei dati informatici: in informatica forense, a differenza di altre scienze forensi, è possibile duplicare in quantità infinita i dati che devono essere sottoposti ad analisi. Tale circostanza gioca a favore tanto di questioni di carattere logistico, permettendo di

[26] *Cfr*. *Annex* A ISO/IEC 27037.

[27] Nello specifico, per affidabilità si intende che tutti i processi eseguiti devono essere ben documentati producendo un risultato ripetibile utilizzando, in qualsiasi momento, la stessa procedura e metodo di misurazione, stessi strumenti e nelle stesse condizioni; la verificabilità delle operazioni richiede di garantire, documentando tutte le attività svolte, ad un consulente tecnico informatico terzo la facoltà di verificare le attività svolte, valutando metodo scientifico, le tecniche e le procedure seguite; infine per giustificabilità si richiede di essere in grado di dimostrare che le scelte adoperate erano le migliori possibili o le uniche possibili per ottenere tutte le potenziali prove digitali.

[28] Per una disamina esaustiva della necessità di acquisire correttamente il dato informatico, si veda C. MAIOLI, *Dar voce alle prove: elementi di informatica forense*, in Pozzi P., Masotti R. e Bozzetti M. (a cura di), Crimine virtuale, minaccia reale, a cura di FrancoAngeli, 2004. Sull'importanza della corretta metodologia da adottare nel trattamento della prova informatica, dalla sua acquisizione alla successiva analisi, si veda S. ATERNO, P. MAZZOTTA, *La perizia e la consulenza tecnica – con approfondimento in tema di Perizie Informatiche (analisi e schede tecniche di D. Caccavella)*, CEDAM, 2006.

distribuire il lavoro tra più analisi o di parallelizzare e rendere autonome le parti coinvolte, quanto di poter differire nel tempo e geograficamente l'analisi rispetto al luogo e all'epoca in cui ci si approccia al dato per la prima volta.

La creazione di copia forense ha, dunque, come fine primario quello di preservare il dato e spostarlo nel tempo e nello spazio, senza che tale operazione possa cagionare alcuna perdita di informazioni.

Tuttavia, da un punto di vista normativo, non risulta alcun ordinamento giuridico che imponga l'acquisizione totale, ossia bit a bit, di dati informatici, bensì vi è un generico richiamo all'adozione di soluzioni atte a garantire integrità e attendibilità dei dati informatici da utilizzare come prova.

Ne consegue che deve essere "scardinata" questa idea per la quale la prova informatica è la copia forense bit a bit, essendo in realtà tale operazione tecnica semplicemente a servizio della fase di analisi dei dati ivi contenuti. Per sostenere la tesi per la quale non è solo la copia bit a bit a doversi considerare "copia forense" è sufficiente spostarsi dal primigenio ambito della *disk forensics* "pura" e prendere in considerazione tutto l'ambito della *mobile forensics*. In tale branca è piuttosto raro che si esegua una copia bit a bit, sia per ragioni tecniche di impossibilità o estrema difficoltà, sia per non intellegibilità dei dati, spesso cifrati, preferendo una soluzione di acquisizione di altro tipo (backup, file system o addirittura fotografica). Si pensi, inoltre, pur rimanendo nel contesto di disk forensics, a tutti quei casi in cui è più che sufficiente acquisire un sottoinsieme di dati, per i quali il dato informatico oggetto di accertamento prescinde dal contesto nel quale è memorizzato (ad esempio, in un caso di contenzioso su un codice sorgente appare superflua l'acquisizione di tutto il sistema informatico che lo contiene).

Chiarito, dunque, quale sia il vero ruolo di una copia forense in un accertamento tecnico di informatica forense, a prescindere dalla modalità e dall'estensione della stessa, si approfondisce nel seguito la modalità di analisi per selezionare i soli dati informatici rilevanti per il procedimento.

5. L'e-discovery per la selezione del materiale rilevante

Dopo aver assicurato una corretta acquisizione e conservazione del reperto informatico, occorre definire i limiti e gli obiettivi dell'analisi fo-

rense da svolgersi sui reperti acquisiti e valutare le risultanze dell'investigazione condotta, presentando gli esiti ottenuti e motivando il percorso scientifico a fondamento delle valutazioni svolte in sede di analisi.

Sebbene tale operazione presenti profili di rischio piuttosto bassi, svolgendosi su una copia terza (c.d. copia lavoro), resiste comunque la necessità di adeguate competenze tecniche per la corretta interpretazione e valutazione delle evidenze informatiche ottenute.

A supporto degli operatori di settore, vi sono procedure consolidate per la conduzione dell'analisi e la ricerca di evidenze memorizzate in formato elettronica, condivise a livello internazionale e recepite nello standard ISO/IEC 27050 che identifica i criteri e i requisiti del c.d. processo di e-discovery.

L'*electronic discovery* è il processo che, nell'ambito delle attività di informatica forense, consente di ricercare e individuare informazioni pertinenti e rilevanti memorizzate in formato digitale (in inglese *electronically stored information*, abbreviato in ESI). Lo standard citato definisce le differenti tipologie e sorgenti di ESI, le molteplici modalità di rappresentazione delle informazioni individuate e le fasi in cui si articola il processo, sovrapponibili a quelle previste per il trattamento della prova digitale[29].

Ogni informazione digitale potenzialmente rilevante deve essere individuata all'interno di una crescente quantità di dati provenienti da fonti molteplici e di uso promiscuo, che dovranno essere acquisite e conservate preservando l'integrità del dato da interventi modificativi e,

[29] Le tipologie descritte dallo standard sono definite dalla distinzione tra dati immediatamente accessibili (*active data*) e dati non immediatamente accessibili (*inactive, residual, legacy data*). Nella tipologia dei c.d. *active data* rientrano tutti i dati memorizzati all'interno del supporto e visibili all'utente nel normale utilizzo del dispositivo; in quella dei *c.d. inactive data* rientrano tutti i dati archiviati e non disponibili all'utente, memorizzati in automatico dai sistemi di backup, spesso custoditi presso fornitori terzi; nella categoria dei c.d. *residual data* vi sono i file nascosti utilizzati dal sistema operativo in uso, quelli danneggiati o cancellati; infine, all'interno dei c.d. *legacy data* rientrano tutte le informazioni generate da sistemi informatici per i quali il produttore non rilascia più aggiornamenti. Le diverse tipologie di fonti sorgenti di ESI sono divise nelle c.d. *Custodian data sources*, ovvero supporti sui quali un determinato utente ha il diretto controllo o gestione, e nelle c.d. *Non-custodian data sources*, ovverosia infrastrutture per la gestione di più informazioni sotto il controllo di un amministratore, come NAS, database e applicazioni per la condivisione di ESI, cloud storage. Infine, tra e forme di rappresentazione per la produzione delle ESI, lo standard prevede la seguente classificazione dei formati: a) *native* e b) *near-native,* consigliata per file non progettati per la stampa come database, fogli di calcolo, etc.; c) *image (near- paper)* e d) *paper*, per la produzione di immagini visive o dati progettati per essere stampati su carta.

successivamente elaborate, mediante il processo di indicizzazione dei contenuti acquisiti, per essere ricercabili mediante criteri predefiniti, calibrati sulle esigenze investigative del caso.

Nella selezione di informazioni potenzialmente rilevanti, le tecniche di ricerca automatizzate a supporto degli operatori del settore sono molteplici e diversamente utili a seconda del contesto investigativo. Nella ricerca di contenuti difficilmente modificabili, l'individuazione dei contenuti di interesse può essere agevolmente effettuata mediante la comparazione delle impronte hash contenute in un insieme di digest noto con quelle dei dati acquisiti[30].

Di maggior diffusione è la metodologia della ricerca per parola chiave, che consente di individuare i dati di interesse utilizzando stringhe di ricerca, composte da termini specifici, diversamente declinabili a seconda della loro utilità. Il rischio di selezionare ed esaminare una grande quantità di falsi positivi è strettamente correlato al grado di specificità dei termini impiegati e alla granularità dei criteri di ricerca utilizzati.

In tale contesto, occorre dedicare particolare attenzione all'individuazione degli obiettivi dell'accertamento e alla definizione di stringhe di ricerca specifiche, combinate con ulteriori condizioni di validità dei riscontri ottenuti, utili all'isolamento del solo materiale di interesse da sottoporre alla successiva valutazione degli attori coinvolti nell'accertamento.

Le differenti tipologie di ricerche per parola chiave permettono di costruire stringhe di ricerca calibrate sulle peculiari esigenze investigative del caso, ricorrendo alla ricerca di termini per corrispondenza esatta, per corrispondenza approssimativa, vincolati alla validità di operatori booleani o di differenti logiche adottate[31].

Pertanto, la selezione di dati di interesse nell'ambito di un accertamento giudiziario dovrà essere attentamente progettata, identificando i parametri da attribuire all'indicizzazione dei contenuti acquisiti e definendo il perimetro della ricerca e dei criteri da applicare nella selezione

[30] Ad esempio, nelle indagini per reati pedopornografici l'utilizzo di un archivio di immagini e video già noti e segnalati per essere contenuti pedopornografici, l'analisi dei dati acquisiti può essere agevolmente comparando le impronte hash dei dati acquisiti con quelli già noti. La stessa logica viene utilizzata negli accertamenti per violazioni in materia di diritto d'autore, proprietà intellettuale.

[31] Ad esempio, gli algoritmi di ricerca che adottano la logica *fuzzy*, evoluzione della logica booleana che consente di attribuire validità logica diverse da vero e falso; oppure la logica *stemming*, per individuare parole derivate dal termine utilizzato; o, ancora, una ricerca per fonemi che permette di individuare parole con stessi fonemi.

del materiale, permettendo di ampliare e restringere la pertinenza dei riscontri ottenuti.

Si noti che tali modalità sono ampiamente in uso nei procedimenti civili relativi a violazioni di segreti industriali, allorquando a seguito di una raccolta dati anche massiva in sede di descrizione, il Giudice solitamente nomina un proprio Consulente Tecnico d'Ufficio affinché possa selezionare unicamente il materiale pertinente con l'oggetto del ricorso o dell'atto di citazione, applicando questo genere di filtri per isolare il solo insieme di file di rilievo e non consentendo alla parte ricorrente di disporre di tutti gli altri dati.

La stessa modalità di selezione di dati rilevanti con tecniche di e-discovery è ampiamente utilizzata in ambito difensivo da parte anche di studi legali che, attraverso idonee piattaforme di e-discovery, permettono la collaborazione parallela da parte di più utenti nel vaglio della documentazione disponibile, sia essa acquisita dal fascicolo processuale o nell'ambito di proprie indagini difensive. Tali piattaforme consentono, tra le altre, di classificare i dati tramite etichette che permettono, attraverso raffinamenti successivi, di potersi focalizzare sulle sole informazioni rilevanti.

6. Protocolli in uso

La necessità di selezionare il solo materiale di interesse investigativo, all'interno della massa magmatica delle informazioni memorizzate in supporti digitali, si manifesta con evidenza nella prassi quotidiana delle investigazioni informatiche, in qualsiasi cornice processuale.

Ad esempio, negli accertamenti in materia di proprietà intellettuale, in cui spesso le informazioni di interesse sono esclusivamente disponibili in formato digitale, si rende necessario procedere ad un'attenta selezione ed estrazione dei soli dati rilevanti per i fatti oggetto di accertamento, contemperando le esigenze di riservatezza delle informazioni acquisite.

Nell'esecuzione di provvedimenti di descrizione, ex art. 129 c.p.i., lo svolgimento della fase cautelare di raccolta degli elementi utili all'accertamento è prassi quotidiana ricorrere ai principi e alle linee guida contenuti negli standard richiamati. Di fatti, in esecuzione del decreto si provvede al congelamento dei dati potenzialmente rilevanti mediante acquisizione forense della memoria dei supporti descritti; suc-

cessivamente si procede ad un'analisi sommaria, per la tipologia di procedura, dei possibili riscontri ottenuti dalle ricerche effettuate per confermare o smentire gli elementi probatori a sostegno del ricorso presentato.

Allo stesso modo, ciò si rende necessario nell'ambito delle indagini aziendali nei casi in cui occorre raccogliere, esaminare e documentare il riscontro di evidenze informatiche, contenute nei supporti informatici aziendali, a dimostrazione di condotte giuridicamente rilevanti. Sebbene sia in una fase prodromica all'instaurazione di un procedimento giudiziario, risulta altrettanto importante eseguire gli accertamenti informatici nel rispetto delle *best practices* di settore, sia in termini di validità probatoria degli elementi informatici raccolti e in termini di efficacia dell'azione legale proposta.

E, come si è visto, ciò risulta a maggior ragione utile negli accertamenti in ambito penale in cui occorre bilanciare, nello svolgimento delle attività tecniche, le diverse prerogative e tutele processuali in gioco. L'esigenza investigativa di eseguire provvedimenti preservando il carattere "a sorpresa" dei mezzi istruttori tradizionali deve misurarsi con la necessità di avere a disposizione competenze tecniche specialistiche in grado di assicurare l'acquisizione dei dati in conformità con le prescrizioni del codice di rito poste a garanzia dell'esercizio del diritto di difesa.

Spesso, tale difficoltà operativa impone, solo per i dispositivi fisicamente disponibili sul luogo di intervento, di procedere all'apprensione del supporto contenente informazioni di interesse investigativo, sottoponendolo alla misura del sequestro probatorio, prodromica all'esecuzione di accertamenti tecnici finalizzati all'acquisizione forense dei contenuti e alla successiva selezione ed estrazione dei dati informatici rilevanti. Permangono in ogni caso le esigenze di acquisire nell'immediatezza delle attività i dati di sistemi che non possono essere oggetto di ablazione per esigenza di continuità del servizio (si pensi, ad esempio, a un server di un ospedale) o per impossibilità di apprensione della *res* (dati memorizzati in sistemi remoti e disponibili in *cloud*).

Le prerogative processuali in ambito penale richiedono di costruire procedure e modelli operativi in cui poter trovare, a seconda della fattispecie, il giusto bilanciamento degli interessi coinvolti nell'accertamento, garantendo l'esecuzione delle operazioni tecniche nel rispetto delle best practices di settore e la partecipazione dei soggetti coinvolti per l'esercizio dei propri diritti.

7. Prospettive *de iure condendo*

Come abbiamo visto nelle recenti attestazioni giurisprudenziali, la crescente importanza probatoria dei dati informatici, memorizzati nei diversi dispositivi di uso quotidiano, ha plasmato l'interpretazione delle novelle introdotte dalla l. 48/2008 negli accertamenti a vocazione informatica. Maggior importanza viene data alla successiva fase di selezione ed estrazione del materiale di interesse, vincolando la legittimità del provvedimento alla definizione di criteri chiari e specifici per la ricerca e selezione all'interno della copia forense acquisita.

Dalla lettura delle evoluzioni interpretative fin qui commentate, si delinea una procedura operativa in cui l'iter da seguire è il seguente:

1. apprensione del supporto contenente dati di interesse, specificando il nesso di pertinenzialità, la finalità probatoria e la ragione del sequestro integrale del supporto con i dati informatici di interesse;
2. definizione di criteri per la selezione dei dati rilevanti rispetto al provvedimento di sequestro e successiva elaborazione dei contenuti mediante *tool* di indicizzazione e ricerca (per parola chiave, per hash, per periodo temporale, per adiacenza di percorso di salvataggio, per esame visivo manuale, ecc.) dei contenuti acquisiti;
3. formazione di una copia forense, da intendersi come insieme di dati selezionati e relativi hash, contenente i soli dati pertinenti e rilevanti oggetto di selezione, con restituzione della copia integrale all'utilizzatore del dispositivo.

L'adozione della procedura appena descritta è già da tempo in uso nella prassi degli operatori del settore nelle investigazioni difensive, mentre lo è raramente in quelle dell'Autorità Giudiziaria, trovando applicazione solo nei rari casi in cui i consulenti tecnici coinvolti sono in possesso di specifiche competenze tecniche e giuridiche oltre che di carisma per poter sostenere la validità tecnico-giuridica di tali procedure di fronte al dibattito processuale. Ciò in quanto tale procedura non è espressamente codificata all'interno del codice di rito ed è soggetta alla discrezionale applicazione dell'Autorità Giudiziaria procedente. Una simile lacuna legislativa presenta molteplici profili di rischio meritevoli di approfondimento e che richiedono di immaginare

nuove vesti processuali agli accertamenti giudiziari a vocazione informatica[32].

Sotto il profilo investigativo occorre, da un lato, assicurare l'efficacia del carattere a sorpresa che connota i mezzi di ricerca della prova, senza che ciò subisca limitazioni in virtù della complessità tecnica delle operazioni da eseguire; dall'altro, occorre prevenire le derive esplorative derivanti dall'acquisizione effettuata senza previa verifica della pertinenza dei contenuti memorizzati all'interno del supporto sequestrato.

Dalla prospettiva difensiva delle indagini penali a vocazione informatica, è di primaria importanza definire modalità operative in cui l'esercizio delle facoltà previste dal codice di procedura siano agevolmente azionabili e non vengano compresse dall'apparente evasione dell'onere motivazionale richiesto per l'adozione di misure cautelari reali.

In tale contesto, occorre riconoscere un'autonoma dignità processuale alla fase di selezione del materiale pertinente con le finalità investigative, costruendo una procedura operativa di applicazione generale e prevedendo modalità operative flessibili e adattabili alle esigenze probatorie di ciascun accertamento.

Una delle possibili soluzioni alla fumosità delle modalità operative adottate nella selezione di dati informatici in ambito giudiziario potrebbe essere individuata nell'inserimento di una procedura speciale che, combinando i principi e le linee guida dello standard ISO/IEC 27037 e 27050, consenta di acquisire le fonti di prova informatica secondo i principi dell'informatica forense e di esaminarli mediante le tecniche fornite dall'e-*discovery*, in un processo di elaborazione della fonte di prova informatica trasparente e verificabile.

Simile obiettivo potrebbe essere realizzato dall'adozione di un algoritmo operativo articolato nelle seguenti operazioni, eseguite garantendo la piena partecipazione delle parti processuali:

- acquisizione integrale dei supporti potenzialmente rilevanti secondo i principi dell'informatica forense, a garanzia della genuinità, integrità ed immodificabilità del contenuto acquisito;
- definizione in contraddittorio dei parametri di indicizzazione e dei criteri di ricerca da adottare per la selezione del materiale per-

[32] Di recente divulgazione la nota d'indirizzo organizzativo diramata dalla Procura Generale della Repubblica di Trento che recepisce il protocollo operativo proposto, uniformando le prassi in uso negli accertamenti tecnici di informatica forense ed adeguandole alle diverse esigenze processuali.

tinente e rilevante; l'esigenza del contraddittorio deriva dalla necessità di consentire non tanto il controllo quanto di favorire anche la permanenza di dati utili per le difese;
- formazione di una copia forense dei dati selezionati in quanto pertinenti e rilevanti per l'oggetto dell'accertamento;
- restituzione della copia forense integrale del supporto acquisito al legittimo utilizzatore.

Nell'esecuzione delle attività previste per ciascuna delle operazioni individuate nella procedura descritta, occorre considerare con particolare attenzione la cornice temporale entro la quale completare tutte le operazioni richieste, che non potranno protrarsi *sine die*, e le modalità di conservazione e gestione degli accessi al contenuto integrale dei supporti acquisiti.

In quest'ottica, la partecipazione alle attività tecniche dei soggetti coinvolti nelle forme più ampie riconosciute dall'ordinamento (accertamento tecnico non ripetibile o, meglio, incidente probatorio) appare elemento indefettibile della procedura proposta, consentendo di bilanciare adeguatamente le esigenze difensive tutelate in ambito penale e permettendo di verificare la legittimità delle operazioni eseguite e la proporzionalità delle misure, dei criteri e del materiale estratto dalla procedura adottata.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464305
pp. 83-99 (gennaio 2022)

Parità delle armi e e-discovery nel processo penale: quali indicazioni da Strasburgo?

Laura Bartoli[1]

1. Introduzione

In un saggio scritto ormai più di quindici anni fa, un autorevole studioso statunitense caldeggiava l'adozione di una «nuova procedura penale», imposta a suo avviso dall'avanzare di una diversa, dirompente categoria di prova: quella digitale[2]. Le regole vigenti, scriveva, avevano radici profonde e nobili: s'erano evolute nei secoli per conciliare diritti individuali e repressione dei reati all'interno di un mondo che aveva subito molti mutamenti, ma poche rivoluzioni. La *summa divisio* in materia probatoria – la contrapposizione tra prove dichiarative e prove reali – era stata consacrata ai tempi di Bentham; certo, molto era cambiato nella disciplina di dettaglio, ma le grandi categorie restavano le stesse, e restavano capaci di spiegare il sistema, nonché di orientare operatori e interpreti. Questa era, avvertiva, col digitale, sarebbe finita. Bisognava affrettarsi a reagire, ad adeguare le norme e approntare un paradigma nuovo, o quelle antiche, nobili radici, in relativamente poco tempo, avrebbero portato frutti avvelenati.

Oggi la prova digitale appartiene al quotidiano; la «nuova procedura penale», invece, si sta ancora facendo attendere. Le modifiche normative si sono limitate a prendere atto dell'esistenza dei dati trattandoli perlopiù come una sorta di appendice delle tradizionali prove fisiche, e la profezia si è avverata: le potenzialità dell'indagine informatica hanno travolto gli equilibri del sistema; di conseguenza, il compromesso tra pubblico potere e garanzie appare, se non più precario, meno collaudato. Gli snodi che ne risentono non sono pochi: perfetti in altri contesti,

[1] Assegnista di ricerca presso l'Università di Torino.
[2] O.S. Kerr, *Digital Evidence and the New Criminal Procedure,* in *Columbia Law Rev.*, vol. 105 (2005), p. 279 ss.

risultano sghembi o comunque mal strutturati dinanzi alle geometrie che l'informatizzazione ha creato.

Tra le molte asimmetrie, una delle più vistose riguarda la *discovery*: si tratta senza dubbio di uno degl'ingredienti fondamentali del diritto a godere del «tempo e delle facilitazioni necessarie a preparare la [propria] difesa» garantito dall'art. 6 § 3 *b* Conv. e.d.u. Senza un'adeguata conoscenza del caso, l'imputato non potrebbe valutare realisticamente le proprie opzioni né predisporre una strategia processuale informata. L'accertamento, insomma, si torcerebbe in agguato[3]. Ma che fare se l'accusa, nel corso delle indagini, ha prelevato milioni e milioni di documenti? Quale e quanto materiale dev'essere sottoposto alla controparte? Con quanto anticipo? In quale formato? [4] Insomma, come si deve strutturare la *discovery* perché rimanga compatibile con il principio di parità delle armi e, più in generale, con i canoni del 'giusto' processo?

Dopo una breve disamina dei fattori che hanno contribuito a complicare il segmento, passeremo in rassegna i principali temi emersi di fronte alla Corte europea dei diritti dell'uomo, nonché le risposte fornite in quella sede.

2. Cause ed effetti di una torsione

Le difficoltà in materia di *discovery* sono spie di un'evoluzione che, in larga parte, si colloca altrove. Se il diritto ad accedere agli atti del pubblico ministero è rimasto tale, tanto nella sua affermazione generale quanto nella disciplina di dettaglio, il digitale ha cambiato l'indagine, sia nell'estensione che nei metodi.

Da un lato, infatti, il semplice ammontare di informazioni disponibili riguardo a un fatto o a una persona è aumentato notevolmente, e non solo a causa dell'ubiquità ormai familiare di telefoni e computer. I congegni con cui una singola persona interagisce sono sempre più vari, numerosi e impercettibili, tanto integrati nella quotidianità da diventare praticamente trasparenti. Non sono rari i casi risolti grazie anche al contributo di orologi, braccialetti, impianti di domotica, pacemaker car-

[3] Per un'analisi della disciplina italiana della *disclosure*, specie in relazione ai diritti garantiti dalla Convenzione e.d.u. v. S. ALLEGREZZA, *La conoscenza degli atti nel processo penale fra ordinamento interno e Convenzione europea*, in A. BALSAMO-R. KOSTORIS, *Giurisprudenza europea e processo penale italiano*, Giappichelli, Torino 2008, p. 143 ss.

[4] Il catalogo delle questioni aperte, in realtà, è ben più esteso: per ragioni di spazio, ci limiteremo qui a trattare queste.

diaci: tutti apparecchi capaci di consegnare agl'investigatori qualche ragguaglio su come una certa vicenda possa essersi svolta. L'accertamento penale, almeno in potenza, è in grado di mappare con precisione fatti della vita che, solo un paio di decadi fa, non sarebbe nemmeno riuscito a lambire.

D'altro canto, la quantità non è l'unico aspetto che merita attenzione. La qualità del materiale ha forzato un adeguamento delle tecniche, in modo da rendere le ricerche il più possibile affidabili e accurate: i dati, infatti, sono elementi preziosi ma effimeri, che possono essere danneggiati o persi se li si maneggia con imperizia; inoltre, è raro che le informazioni rilevanti siano nettamente separate da tutto il resto, facili da individuare e interpretare senza analisi più raffinate sull'archivio dal quale provengono. Per queste ragioni, molte linee guida di settore raccomandano prudenza: almeno per i casi più delicati, è bene clonare l'intera memoria informatica con metodi che garantiscano la conformità della copia all'originale. Anziché prelevare solo quel che serve, si preferisce talvolta raccogliere tutto: le porzioni interessanti saranno individuate in un secondo momento, in un ambiente protetto, magari con l'aiuto di strumenti appositi e personale specializzato[5].

Il modo di procedere, tuttavia, presenta qualche inconveniente: esso costringe a estrarre e conservare molte più informazioni di quelle strettamente rilevanti per l'indagine, sacrificando la *privacy* dei soggetti coinvolti e imponendo tanto agl'inquirenti quanto alla difesa un'operazione di spoglio che, a seconda delle circostanze, può rivelarsi più o meno onerosa. Ad esempio: se i dati provenissero da un solo dispositivo appartenente al sospettato, le ricerche si farebbero probabilmente semplici; l'accusa potrebbe avvalersi delle proprie strutture e la difesa prenderebbe presto confidenza con un apparecchio organizzato dalla persona sottoposta a indagini. Se ad essere sotto scrutinio fossero invece più dispositivi appartenenti a individui diversi, il tema del tempo e delle facilitazioni necessarie alla preparazione della difesa emergerebbe in maniera prepotente. Non che le operazioni non si facciano più complesse anche per gli inquirenti, ma per loro, verosimilmente, si tratte-

[5] Per una ricognizione degli standard tecnici e, soprattutto, per una proposta metodologica più selettiva, ma non meno affidabile, v. R. Brighi-M. Ferrazzano, *Digital Forensics: Best Practices and Perspectives*, in M. Caianiello-A. Camon, *Digital Forensic Evidence*, CEDAM, 2020, p. 43 ss. Per approfondimenti si veda il contributo di M. Ferrazzano, L. Summa, *La selezione di dati informatici in ambito giudiziario: prassi e modalità operative*.

rebbe più che altro di una questione di scala: sono professionisti dell'accertamento; dispongono di operatori specializzati o comunque delle risorse per assumere professionisti dedicati. L'accusa, inoltre, muove per prima: ha l'onere di ricostruire l'accaduto e di dimostrare la correttezza della propria versione ma, almeno inizialmente, può lavorare nel segreto e con relativa calma. Non appena si indossano i panni del difensore, invece, l'orizzonte cambia. È difficile immaginare un avvocato che, per quanto competente e avviato, disponga di una struttura tale da rivaleggiare con un ufficio di procura: non potrà contare su unità di investigatori formati e l'aggiunta di consulenti esterni al collegio difensivo dipende in maniera cruciale dalle possibilità economiche dell'assistito; i tempi della preparazione, infine, non sono indefiniti, ma dettati dell'incedere di un procedimento cui altri hanno dato impulso.

Dinanzi a questa realtà, ci si è chiesti se e come risulterebbe opportuno aggiornare la nozione di "facilitazioni" utili a predisporre efficacemente la difesa, e lo si è domandato all'organo meglio piazzato per dare risposte innovative: non essendo vincolata dagli ordinamenti nazionali, la Corte europea dei diritti dell'uomo non deve marciare al passo dei legislatori. Essa è giudice ultimo dell'equità del processo ai sensi della Convenzione e.d.u.: poco importa che le autorità abbiano seguito fedelmente leggi vigenti o prassi consolidate; se il risultato appare sbilanciato, la Corte e.d.u. può censurarlo.

3. Diritto d'accedere a cosa? Perimetro della *discovery* digitale

Nella definizione del portafoglio di diritti e prerogative della difesa nell'ambito della *disclosure* digitale, una questione è preliminare rispetto alle altre. Abbiamo visto che, spesso, il materiale prelevato eccede di gran lunga la quantità di materiale utile; nell'ambito di un'indagine, quindi, potranno coesistere diverse collezioni di dati: quella più vasta conterrà le informazioni "grezze", così come sono state raccolte; quello più ristretto comprenderà solo il materiale ritenuto rilevante, che l'accusa ha intenzione di utilizzare nel corso del processo.

Ora, nessuno dubita del diritto della difesa d'accedere all'ultimo insieme: in assenza di particolari ragioni di sicurezza o di ordine pubblico, l'imputato deve poter se non altro consultare ogni elemento che lo incrimini o che lo aiuti; la violazione di tale principio condurrebbe senz'altro alla dichiarazione d'iniquità del processo. Riguardo all'intera

collezione, però, il discorso si fa più sfumato: la maggior parte delle informazioni che contiene avrà probabilmente poco o niente a che vedere con il caso – serve a garantire l'autenticità delle informazioni e la correttezza epistemologica dell'indagine; sul piano del contenuto, però, non ha nulla da offrire. Può la difesa vantare il diritto d'accedere ai dati grezzi, prevalentemente irrilevanti; deve accontentarsi della selezione operata dal pubblico ministero o i canoni del 'giusto' processo esigono qualche equilibrio intermedio?

La domanda è stata posta alla Corte e.d.u. in un caso emblematico, sorto a seguito delle indagini e del processo contro i responsabili del fallimento delle maggiori banche islandesi coinvolte dalla crisi finanziaria del 2008[6]. Gli investigatori, diretti da un procuratore *ad hoc*, avevano acquisito praticamente tutti i dati presenti nei computer delle società interessate, oltre a diverse memorie esterne di proprietà dei dipendenti delle aziende. La mole di materiale prelevato, insomma, aveva del monumentale e chiedere a una squadra d'agenti di esaminare ciascun documento alla ricerca di elementi utili sarebbe stato irragionevolmente dispendioso in termini di tempo e di risorse; la raccolta grezza, quindi, è stata analizzata con un software in grado di eseguire ricerche per parole chiave. La soluzione è ormai diffusa perché consente non solo di separare il grano dal loglio in maniera assai più efficiente[7]; essa consente anche di proteggere meglio alcuni interessi rilevanti sul piano giuridico: nessun essere umano andrà a rovistare in ogni cartella, né dovrà

[6] Corte e.d.u., 4 giugno 2019, Sigurður Einarsson c. Islanda.

[7] In generale, non si tratta di un obbligo: gli inquirenti conservano un buon grado di discrezionalità quanto alla scelta delle tecniche, anche di spoglio. Tuttavia, l'impiego di programmi informatici capaci di setacciare il materiale è ormai all'ordine del giorno, imposto da limiti di tempo e di risorse. Le linee guida emesse dal *Attorney General Office* britannico, per esempio, recitano chiaramente che, se il materiale fosse troppo, sarebbe impossibile esaminare singolarmente ciascun documento elettronico, «dunque, non ci si deve aspettare che ciò accada». Anzi, nei casi in cui il materiale sia troppo «è perfettamente accettabile la ricerca a campione o per parole chiave […]. Le tecnologie di ricerca che fanno uso di calcoli inequivoci per risolvere problemi determinati, come algoritmi o *predictive coding*, costituiscono metodi accettabili per esaminare e selezionare il materiale»: *Attorney General's Guidelines on Disclosure. For investigators, prosecutors and defence practitioners*, p. 32,18 dic 2020, disponibili al sito *gov.uk.*

La Corte di cassazione italiana, a volte, pare essersi spinta un passo oltre, mostrando un certo favore per metodi simili. In un caso, per esempio, ha annullato il sequestro «onnivoro» di numerosi dispositivi proprio perché la polizia giudiziaria aveva svolto un esame preliminare su tutte le informazioni duplicate anziché attendere che il consulente tecnico nominato dal pubblico ministero svolgesse la selezione per parole chiave. Il modo di procedere non è stato ritenuto conforme ai principi di adeguatezza e proporzionalità: Cass., Sez. VI, 22 settembre 2020, Aleotti, n. 34265, in *SentenzeWeb.*

direttamente vedere o leggere ogni singolo file. Di conseguenza, la tecnica consente di tutelare almeno entro certi limiti la privacy dei soggetti coinvolti e la stessa integrità metodologica dell'indagine. Quanto al primo profilo, le ricerche per parole chiave permettono di isolare il materiale che più interessa, lasciando tutto il resto in una massa confusa; la selezione non sarà perfetta, peccherà per eccesso o per difetto, ma eviterà comunque il sistematico esame di dati che, con l'ipotesi di reato, non hanno nemmeno un termine in comune. Quanto al secondo versante, il metodo evita che l'atto d'indagine, da mezzo di ricerca di elementi di prova, si trasformi in uno strumento esplorativo, che cerca notizie di reato nuove anziché indizi capaci di corroborare o smentire un'ipotesi già formata: perché la ricerca per parole chiave sia efficace, infatti, gl'investigatori dovranno filtrare il materiale in base a conoscenze prestabilite, a piste già tracciate[8].

Una volta individuati i singoli *file* pertinenti, gli investigatori li hanno inseriti nel fascicolo d'indagine: la difesa, a quel punto, ha potuto consultarli ed estrarne copia. L'accesso all'intera raccolta, invece, le veniva ripetutamente negato.

Gli imputati – incassata la condanna – hanno lamentato davanti alla Corte e.d.u. la violazione dell'art. 6 c. 1 e 3 lett. *b* della Convenzione: secondo i ricorrenti, l'accusa aveva potuto esaminare tutte le informazioni a suo piacimento, avvalendosi di strumenti all'avanguardia per scegliere cosa presentare in tribunale e cosa lasciar fuori; la difesa, invece, non si era potuta avvicinare: non aveva potuto svolgere ricerche autonome sulla base di diverse parole chiave. Il monopolio di fatto che la parte pubblica deteneva sulla collezione "integrale" si sarebbe risolto in una plateale e ingiustificata violazione del principio della parità delle armi: se l'accusa avesse voluto trattenere dati riservati, di cui non avesse ritenuto opportuna la diffusione, avrebbe dovuto individuarle e sbarrare l'accesso solo a quelle porzioni, non a tutto il compendio.

[8] Naturalmente entrambi gli assunti reggono soltanto a patto di prendere sul serio la cernita. In particolare, le parole chiave dovrebbero esprimere, in essenza, il nesso di pertinenza tra informazioni che si cercano e l'oggetto delle indagini. Non mancano però casi in cui i criteri di ricerca appaiono, quantomeno alle difese, eccessivamente larghi: anziché restringere il campo e prevenire abusi, manovre di questo tipo renderebbero inutile il passaggio, a quel punto poco selettivo. Il lavoro manuale delle parti lieviterebbe e l'esigenza di concentrare gli sforzi su temi d'indagine preselezionati sarebbe vanificata. V., per esempio, Cass., Sez. VI, 22 settembre 2020, Aleotti, cit.; attestano lo stesso fenomeno nella giurisprudenza lussemburghese K. Ligeti-G. Robinson, *The Handling of Digital Evidence in Luxembourg,* in M. Caianiello-A. Camon, *Digital Forensic Evidence*, cit., p. 149.

La Corte europea dei diritti dell'uomo ha innanzitutto escluso l'utilità dei precedenti elaborati in materia di prove formate al di fuori del contraddittorio, nascoste alla difesa per ragioni di sicurezza della fonte o di ordine pubblico[9]: per comune ammissione delle parti, tutto il materiale poi utilizzato per discutere la causa era stato messo a disposizione degli imputati e, nel corso del processo, non si era mai fatto riferimento ad altro. La controversia, insomma, non riguardava il diritto a conoscere ed esprimersi sulle prove presentate al giudice, ma l'eventuale diritto a cercarne, estraendole da una miniera di materiale indeterminato.

Prendendo atto dei bisogni operativi degli investigatori, la Corte s'è soffermata sul loro metodo di lavoro: nell'ambito di un'indagine digitale di tale complessità, è inevitabile che la massa di dati grezza, così come raccolta, contenga elementi che nulla hanno a che vedere con il caso; è dunque normale che gli agenti cerchino di scartare ciò che non serve, riducendo il fascicolo a dimensioni almeno gestibili. In questa fase, ha affermato la Corte, sarebbe opportuno, almeno in linea di massima, coinvolgere anche la difesa, in modo che i criteri di selezione dei dati siano condivisi. L'affermazione è importante; vedremo che sarà smorzata, ma vale la pena guardarla più da vicino. Il collegio non si è spinto fino a postulare il diritto d'accesso a tutto il materiale raccolto dall'accusa, ma sembra aver proiettato il principio della parità delle armi su una dimensione nuova. Normalmente, infatti, la nozione è riferita alla possibilità di presentare i propri argomenti davanti al tribunale, in condizioni che non mettano una parte in conclamato svantaggio rispetto all'altra: non si tratta di stabilire precisi equilibri durante le indagini, ma della pari opportunità di convincere il giudice che pronuncerà sentenza. Qui, invece, la Corte sembra collocare la necessità anche "a monte": se la cernita fosse fatta unilateralmente, senza controlli e senza dare alla controparte occasione di partecipare, l'articolo 6 § 1 Conv. e.d.u. ne uscirebbe leso.

La Corte e.d.u., però, non ha portato il principio alle sue estreme conseguenze, anzi: lo ha moderato con due considerazioni. Innanzi tutto, dice la decisione, si può chiedere alla difesa di motivare la propria richiesta, e si può far sì che le ragioni addotte siano vagliate dalle corti nazionali. Una generica richiesta d'accesso all'intero archivio si tradurrebbe in una "spedizione aleatoria" che non può essere legittimata, né

[9] Tali principi sono stati di recente compendiati da Corte e.d.u., 23 maggio 2017, Van Wesenbeeck c. Belgio. Per una disamina della giurisprudenza precedente v. S. ALLEGREZZA, *La conoscenza degli atti nel processo penale*, cit., p. 149 ss.

la parità delle armi risulta automaticamente compromessa da un eventuale diniego: in questo caso, ad esempio, il pubblico ministero non aveva perfetta cognizione di tutto il materiale; gli era noto il contenuto degli stessi documenti sottoposti alla difesa e, quindi, non si trovava in una posizione di vantaggio. I dati non prodotti, secondo la motivazione, erano più affini a oggetti mai sequestrati che non a elementi sottratti alla *discovery* «in senso tradizionale».

L'assetto che la decisione tratteggia non è del tutto cristallino, anzi: la Corte pare affermare allo stesso tempo due cose diverse, non del tutto compatibili tra loro. Da un lato, sembra chiedere alle autorità investigative di tessere un dialogo anticipato non tanto per definire i modi d'accesso al materiale, ma per accordarsi sui filtri da applicare: la signoria sull'archivio resterebbe dell'accusa, che dovrebbe confrontarsi con la difesa per stabilire un metodo d'esame condiviso – per esempio: una lista comune di parole chiave, un ambito temporale determinato in cui concentrare le ricerche, un elenco di persone di cui studiare la corrispondenza, e così via. D'altro canto, però, la medesima sentenza percorre una strada alternativa: la difesa deve giustificare le proprie richieste; o fornisce specifici motivi per cui è ragionevole farla accedere ai dati, o può restare alla finestra: tollererà un'asimmetria di potere che però non si produce necessariamente uno svantaggio cognitivo.

Non è chiaro, insomma, chi debba prendere l'iniziativa: è il pubblico ministero che deve aprire la conversazione con i difensori o, al contrario, sono questi ultimi a dover sollecitare approfondimenti specifici? Quando dovrebbero avvenire gli scambi? Dinanzi a quale organo? Sono temi delicati su cui la Corte e.d.u. ha preferito non prendere posizione.

4. *Segue*. Cooperazione e controllo

Eppure, dalla pronuncia possono scaturire spunti interessanti a patto di riordinare il quadro e precisarne meglio la premessa maggiore: nulla vieta agli investigatori di fornire alla difesa tutto il materiale prelevato, rilevante e irrilevante. Se l'accusa, anzi, mettesse a disposizione tutti i dati, incontrerebbe l'approvazione di un nutrito filone giurisprudenziale della stessa Corte e.d.u. che, in casi non dissimili, ha riconosciuto il diritto della difesa di accedere anche agli elementi privi di valore probatorio «in senso stretto, in quanto non può essere limitato a ciò che la sola accusa considera rilevante. La nozione copre piuttosto tutto il

materiale che è nel possesso delle autorità e che sia dotato di rilevanza potenziale, anche se non esaminato o non ritenuto pertinente»[10]. L'accesso completo, insomma, dovrebbe essere la modalità "di default", tanto che l'imposizione di barriere del tutto arbitrarie costituirebbe un rifiuto delle facilitazioni necessarie alla preparazione del processo e, quindi, una violazione dell'art. 6 § 3 lett. *b* Conv. e.d.u.[11].

Essa, però, non costituisce un percorso obbligato: abbiamo visto che la Corte e.d.u. ha ratificato anche scelte diverse; si tratta insomma di capire quando e a che condizioni tali alternative siano sostenibili. Sui dettagli, il collegio di *Sigurður Einarsson* c. Islanda si è spaccato: l'opinione dissenziente parteggiava per l'applicazione del test più severo, cioè quello utilizzato dalla Corte e.d.u. per stabilire se un processo possa equo quando determinate prove siano state assunte escludendo deliberatamente la difesa[12]. Secondo tale schema, ogni restrizione dovrebbe essere motivata dal bisogno di salvaguardare un diritto fondamentale altrui o un importante interesse pubblico – per esempio: la tutela dell'incolumità di un testimone o la sicurezza nazionale – e sarebbe legittima solo se strettamente necessaria. Se si applicasse la stessa misura alla *discovery* digitale, quindi, dovrebbe essere consegnato alla difesa ogni byte che non fosse indispensabile sottrarle. La maggioranza dei giudici, invece, ha abbandonato maglie così strette e la posizione, tutto sommato, pare equilibrata: un conto è nascondere alla difesa prove presentate al giudice del dibattimento; altro è limitare l'accesso a un compendio che, per la maggior parte, è destinato comunque a rivelarsi inutile. Applicare lo stesso metro alle due situazioni sarebbe forse esagerato, poco pratico e a tratti addirittura controproducente: gl'inquirenti dovrebbero vagliare tutto il compendio al solo scopo di individuare il materiale che è necessario escludere; i dati irrilevanti dovrebbero essere studiati nonostante non abbiano nessuna pertinenza con il fatto da accertare e i benefici portati dalla ricerca per parole chiave sfumerebbero.

Sembra insomma più saggio lasciare agl'investigatori un margine di manovra più ampio, accettando limitazioni d'accesso a tutte le infor-

[10] Corte e.d.u., 31 luglio 2019, Rook c. Germania, § 58.

[11] In questo senso v. Corte e.d.u., 31 luglio 2019, Rook c. Germania, § 58; Corte e.d.u., 8 dicembre 2009, Janatuinen c. Finalndia, § 45; Corte e.d.u., 31 marzo 2009, Natunen c. Finlandia, § 42-43, che, come pure il caso precedente, aveva a che fare con intercettazioni selezionate unilateralmente dagl'inquirenti e poi distrutte così come previsto dalla legge finlandese. In entrambe le occorrenze, la Corte dichiarò la violazione dell'art. 6 § 1 e 6 § 3 lett. *b* Conv. e.d.u.

[12] Opinione dissenziente del giudice Pavli a Corte e.d.u., 4 giugno 2019, Sigurður Einarsson c. Islanda, § 4.

mazioni prelevate anche sulla base di una generica quanto condivisibile preoccupazione per la riservatezza altrui. In definitiva, il perimetro della *discovery* digitale dipende, almeno in prima battuta, dalla leale collaborazione tra accusa e difesa: se la natura del materiale e le circostanze del caso permettessero la serena condivisione dei dati, la procura dovrebbe consentire alla difesa d'accedere senza ulteriori mediazioni; se, al contrario, la situazione fosse più delicata, gl'investigatori potrebbero a buon diritto mostrarsi più circospetti.

Perché le precauzioni degl'inquirenti non si risolvano in una problematica selezione unilaterale – o peggio: in un mero esercizio d'arbitrio – dovrebbero essere predisposti contrappesi adeguati: le prese di posizione della Corte e.d.u. in *Sigurður Einarsson*, se considerate singolarmente e risistemate, offrono suggerimenti preziosi. Un'affermazione in particolare merita d'essere presa sul serio: se la difesa non potesse prendere visione del materiale in maniera indipendente, dovrebbe almeno poter contribuire alla scelta i criteri secondo cui vagliare il materiale. La discrezionalità nella scelta del metodo resterebbe in mano agl'investigatori, senza implicare però una totale mancanza di trasparenza: i termini di ricerca potrebbero essere stabiliti in maniera condivisa o, se non altro, l'indagato saprebbe dall'inizio dell'opzione strategica della controparte e potrebbe organizzarsi di conseguenza[13]. L'incontro tra contendenti potrebbe essere poi valorizzato al meglio se fosse sfruttato per accordarsi anche su altri aspetti: le parti potrebbero stabilire un calendario condiviso, dandosi scadenze di massima per la consegna del materiale rilevante; esse potrebbero poi stabilire un formato in cui preferiscono lavorare, disinnescando fin dal principio un buon numero di potenziali complicazioni.

Accusa e difesa potrebbero quindi collaborare e gestire la *discovery* in maniera autonoma. Se la concordia non fosse totale, però, sarebbe

[13] Una soluzione simile è raccomandata in Gran Bretagna dalle linee guida emesse dal *Attorney General Office*: la polizia giudiziaria stabilisce una strategia insieme al pubblico ministero, messa per iscritto in un *disclosure management document* (*DMD*); esso sarà inoltrato alla difesa e al tribunale. Oltre ciò, gli stessi standard stabiliscono che la controparte debba essere coinvolta «nella definizione del raggio delle ricerche che possono ragionevolmente essere condotte sul materiale digitale, allo scopo di identificare materiale che potrebbe ragionevolmente indebolire l'ipotesi d'accusa o essere d'aiuto alla difesa»: *Attorney General's Guidelines on Disclosure*, cit., p. 26. Il documento prosegue indicando che gli agenti, una volta compilata una lista delle parole chiave che intendono utilizzare, dovrebbero chiedere alla difesa di individuare «altri termini di ricerca ragionevoli», cioè apparentemente capaci di intercettare materiale rilevante; termini troppo ampi, che evidenzierebbero anche una grande quantità di informazioni irrilevanti, potranno essere esclusi.

auspicabile l'intervento di un giudice: se l'attività di spoglio degl'inquirenti fosse insoddisfacente; se i tempi previsti non fossero rispettati; se l'indagato volesse chiedere l'accesso all'intero archivio a dispetto delle scelte iniziali degl'investigatori, dovrebbe esserci un soggetto terzo e imparziale da investire delle questioni. L'interessato dovrebbe a quel punto mostrare come le scelte della controparte gli stiano impedendo di preparare al meglio la propria difesa. Idealmente, un controllo simile dovrebbe collocarsi prima dell'inizio del processo, in modo da affrontare le questioni in tempo utile ed evitando, per quanto possibile, intoppi nelle fasi successive. La Corte e.d.u., ad ogni modo, non si è mostrata rigida sul limite temporale: l'art. 6 § 3 lett. *b* tollera anche soluzioni posticipate, purché la difesa possa ragionevolmente familiarizzare col materiale in tempo utile per la decisione[14].

5. Quali facilitazioni?

Poniamo che la difesa riesca a ottenere una copia integrale dei dati prelevati. Le difficoltà che abbiamo appena descritto sarebbero superate, ma non ci troveremmo comunque davanti a uno scenario del tutto libero da asimmetrie: il tema della parità delle armi tornerebbe ad affacciarsi seguendo percorsi diversi, quasi rovesciati rispetto a quelli esaminati fin qui. Se la selezione unilaterale del materiale rilevante limita eccessivamente gli orizzonti della difesa, la condivisione dell'intero archivio potrebbe allargarli troppo: esplorare tutto con scrupolo sarebbe difficile, specie per un professionista che non è necessariamente organizzato per quel tipo di lavoro[15]. Se non gli si fornisse alcun aiuto, l'accesso al compendio integrale si rivelerebbe perfino svantaggioso rispetto a una cernita unilaterale "garantita": su grossi volumi, incappare rapidamente in dati utili sarebbe improbabile; trovare anche solo la cartella in cui potrebbe celarsi qualche elemento interessante potrebbe richiedere settimane di lavoro. Di fatto, la selezione finirebbe per essere parziale

[14] Corte e.d.u., 31 luglio 2019, Rook c. Germania, § 73.

[15] Come accennato (v. *supra*, § 2), le distanze con l'accusa si ridurrebbero se le risorse messe a disposizione dall'indagato permettessero di assumere un consulente tecnico: il fardello sarebbe scaricato su uno specialista, formato e attrezzato per svolgere ricerche. Se però l'indagato non potesse permettersi una simile integrazione del collegio difensivo, torneremmo ai blocchi di partenza: da una parte l'accusa, ben equipaggiata; dall'altra il difensore, schiacciato da una *discovery* troppo pesante.

quanto prima, troncando per di più sul nascere ogni possibile lamentela della difesa, cui è stato riconosciuto il massimo accesso possibile.

Da una considerazione simile muove gran parte del dibattito statunitense, più preoccupato dalla sistematica *disclosure* dell'intero archivio che non dalle omissioni delle procure. In quell'ordinamento, del resto, la legge non chiede all'accusa di mostrare tutte le carte, anzi: la regola del "fascicolo aperto" è del tutto recessiva. Il dovere di rivelazione degli atti d'indagine si estende soltanto a ciò che si intende presentare al giudice, nonché agli elementi che possono essere considerati favorevoli all'imputato[16]: normalmente, quindi, la difesa accede a un compendio altamente selezionato, che le permette di comprendere la strategia dell'avversario e lavorare di conseguenza[17]. Il digitale, però, ha complicato lo scenario: realisticamente, il procuratore non riuscirà a cercare, nel pagliaio, l'ago che anche solo per ipotesi potrebbe essere utile alla difesa; per non incorrere nella violazione dei suoi doveri istituzionali, allora, rivela tutto, lasciando all'imputato il compito di sbrogliare la matassa e trovare ciò che può essere rilevante. Più che essere vista e percepita come un diritto, la possibilità di rovistare in tutte le memorie informatiche sequestrate è quindi vissuta come un passo indietro, se non proprio come una strategia elusiva o una «trappola»[18]. Alcuni autori, in quel contesto, hanno quindi provato a riaffermare la necessità di una selezione attenta: la tecnologia è mutata, ma i doveri costituzionali che gravano sull'accusa no. Gli investigatori avrebbero dunque l'onere di setacciare tutto il materiale, in modo da poter sottoporre alla controparte gli elementi potenzialmente rilevanti[19]: aiutare la difesa significherebbe studiare il contenuto di ogni file. Una richiesta simile nelle

[16] È il contenuto della celebre dottrina *Brady*, affermata dalla Corte suprema in Brady v. Mayland, 373 U.S. 83, 1963: «the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution». La giurisprudenza successiva ha poi avuto modo di affinare la nozione trasformandola innanzitutto in un obbligo della parte pubblica, indipendentemente dalle richieste di parte: United States v. Agurs, 427 U. S. 97, 1976; United States v. Bagley, 473 U. S. 667, 1985.

[17] Si tratta di un contrappeso alla strutturale superiorità dei mezzi della pubblica accusa: v. U.S. v. Tavera, 719 F.3d 705, 6 Cir., 2013, II.A.

[18] L'espressione è di A. Camon, *The Project DEVICES and Digital Evidence in Europe*, in M. Caianiello-A. Camon, *Digital Forensic Evidence*, cit., p. 5. Per un'efficace illustrazione di tale prospettiva, v. H. Oran, *Does* Brady *Have a Byte? Adapting Constitutional Disclosure for the Digital Age*, in *Columbia Journal of Law and Social Problems*, vol. 50 (2016), f. 1, p. 98 ss.

[19] Sposa la tesi del «new medium, same rule» H. Oran, *Does* Brady *Have a Byte?*, cit., p. 129 ss.

implicazioni, pur partendo da una situazione di fatto capovolta[20], è stata avanzata anche nel caso *Sigurður Einarsson*: i difensori del ricorrente avevano chiesto al procuratore di escludere solo il materiale segreto a fornire tutto il resto o, in alternativa, di produrre almeno un riassunto dei contenuti del materiale ritenuto irrilevante. Per accontentare la controparte, gl'inquirenti avrebbero dovuto scrutinare tutto, così da poter identificare i frammenti da oscurare o poter riferire sui contenuti.

Al fondo delle tesi si rintraccia la stessa nozione: per rendere equo il processo, occorre che tutti i dati siano sondati e, singolarmente, siano conservati o esclusi; il peso dell'operazione non potrebbe che cadere sulla parte meglio strutturata per condurre un lavoro di questo tipo, ovvero la pubblica accusa. La linea, comprensibilmente, ha incontrato una ferma opposizione: il carico di lavoro sarebbe enorme, e non è detto porterebbe a risultati soddisfacenti; per presentare una sintesi utile o per rinvenire elementi a discarico, gli agenti dovrebbero prendere familiarità con buona parte delle informazioni raccolte – giova ripeterlo: molte delle quali irrilevanti. Inoltre, gli organi di accusa potrebbero non avere la giusta sensibilità per valorizzare le sfumature più favorevoli alla difesa, che potrà avvalersi anche delle conoscenze e delle indicazioni confidenziali del diretto interessato per offrire una ricostruzione alternativa degli eventi. Per questo, gli standard delle autorità investigative[21], diverse decisioni[22] e non pochi studiosi[23] hanno respinto l'opinione; anche la Corte e.d.u. se ne è distaccata, condividendo i dinieghi dei giudici islandesi.

Una strada più proficua, forse, potrebbe passare da una riflessione sugli strumenti dello scrutinio più che sull'attività in quanto tale: se la

[20] Come abbiamo visto, i presupposti del caso sono diversi: la difesa non doveva navigare una mole eccessiva di materiale, anzi: voleva accedervi.

[21] V. *Attorney General's Guidelines on Disclosure*, cit., p. 31: «l'accusa non ha il dovere di esaminare tutto il materiale in suo possesso alla ricerca di qualunque cosa possa […] indebolire l'accusa o favorire la difesa. L'accusa ha il dovere di produrre il materiale che può indebolire l'accusa o favorire la difesa di cui è venuta a conoscenza, o su cui la sua attenzione è stata diretta».

[22] Tra le numerose affermazioni, basti qui riportare quella – perentoria – che si legge in United States v. Ohle, S3 08 CR 1109, S.D. New York, 2011: «Placing a higher burden on the Government to uncover such evidence would place prosecutors in the untenable position of having to prepare both sides of the case at once. Indeed, the adversarial system presumes that the defense will be more highly motivated to uncover exculpatory evidence […] considering that, if exculpatory evidence exists, the defense is in the best position to know what such evidence might be and where it might be located».

[23] V. J.I. Turner, *Managing Digital Discovery in Criminal Cases*, in *Journal of Criminal Law and Criminology*, vol. 109 (2017), f. 2, p. 301 cui si rinvia anche per ulteriori riferimenti dottrinali.

difesa avesse modo di svolgere analisi autonome, agevolata da programmi informatici paragonabili a quelli del pubblico ministero, le difficoltà d'orientamento si diraderebbero. La giurisprudenza statunitense procede spedita in quella direzione: per soddisfare i propri doveri, il pubblico ministero non può limitarsi ad aprire il fascicolo e lasciare che l'imputato trovi gli elementi che più gl'interessano; deve condividere dati su cui si possano svolgere ricerche mirate[24]. Sul fronte europeo, la Corte e.d.u. ha avuto modo di dare qualche direttiva nella pronuncia *Rook* c. Germania, di cui gioverà occuparsi brevemente.

Nell'ambito di un procedimento che vedeva nove indagati per corruzione in rapporti commerciali, la polizia tedesca aveva sequestrato quattordici milioni di file contenuti in vari dispositivi personali e aziendali. Ancora una volta, gl'inquirenti avevano filtrato il materiale rilevante tramite un software, individuando poco più di mille documenti utili, che venivano stampati e messi a disposizione delle parti. L'insieme di dati, ad ogni modo, era rimasto nella caserma della polizia giudiziaria: le difese avrebbero potuto esaminarlo indicando le parole chiave desiderate; gli agenti avrebbero condotto una ricerca e caricato il materiale su un dispositivo riservato alla consultazione. In seguito, uno degli avvocati del ricorrente aveva chiesto una copia di tutte le informazioni sequestrate e, una volta ottenuta, si rendeva conto del fatto che l'archivio poteva essere letto solo tramite lo stesso programma usato dalla polizia, disponibile sul mercato per poco più di € 4.000. Egli aveva chiesto al tribunale regionale che gli fosse fornita gratuitamente una licenza. I giudici tedeschi rispondevano che sarebbe stato un dovere assistere la difesa qualora, per accedere ai file, essa avesse dovuto sostenere spese spropositate, se essa non fosse stata in grado di avanzare la somma o se il software non fosse stato reperibile. Nel caso concreto, però, nessuna di queste condizioni sembrava ricorrere: l'imputato era assistito da tre difensori; la spesa per procurarsi l'applicativo sembrava quindi relativamente contenuta, ben entro la portata finanziaria dell'interessato. La polizia, ad ogni modo, aveva poi consegnato alla difesa un'altra copia della collezione, tradotta in un formato leggibile tramite programmi a licenza gratuita.

[24] Sul punto, basti qui rinviare a E.H. HOLDER, *In the Digital Age, Ensuring That the Department Does Justice*, in *Georgetown Law Journal – 41st Annual Review of Criminal Procedure*, 2012, p. viii ss. e giurisprudenza ivi citata.

La Corte e.d.u. ha ritenuto che un simile modo di procedere fosse del tutto compatibile con le garanzie della Convenzione e, forse, potremmo trarre qualche insegnamento più generale: se le autorità decidessero di consegnare tutti i dati alla difesa, non dovrebbero costringerla al lavoro che loro rifuggono, e cioè lo spoglio manuale, byte per byte. Dovrebbero quindi far sì che il materiale trasmesso sia leggibile e navigabile: il difensore dovrebbe essere in grado di condurre ricerche senza troppo aggravio. Se l'operazione richiedesse necessariamente strumenti tecnici costosi e avanzati, il dovere d'assistenza delle autorità sarebbe da graduare in base alle possibilità economiche del diretto interessato. Come accennato, la distanza tra le parti si ridurrebbe se le risorse messe a disposizione dall'indagato permettessero di assumere un consulente tecnico: il fardello sarebbe scaricato su uno specialista, formato e attrezzato per svolgere ricerche. Se però l'indagato non potesse permettersi una simile integrazione del collegio difensivo o se i mezzi per esaminare i materiali fossero irragionevolmente costosi, la pubblica accusa potrebbe condividere le proprie strutture, offrendosi, per esempio, d'isolare il materiale che reca i termini di ricerca individuati dalla difesa.

6. Conclusioni

Dalle vicende che abbiamo riassunto emerge un tratto comune: quando il volume d'informazioni è umanamente inaffrontabile, le dinamiche della *discovery* meritano di essere riconsiderate. L'impersonale deposito del fascicolo, in quelle condizioni di lavoro, non è sufficiente: se esso contenesse tutto, rischierebbe di paralizzare la difesa dell'imputato, specie se non facoltoso; se esso includesse solo i frammenti scelti dal pubblico ministero, la difesa avrebbe probabilmente difficoltà a procurarsi ciò che serve a presentare una ricostruzione alternativa al giudice.

Da questo paradosso, la prassi tende a uscire innanzi tutto tramite il dialogo tra le parti: la leale collaborazione, almeno potenzialmente, potrebbe sciogliere parecchi nodi di metodo, di calendario e di formato. Ciò però non significa che accusa e difesa, debbano essere lasciate sole, anzi: i loro accordi guadagnerebbero in equità e trasparenza se la conversazione partisse da presupposti chiari e si svilup-

passe in sedi e in tempi stabiliti, con la possibilità di chiamare in causa garanti imparziali[25].

Le corti statunitensi, pur muovendo da diverse premesse, hanno già avuto modo di dettare regole più avanzate; sull'onda di quell'evoluzione, anche i testi normativi sono stati aggiornati[26]. Gli ordinamenti europei sembrano presentare tempi di reazione più lenti: a maggior ragione, la Corte di Strasburgo avrebbe potuto fare da apripista e spronare legislatori e interpreti. Essa, però, non ha sfruttato fino in fondo le occasioni che le sono finora state offerte: non ha mai tentato di dettare uno statuto completo della *discovery* digitale pienamente compatibile con i diritti garantiti dalla Convenzione; si è limitata a giocare di rimessa, ratificando gli atteggiamenti virtuosi e censurando a parole le prassi meno trasparenti. Anche le dichiarazioni più utili e coraggiose sono state stemperate in passaggi motivazionali imprecisi, poco chiari quanto a oggetto e scopi e, infine, neutralizzate dalla valutazione dell'equità del procedimento "nel suo complesso", ormai consueta quanto criticata[27].

La vicenda della *discovery* digitale, insomma, sembra confermare una diagnosi già formulata in termini più generali[28]: anche in questo settore, pare che la Corte europea abbia deciso di abdicare al ruolo di

[25] Pur cercando soluzioni a un problema parzialmente diverso, la dottrina di lingua italiana ha avanzato varie proposte, come quella di svolgere lo scrutinio del materiale in incidente probatorio (F. IOVENE, *Perquisizione e sequestro di computer: un'analisi comparatistica*, in *Riv. dir. proc*., 2012, p. 1616) o di istituire un'apposita udienza di selezione (L. BARTOLI, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen. (web)*, 2018, p. 18; S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati*, in *Dir. pen. proc*., 2008, p. 481; L. LUPARIA, Computer crimes *e procedimento penale*, in *Modelli differenziati d'accertamento*, a cura di G. GARUTI, in *Trattato di procedura penale*, diretto da G. SPANGHER, vol. VII, t. 1, UTET, Torino 2011, p. 375; G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *Cass. pen.*, 2016, p. 306).

[26] In particolare, è stata aggiunta una disposizione alle *Federal Rules of Criminal Procedure*, la n. 16.1, che obbliga le parti a incontrarsi non oltre 14 giorni dopo la contestazione dell'imputazione per trovare un accordo sugli aspetti salienti della *discovery*; esse potranno rivolgersi al giudice per chiedere modifiche o per sollecitare una decisione sui profili controversi.

[27] Per un recente consuntivo, v. A. BOLDRIN, *Approccio compensativo e* overall fairness *nella giurisprudenza della Corte EDU, tra relativismo delle garanzie e altre derive*, in *Leg. pen. (web)*, 26 ottobre 2021. L'opinione dissenziente del giudice Pavli a Corte e.d.u., 4 giugno 2019, Sigurður Einarsson c. Islanda, § 28 ha fortemente criticato tanto gli argomenti, incluso l'impiego indiscriminato del criterio della equità del caso nel suo complesso, tanto il generale atteggiamento elusivo a suo avviso adottato dalla maggioranza del collegio.

[28] M. CAIANIELLO, *You Can't Always Counterbalance What You Want*, in *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 25 (2017), f. 4, p. 283 ss.

avanguardia che un tempo rivendicava; se si esaspera l'approccio caso per caso e se si ammettono fattori compensativi capaci di rimediare a (quasi) qualsiasi violazione[29], la giurisprudenza nel suo insieme non potrà che risultare ambivalente, incapace d'esprimere equilibri univoci. L'opera di razionalizzazione degli interpreti, dunque, appare più che mai preziosa: da una serrata analisi dell'attuale possono scaturire non solo utili istruzioni operative, ma anche innesti più duraturi e meditati, capaci di risolvere i rebus della prova digitale.

[29] Fanno eccezione soltanto le violazioni all'art. 3 Conv. e.d.u., costantemente e severamente riconosciute inaccettabili e, quindi, non bilanciabili: Corte e.d.u., 5 novembre 2020, Ćwik c. Polonia. Per una lettura ordinata del fenomeno v. A. CABIALE, *I limiti alla prova nella procedura penale europea*, CEDAM, Padova 2019, p. 133 ss.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464306
pp. 101-113 (gennaio 2022)

Data retention, tra diritto alla protezione dei dati personali ed esigenze di accertamento dei reati

SILVIA SIGNORATO[1]

1. Informazioni digitali

Il fatto che la «giustizia umana non possa fondarsi sulla certezza del conseguimento della verità […], non vuol dire che si possa prescindere dall'operare il massimo sforzo per cercare di conseguirla»[2]. In questa prospettiva, un ruolo centrale rivestono gli elementi di prova e le prove. Se questi ultimi, nell'impostazione originaria del codice di procedura penale[3], si connotavano tendenzialmente per materialità, a fronte dell'uso sempre più diffuso di sistemi informatici e telematici[4], si è delineata invece la possibilità investigativa di acquisire elementi di prova e prove immateriali[5], digitali, che presentano caratteristiche strutturali differenti rispetto alle *evidence* materiali[6]. Tali specifiche caratteristiche si riverberano nella peculiarità delle indagini digitali[7], le quali devono essere in

[1] Professore associato di Diritto processuale penale nell'Università degli Studi di Padova. *Lecturer* di Diritto processuale penale nell'Università di Innsbruck.

[2] In questi termini, G. GIOSTRA, *Prima lezione sulla giustizia penale*, Editori Laterza, Bari-Roma 2020, p. 7.

[3] Il codice di procedura penale vigente è stato approvato con d.p.r. 22 settembre 1988, n. 447.

[4] Tanto che la distinzione tra *on line* ed *off life* sembra perdere sempre più la sua importanza, nella direzione di una dimensione *on life*. Al riguardo, cfr. L. FLORIDI (a cura di), The Onlife Manifesto. Being Human in a Hyperconnected Era, Cham, 2015.

[5] In ambito giuridico il concetto di «materia» viene tradizionalmente ricollegato alla possibilità di percezione tattile, che non si delinea a fronte di elementi di prova digitali. Infatti, ciò che potrà essere toccato sarà il supporto che contiene i dati, ma non il dato digitale in sé. Altro discorso è invece che, da un punto di vista prettamente fisico, anche i dati digitali possano essere qualificati in termini di «materia».

[6] Al riguardo, cfr. M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.,* 2011, p. 283 ss.

[7] Tale tipologia investigativa si connota per caratteristiche particolari, tali da incidere sulla stessa sistematica del processo penale. Per un approfondimento al riguardo, cfr., volendo, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018. Va rile-

grado di non alterare gli elementi di prova digitali[8] che, a causa della loro immaterialità, sono invece facilmente modificabili o volatili. Inoltre, non bisogna dimenticare come tali *evidence* svolgano non di rado un ruolo cruciale nell'ambito di un procedimento penale. Si pensi solo all'importanza accertativa che possono rivestire *email*, messaggi telefonici o scambiati in *chat* o, ancora, *post* inseriti in *social network*. Senza contare il novero degli elementi di prova digitali rinvenibili in conseguenza dell'impiego dell'*Internet of things.*

Se nessuno dubita che simili elementi di prova digitali, nel rispetto delle garanzie, possano essere acquisiti a seguito della commissione di un reato, più problematica appare invece la possibilità di conservare taluni dati *prima* della commissione di un reato, a prescindere dalla sua commissione e dal soggetto a cui si riferiscono, per fini di prevenzione e di accertamento.

Al riguardo, si può rilevare come la possibilità per gli investigatori di disporre di un ampio bacino di informazioni possa senz'altro contribuire all'efficacia investigativa[9]. Tuttavia, si tratta di comprendere come, quando e in che quantità tali informazioni possano essere legittimamente acquisite.

Da un lato, infatti, la tecnologia digitale ha ampliato le possibilità di trattamento[10] di dati[11]. Dall'altro lato, però, vi è il rischio che il mo-

vato come le indagini digitali possano essere marcatamente lesive dei diritti fondamentali, come accade a fronte dell'impiego del captatore informatico, per i cui aspetti tecnici si rinvia a R. BRIGHI, *Requisiti tecnici, potenzialità e limiti del captatore informatico. Analisi sul piano informatico-forense*, in G. GIOSTRA- R. ORLANDI, *Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie informatiche,* Giappichelli, Torino 2021.

[8] «A tale fine, l'obiettivo dell'informatica forense è costituito dallo studio delle tecniche per l'individuazione, acquisizione. conservazione, analisi e valutazione dei dati prodotti da un sistema informatico o telematico senza alterarli». In questi termini, C. MAIOLI, *Questioni di informatica forense,* Aracne, Ariccia 2015, p. 16.

[9] Naturalmente, purché tali informazioni siano corrette e adeguatamente selezionate. Va rilevato come, con specifico riguardo al principio della correttezza nel trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, l'art. 4 direttiva (UE) 2016/680 (cd. direttiva *law enforcement*) preveda espressamente il principio della correttezza nel trattamento dei dati.

[10] Ai sensi dell'art. 3 n. 2 della direttiva (UE) 2016/680 per «trattamento» si intende «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

[11] Si pensi solo all'impiego delle videoriprese per la sicurezza delle città. Per una riflessione sul tema, cfr. EUROPEAN FORUM FOR URBAN SECURITY, *Cittadini, città e videosorveglianza*, Stipa, Montreuil 2010.

nitoraggio delle persone si trasformi in «capitalismo della sorveglianza»[12] o schiuda scenari da panopticon[13] idonei a determinare significative compressioni dei diritti fondamentali e, in fondo, un *vulnus*, alla stessa dignità dell'uomo, attraverso la reificazione di quest'ultimo, ricondotto a mero insieme di dati[14].

Nella problematica della difficile armonizzazione tra logiche securitarie ed esigenze di tutela del diritto alla protezione dei dati personali si inserisce il tema della possibilità che i fornitori di servizi telefonici e telematici, per finalità di prevenzione e di accertamento dei reati, conservino i dati relativi alle comunicazioni telefoniche e telematiche di chiunque, per il solo fatto che venga effettuata una comunicazione e, quindi, a prescindere dalla circostanza che chi comunica commetta o non commetta reati.

2. La ricerca di un punto di equilibrio in materia di *data retention*

La locuzione *data retention* indica la disciplina che, per finalità di accertamento e repressione dei reati, prevede in capo ai fornitori di comunicazione elettronica obblighi di conservazione di taluni dati per predeterminati archi temporali. Tali obblighi non derivano da un provvedimento dell'autorità giudiziaria, ma vengono previsti direttamente dalla legge. Inoltre, essi sussistono per il solo fatto che venga effettuata una comunicazione, a prescindere dai soggetti che comunicano.

A livello globale, emerge la difficoltà di trovare un punto di equilibrio nel dettare una disciplina in tema di *data retention*, che riesca a bilanciare in modo armonico le esigenze securitarie con quelle di rispetto dei diritti fondamentali.

[12] Cfr. S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, tradotto da P. Bassotti, Luiss University Press, Roma 2019.

[13] Al riguardo, si rinvia a M. FOUCAULT – M. PERROT (a cura di), Jeremy Bentham. *Panopticon ovvero la casa d'ispezione*, IV ed., Marsilio, Venezia, 2001.

[14] Una volta che «la persona si pone come una "entità disincarnata", ne consegue l'esigenza di tutelarne il "corpo elettronico". In questi termini, si sente il bisogno di una sorta di "habeas corpus", nella forma di un "habeas data", configurabile come l'evoluzione del nucleo dal quale storicamente si è sviluppata la libertà personale». Così, L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali,* in ASSOCIAZIONE TRA GLI STUDIOSI DEL PROCESSO PENALE, *Diritti della persona e nuove sfide del processo penale,* Giuffrè Francis Lefevre, Milano 2019, p. 211, nonché S. RODOTÀ, *Il mondo della rete. Quali vincoli, quali diritti*, Laterza, Roma 2014, p. 30.

In questa prospettiva, a livello europeo, si è cercato di individuare almeno due punti fermi.

Anzitutto, al fine di salvaguardare quantomeno la libertà e la segretezza delle comunicazioni, viene sempre vietata la conservazione del contenuto comunicativo[15]. È quindi consentita la conservazione dei soli dati esterni alle comunicazioni, quali numero telefonico del chiamante, identificativo dell'utente, dati necessari per individuare la data, l'ora e la durata di una comunicazione, data e ora del *log-in* e del *log-off*, ecc.[16].

[15] In tema, cfr. Corte cost. 11 marzo 1993, n. 81, nonché N. GALLO, *L'acquisizione del traffico telefonico nelle indagini di polizia*, in *Riv. di polizia*, II, 2008, p. 73 ss.

[16] Più specificamente, le categorie di dati che possono essere conservate coincidono con quelle indicate all'art. 5 dell'abrogata direttiva 2006/24/CE. Si tratta anzitutto dei «a) dati necessari per rintracciare e identificare la fonte di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero telefonico chiamante; ii) nome e indirizzo dell'abbonato o dell'utente registrato; 2) per l'accesso Internet, posta elettronica su Internet e telefonia via Internet: i) identificativo/i dell'utente; ii) identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica; iii) nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico; b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero/i digitato/i (il numero o i numeri chiamati) e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i; 2) per la posta elettronica su Internet e la telefonia via *Internet*: i) identificativo dell'utente o numero telefonico del/dei presunto/i destinatario/i di una chiamata telefonica via Internet; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i e identificativo del presunto destinatario della comunicazione; c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione; 2) per l'accesso *Internet*, la posta elettronica via Internet e la telefonia via Internet: i) data e ora del *log-in* e del *log-off* del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo *IP*, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato; ii) data e ora del *log-in* e del *log-off* del servizio di posta elettronica su *Internet* o del servizio di telefonia via *Internet* sulla base di un determinato fuso orario; d) i dati necessari per determinare il tipo di comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato; 2) per la posta elettronica Internet e la telefonia *Internet*: il servizio *Internet* utilizzato; e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature: 1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati; 2) per la telefonia mobile: i) numeri telefonici chiamanti e chiamati; ii) *International Mobile Subscriber Identity* (IMSI) del chiamante; iii) *International Mobile Equipment Identity* (IMEI) del chiamante; iv) l'IMSI del chiamato; v) l'IMEI del chiamato; vi) nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (*Cell ID*) dalla quale è stata effettuata l'attivazione; 3) per l'accesso *Internet*, la posta elettronica su *Internet* e la telefonia via *Internet*: i) numero telefonico chiamante per l'accesso commutato (*dial-up access*); ii) *digital subscriber line* (DSL) o un altro identificatore finale di chi è all'origine della comunicazione;

In secondo luogo, nel rispetto del principio di proporzionalità[17], la conservazione dei dati può avvenire solo per archi temporali predefiniti e limitati.

3. La disciplina prevista dall'art. 132 del Codice in materia di protezione dei dati personali.

Sul piano delle fonti interne, la disciplina di *data retention* è prevista dall'art. 132 d. lgs. 30 giugno 2003, n. 196[18] recante il Codice in materia di protezione dei dati personali (cd. Codice *privacy*), il quale, in linea con l'art. 15 Cost.[19], chiarisce anzitutto che non possono essere conservati i contenuti comunicativi, ma solo i cd. dati esterni alle comunicazioni.

Inoltre, la previsione *ex* art. 132 Codice *privacy* fissa una disciplina differenziata circa le tempistiche di conservazione dei dati. In particolare, essa effettua una bipartizione basata sulla tipologia di reato. Da un lato, infatti, si stabiliscono specifici archi temporali di conservazione dei dati per finalità di accertamento e di repressione dei reati diversi da quelli indicati agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera a), c.p.p.; dall'altro lato, si individua un arco temporale più dilatato di conservazione dei dati per finalità di accertamento e di repressione dei reati previsti agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera a), c.p.p. Iniziando dalla conservazione dei dati per il contrasto ai reati differenti da quelli indicati agli articoli 51, comma 3-*quater*, e 407, comma 2,

f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile: 1) etichetta di ubicazione (*Cell ID*) all'inizio della comunicazione; 2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni».

[17] Per un approfondimento di tale principio cfr., *ex multis,* M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Diritto penale contemporaneo. Trimestrale*, 2014, p. 143 ss.; nonché R. ORLANDI, *La riforma del processo penale tra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, p. 1151 ss.

[18] L'art. 132 codice *privacy* rappresenta una norma dalla storia travagliata. In parte riscritto, in parte abrogato, in parte innovato, il testo dell'art. 132, anche per la necessità di allinearne la disciplina alle fonti europee, è stato oggetto di plurimi interventi, ad esempio, da parte del d.l. 24 dicembre 2003, n. 354; del d.l. 27 luglio 2005, n. 144; del d.lgs. 30 maggio 2008, n. 109; del d. lgs. 10 agosto 2018, n. 101; della l. 18 marzo 2008, n. 48; della l. 20 novembre 2017, n. 167; del d.l. 30 settembre 2021, n. 132, così come convertito con modificazioni dalla l. 23 novembre 2021, n. 178.

[19] L'art. 15 Cost. tutela l'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione.

lettera a), c.p.p., in rapporto ad essi, la disciplina *ex* art. 132 codice *privacy* modula in maniera tripartita le tempistiche di conservazione. Tale norma stabilisce infatti che per finalità di accertamento e repressione dei reati, il fornitore debba conservare per ventiquattro mesi i dati relativi al traffico telefonico, per dodici mesi i dati relativi al traffico telematico e per trenta giorni i dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione. Tali tempistiche di conservazione dei dati vengono calcolate a partire dalla data della comunicazione.

In aggiunta, con l'obiettivo di rendere la disciplina di *data retention* conforme al principio di proporzionalità, il legislatore italiano è da ultimo intervenuto in materia[20], subordinando l'acquisizione dei dati a due requisiti, la cui violazione determina l'inutilizzabilità dei dati stessi[21].

Il primo requisito attiene alla tipologia ed alla gravità dei reati. Infatti, l'acquisizione dei dati può avvenire solo se sussistono «sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni[22] […] e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi»[23].

Quanto al secondo requisito, esso richiede che l'acquisizione dei dati sia rilevante all'accertamento dei fatti[24]. Si tratta di una formula che, da un lato, sotto il profilo temporale, lascia aperta la possibilità che la richiesta di acquisizione dei tabulati avvenga in un momento successivo

[20] Il riferimento è alla l. 23 novembre 2021, n. 178 di conversione in legge, con modificazioni, del d.l. 30 settembre 2021, n. 132, recante misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP.

[21] Cfr. art. 132, comma 3 *quater*, d. lgs. 30 giugno 2003, n. 196, così come riformulato dal d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla l. 23 novembre 2021, n. 178.

[22] Determinata a norma dell'art. 4 c.p.p.

[23] Cfr, art. 132, comma 3, d. lgs. 30 giugno 2003, n. 196, così come riformulato dall'art. 1, comma 1, lett. a), d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla l. 23 novembre 2021, n. 178.

[24] Al riguardo, si può rilevare come il d.l. 30 settembre 2021, n. 132 subordinasse invece l'acquisizione dei dati «ai fini della prosecuzione delle indagini». La dottrina non aveva però mancato di rilevare come tale formulazione apparisse imprecisa e limitativa. Infatti, la disciplina faceva riferimento, da un lato, alle indagini e, dall'altro, alla istanza del difensore dell'*imputato*; in secondo luogo, sembrava dimenticare che la necessità di acquisire i dati si può manifestare anche in un momento successivo all'esercizio dell'azione penale. Di qui il *revirement* in sede di conversione e la sostituzione della formula «ai fini della prosecuzione delle indagini» con quella di «rilevante ai fini dell'accertamento dei fatti».

a quello delle indagini preliminari; dall'altro lato, non correla l'acquisizione dei dati alle mere esigenze accusatorie.

a) Focalizzando l'attenzione sulla diversa ipotesi della conservazione dei dati per il contrasto ai delitti consumati o tentati con finalità di terrorismo (articoli 51, comma 3-*quater*) e per il contrasto ai reati *ex* art. 407, comma 2, lettera a), c.p.p., la disciplina di riferimento in materia è rappresentata dall'art. 132, comma 5 *bis*[25] Codice *privacy*. In forza di tale previsione non si applicano i ricordati archi temporali di conservazione dei dati (ventiquattro mesi, dodici mesi, trenta giorni a seconda del tipo di comunicazione), ma, nell'ottica di un efficace contrasto al terrorismo, il periodo di conservazione viene fissato in settantadue mesi a partire dalla data della comunicazione[26]. Al riguardo, va precisato che tale arco temporale di conservazione vale sia per i dati relativi al traffico telefonico, sia per quelli relativi al traffico telematico, sia per i dati relativi alle chiamate senza risposta.

4. *Segue*: questioni problematiche in tema di disciplina italiana della conservazione dei dati di traffico.

La disciplina prevista dall'art. 132 Codice *privacy* non è scevra di aspetti problematici.

Al riguardo, è possibile rilevare anzitutto come una simile previsione appaia in parte anacronistica. In particolare, in riferimento alla conservazione dei dati per il contrasto ai reati differenti da quelli indicati agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera a), c.p.p., non è agevole comprendere come mai i dati relativi al traffico telematico debbano essere trattenuti per un arco temporale corrispondente alla metà di quello previsto per i dati di traffico telefonico, nonostante siano proprio i dati telematici ad essere maggiormente impiegati. Ancora, ci si può chiedere quale sia la ragione alla base della conservazione per soli trenta giorni dei dati relativi alle chiamate senza risposta. In generale, le tempistiche di conservazione (specie quelle relative ai dati di

[25] A seguito della cd. legge europea 2017, tale previsione fa salva la disciplina *ex* art. 24 della legge 20 novembre 2017, n. 1677.

[26] Per una più ampia riflessione sul tema, cfr., volendo, S. Signorato, *Novità in tema di* data retention. *La riformulazione dell'art. 132 codice* privacy *da parte del d.lgs. 10 agosto 2018, n. 101,* in *Diritto penale contemporaneo*, 28 novembre 2018, p. 153 ss.

traffico telematico ed alle chiamate senza risposta) non sembrano tenere conto che, nella realtà, non è raro che la necessità di acquisire i dati emerga quando essi sono ormai stati cancellati, non solo perché la denuncia o querela vengono presentate sovente a distanza di tempo dalla commissione del reato, ma anche perché l'esigenza di acquisizione dei dati potrebbe emergere in un momento di molto successivo a quello in cui è iniziata la conservazione dei dati.

Da un punto di vista sistematico, si delineano poi dei profili problematici in riferimento al campo applicativo delle due diverse discipline in tema di tempistiche di conservazione dei dati, previste dall'art. 132 codice *privacy*.

Come si è già ricordato, il legislatore ha dettato una sorta di doppio binario, apparentemente garantista e rispettoso dl principio di proporzionalità, dato che modula il tempo di conservazione dei dati in rapporto alla gravità del reato da contrastare.

Infatti, da un lato, per il contrasto ai reati *ex* art. 51 comma 3 *quater* c.p.p. e *ex* art. 407 comma 2 lett. a c.p.p., il periodo di conservazione è individuato in settantadue mesi sia per i dati di traffico telefonico, sia per quelli di traffico telematico, sia per i dati relativi alle chiamate senza risposta.

Dall'altro lato, al fine del contrasto ai restanti reati, l'arco temporale di conservazione viene fissato in ventiquattro mesi per i dati relativi al traffico telefonico, in dodici mesi per quelli relativi al traffico telematico e per trenta giorni per i dati relativi alle chiamate senza risposta.

Occorre però rilevare che, nel momento della conservazione dei dati, il fornitore non solo ignora se, in futuro, quei dati gli verranno richiesti dall'autorità giudiziaria, ma gli è pure sconosciuto se tali dati potranno essere richiesti per un reato di terrorismo o per un reato previsto dall'art. 407 comma 2 lett *a* c.p.p. o per un altro reato. Invero, una simile informazione sarà nota al fornitore soltanto in un momento successivo, coincidente con quello in cui avverrà la richiesta dei dati da parte dall'autorità giudiziaria.

Ne deriva l'impossibilità per il fornitore di modulare a monte le tempistiche di conservazione dei dati in rapporto alla tipologia di reato. Tale profilo indebolisce, però, la portata applicativa dell'art. 132 Codice *privacy*, salvo procedere ad un'operazione di ortopedia interpretativa dello stesso. In tale prospettiva, si potrebbe sostenere che la disciplina prevista dall'art. 132 Codice *privacy* comporti l'obbligo per i fornitori di conservare tutti i dati di traffico telefonico, telematico e relativi alle chiamate senza risposta per ben settantadue mesi. Le preclusioni

temporali di dodici, ventiquattro mesi, trenta giorni o settantadue mesi opererebbero infatti a valle, nel momento della trasmissione dei dati all'autorità giudiziaria. Nello specifico, a fronte di una richiesta da parte dell'autorità giudiziaria, il fornitore dovrà verificare quale sia il tempo di conservazione dei dati previsto in rapporto a quel reato e, nel caso in cui il termine sia già decorso, non potrà trasmettere i dati.

5. Travaglio europeo e ricadute interne.

Incuneandosi nel difficile rapporto tra esigenze securitarie e protezione della *privacy*, la disciplina in tema di *data retention* appare particolarmente tormentata anche sul piano delle fonti europee, con conseguenti ricadute interne.

Al riguardo, occorre ricordare come la direttiva 2006/24/CE (cd. direttiva Frattini) riguardasse proprio «la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione»[27]. Tuttavia, tale direttiva è stata dichiarata invalida dalla Corte di Giustizia[28] per violazione del principio di proporzionalità[29].

Dal che è derivato un dibattito circa i possibili effetti di una simile declaratoria sulla disciplina prevista dall'art. 132 Codice *privacy*, attuativa della direttiva 2006/24/CE[30]. In materia, a fronte della tesi della

[27] A seguito di tale direttiva, a livello interno venne emanato il d.lgs. 30 maggio 2008, n. 109 di attuazione della c.d. direttiva Frattini (direttiva 2006/24/CE).

[28] C. Giust., 8 aprile 2014, *Digital Rights Ireland Ltd e a.* Rileva come la proclamazione di uno *standard* tanto elevato di protezione del diritto alla *privacy* nelle pronunce *Digital Rights* e *Tele 2 Sverige AB* non sia stata – a oggi – sufficientemente valorizzata tanto da molti legislatori interni, quanto da quello europeo» L. Luparia, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio,* in *Dir. di internet*, 2019, p. 760.

[29] In particolare, la Corte di Giustizia ha rilevato come un simile principio non fosse stato rispettato in rapporto a più profili. Tra essi, la circostanza che la conservazione dei dati non venisse posta in correlazione all'esistenza di una minaccia per la sicurezza pubblica; la mancanza di criteri oggettivi tali da consentire l'accesso ai dati solo per il contrasto a reati «sufficientemente gravi da giustificare una simile ingerenza»; l'assenza di presupposti sostanziali e procedurali per l'accesso ai dati; il fatto che non fosse previsto un controllo da parte di un giudice o di un ente indipendente; l'omissione della preclusione alla conservazione dei dati in Paesi terzi.

[30] In giurisprudenza, cfr. Trib. pen. Padova, ord. 15 marzo 2017 (inedita) e le riflessioni al riguardo di R. Flor, *Data retention ed art. 132 cod. privacy: vexata quaestio (?),* in *Dir. pen. cont.,* 29 marzo 2017. Si vedano inoltre, *ex multis,* E. Colombo, *«Data retention» e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.,* 2014, p. 2705 ss.; R. Flor, *La Corte di Giustizia considera la direttiva europea*

disapplicazione dell'art. 132 Codice *privacy*, è prevalsa la tesi della validità della disciplina da esso prevista o, al più, della possibilità di una eventuale declaratoria di incostituzionalità dell'art. 132 codice *privacy*, per contrasto con l'art. 117 Cost., in rapporto agli artt. 7 e 8 della Carta dei diritti fondamentali e all'art. 8 Cedu.

Va chiarito che la direttiva Frattini aveva modificato la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (cd. direttiva relativa alla vita privata e alle comunicazioni elettroniche). Di conseguenza, a seguito della declaratoria di invalidità della direttiva Frattini, sono venute meno anche le modifiche alla direttiva relativa alla vita privata e alle comunicazioni elettroniche, che è tornata ad essere la fonte di riferimento in materia ed è stata oggetto, da ultimo, di domanda di pronuncia pregiudiziale alla Corte di Giustizia in relazione all'interpretazione dell'art. 15, paragrafo 1.

A seguito di una simile domanda, la Grande Sezione della Corte di Giustizia[31] è tornata ad occuparsi di *data retention*, chiarendo anzitutto come l'art. 15, paragrafo 1 debba essere interpretato nel senso che, a prescindere dalla quantità dei dati e dalla natura degli stessi, l'accesso dell'autorità pubblica ai dati non può avvenire «senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica»[32].

Inoltre, la Corte di Giustizia ha precisato che una corretta interpretazione della norma preclude la possibilità di una normativa nazionale che renda il pubblico ministero, «il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di

2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?, in *Dir. pen. cont., Trimestrale*, 2/2014, p. 178 ss; F. Iovene, *Data retention tra passato e futuro. Ma quale presente?,* in *Cass. pen.,* 2014, p. 808 s.; S. Marcolini, *L'istituto della* data retention *dopo la sentenza della Corte di Giustizia* del 2014, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), *Cybercrime,* Utet, Torino 2019, p. 1586; F. Ruggieri, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen.,* 2017, p. 2483 ss.

[31] Cfr. C. Giust., 2 marzo 2021, C-746/18. Per un approfondimento sul tema, si rinvia a T. Rafaraci, *Verso una* law of evidence *dei dati,* in *Dir. pen. proc.*, 7, 2021, p. 853 ss. Si può ricordare che la domanda pregiudiziale alla Corte di Giustizia era stata presentata dal *Riigikohus* (Corte suprema dell'Estonia) nell'ambito di un procedimento penale nei confronti di H.K. accusato di furto, uso della carta bancaria di un terzo e di violenza nei confronti di persone partecipanti ad un procedimento giudiziario.

[32] In questi termini, C. Giust., 2 marzo 2021, C-746/18, § 60, *sub* 1.

un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale».

La fissazione di quest'ultimo principio ha indotto la dottrina e la giurisprudenza italiane ad interrogarsi sulle ricadute interne della sentenza della Corte di Giustizia, dato che l'art. 132, comma 3, Codice *privacy* prevedeva che i dati fossero acquisiti presso il fornitore con decreto motivato del pubblico ministero[33].

Secondo un'impostazione, i principi affermati dalla Corte di Giustizia nella sentenza in esame non potrebbero avere «effetti applicativi immediati e diretti, per la indeterminatezza, nella sentenza, del riferimento ai casi nei quali i dati di traffico telematico e telefonico possono essere acquisiti»[34]. Inoltre, il ruolo del pubblico ministero nell'ordinamento italiano differisce in modo marcato da quello che lo stesso riveste nell'ordinamento estone[35].

Al contrario, secondo un diverso orientamento, la disciplina italiana si caratterizzerebbe per un *deficit* di garanzie rispetto a quanto stabilito dalla sentenza della Corte di Giustizia, tale da rendere la disciplina interna contrastante con le indicazioni della Corte. Il che determinerebbe la diretta disapplicazione della confliggente normativa nazionale.

Infine, un ulteriore orientamento ha ritenuto che la via non possa essere ravvisata nella disapplicazione, ma nella proposizione di una questione pregiudiziale[36], chiedendo alla Corte di Giustizia se l'articolo 15, paragrafo 1, della direttiva 2002/58/CE, letto alla luce degli articoli

[33] Al riguardo, non mancano voci volte ad affermare che l'acquisizione di dati di traffico telefonico, telematico e telematico porterebbe a conoscere anche aspetti così delicati di un soggetto, rispetto ai quali risulterebbe insoddisfacente un mero decreto dell'organo dell'accusa, sembrando invece necessario un provvedimento di un soggetto terzo e imparziale, qual è il giudice delle indagini preliminari.

[34] Così, Trib. ordinario di Roma, 2021, gip dott. V. Savio. Nel caso di specie il pubblico ministero, a seguito della sentenza della Corte di Giustizia, aveva richiesto di essere autorizzato dal gip a disporre l'acquisizione dei dati relativi al traffico telefonico e telematico. Escludendo l'effetto applicativo diretto dei principi affermati dalla Corte di Giustizia, il gip aveva dichiarato però non luogo a provvedere sull'istanza del pubblico ministero, con restituzione degli atti allo stesso. Per un'opposta impostazione, si veda invece G.i.p. Roma, decreto 25 aprile 2021, in cui il giudice ha autorizzato l'acquisizione di dati relativi al traffico telefonico, sul presupposto della disapplicazione dell'art. 132 codice *privacy* in conseguenza della ricordata sentenza della Corte di Giustizia. Al riguardo, cfr. J. Della Torre, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma,* in *Sistema penale,* 29 aprile 2021.

[35] Cfr. Trib. Milano, VII sez. pen., 22 aprile 2021, il quale pone in evidenza come il pubblico ministero italiano differisca significativamente da quello estone, dato che il pubblico ministero italiano assurge ad autorità giudiziaria ed è una parte pubblica.

[36] Per questa impostazione, cfr. Trib. Rieti, ordinanza di domanda di pronuncia pregiudiziale della Corte di Giustizia dell'Unione europea, 4 maggio 2021.

7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta di Nizza, anche sulla base dei princìpi fissati nella sentenza della Corte del 2 marzo 2021, debba essere interpretato nel senso che esso osta alla disciplina prevista dall'art. 132 codice *privacy* italiano, nonostante il pubblico ministero italiano sia un organo assistito da garanzie di indipendenza e autonomia.

Da ultimo, sospinto dall'esigenza di adeguare la disciplina italiana alle indicazioni contenute nella sentenza della Corte di Giustizia del 2 marzo 2021, il legislatore è intervenuto in materia. Infatti, dapprima con il d.l. 30 settembre 2021, n. 132 e, poi, con la legge 23 novembre 2021 n. 179, che ha convertito con modificazioni il decreto[37], sono state dettate disposizioni in materia di acquisizione dei dati di traffico telefonico e telematico per fini di indagine penale. Nello specifico, tale norma ha previsto *expressis verbis* che l'acquisizione di simili dati possa avvenire solo in forza di un previo decreto motivato da parte del giudice, su richiesta del pubblico ministero o a seguito di istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa o delle altre parti private.

Solo se «sussistono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini», l'acquisizione dei dati viene disposta con decreto motivato del pubblico

[37] Legge di conversione, con modificazioni, del d.l. 30 settembre 2021, n. 132 recante «Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP». Al riguardo, cfr. G. Amato, *Nella costruzione normativa si è sminuito il ruolo del Pm,* in *Guida al Diritto*, 2021, 39, p. 18 ss.; G. Battarino, *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021 n. 132*, in *Questione Giustizia,* 5 ottobre 2021; Corte di Cassazione, Ufficio del massimario e del ruolo, Sevizio penale, *Relazione su novità normative,* Roma, 13 ottobre 2021, nonché Id., *Relazione su novità normative,* Roma, 2 dicembre 2021; L. Filippi, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *Penale. Diritto e Procedura,* 1° ottobre 2021; L. Giordano, *La Corte di Cassazione ritorna sull'acquisizione dei tabulati telefonici dopo le indicazioni della CGUE*, in *il Penalista*, 5 ottobre 2021; A. Malacarne, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l.30 settembre 2021, n. 132*, in *Sistema penale,* 8 ottobre 202; C. Parodi, *Tabulati telefonici: la Suprema Corte si esprime dopo le indicazioni della CGUE,* in *il Penalista,* 5 agosto 2021; Id., *Convertito il decreto in tema tabulati: (quasi) tutto chiaro*, in *il Penalista,* 19 novembre 2021; G. Pestelli, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici,* in *Quotidiano Giuridico,* 4 ottobre 2021; F. Resta, *La nuova disciplina dell'acquisizione dei tabulati,* in *Giustizia insieme*, 2 ottobre 2021; F. Rinaldini, *La nuova disciplina del regime di acquisizione dei tabulati telefonici e telematici: scenari e prospettive*, in *Giurisprudenza penale web,* 2021, 10; G. Spangher, *Data retention: svolta garantista ma occorre completare l'impianto,* in *Guida al Diritto*, 2021, p. 11 ss.

ministero, peraltro soggetto a convalida del giudice entro quarantotto ore[38].

6. Conclusioni

La disciplina di *data retention* è al centro di un intenso dibattito dottrinale e giurisprudenziale. I fattori in gioco sono diversi; da un lato, la sensibilità sempre più intensa nei confronti del diritto alla protezione dei dati ed il timore di controlli orwelliani sospingono nella direzione di una disciplina caratterizzata da tempistiche minime di conservazione dei dati, secondo una posizione garantista in parte avallata dalla stessa Corte di Giustizia; dall'altro lato, le esigenze investigative richiedono invece tempistiche più dilatate di conservazione dei dati.

Di regola, il dibattito in materia si incentra su questi due poli, in una sorta di contrapposizione tra *privacy* e sicurezza. Si dimentica un terzo contrappeso, che andrebbe invece adeguatamente considerato per l'individuazione di una disciplina effettivamente garantista in materia.

Il riferimento è alla necessità di assicurare il diritto di difesa. Invero, i dati di traffico telefonico, telematico e delle chiamate senza risposta non sono funzionali soltanto all'accusa, ma anche alla difesa, che proprio in quei dati potrebbe rinvenire elementi fondamentali per provare la non colpevolezza dell'indagato o dell'imputato. Una equilibrata disciplina in tema di *data retention* dovrebbe tenere presente anche tale aspetto.

[38] Nel caso di mancata convalida entro il termine di quarantotto ore i dati non sono utilizzabili.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464307
pp. 115-136 (gennaio 2022)

Sull'analisi forense dei tabulati di traffico: aspetti giuridici, metodologici e tecnici

Ilaria Caprilli[1], Raffaella Brighi[1]

1. Introduzione: brevi cenni alla normativa di riferimento

Nella sentenza *Riley v. California*[2] (2014) la Corte Suprema degli Stati Uniti ha affermato che « […] *modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy*». Da questa considerazione si comprende il motivo del travagliato *iter* dottrinale e giurisprudenziale che ancora oggi vede la procedura sull'acquisizione dei dati sul traffico telefonico e telematico (cosiddetti tabulati), in particolare in tema di *data retention*, oggetto di ampi dibattiti e di numerosi interventi normativi.

Se da una parte, infatti, tale strumento investigativo ricopre un ruolo fondamentale per finalità di accertamento, prevenzione e repressione dei reati, dall'altra si scontra con l'interesse antagonista, ossia la tutela alla riservatezza, atteso che, alla stregua delle comunicazioni riservate, i dati esteriori delle stesse sono protetti dall'art. 15 Cost.[3]. Con dati esteriori si intende una serie di elementi eterogeni che attestano il fatto storico di una comunicazione già avvenuta e coessenziale alla stessa; at-

[1] CIRSFID – Alma Human Artificial Intelligence, Università di Bologna.

[2] Sentenza disponibile su www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

[3] Sul tema si v. Corte cost. 11 marzo 1993, n. 81; A. Camon, *et al.*, *Fondamenti di procedura penale*, CEDAM, 2021, p. 99 s.; Corte cost. 6 marzo 2019, n. 38 in cui la Corte costituzionale conferma che i dati esterni delle conversazioni sono di indubbio significato comunicativo e, richiamando la giurisprudenza della stessa Corte (sent. n. 188 del 2010), rimarca la «notevole capacità intrusiva» di un'attività investigativa che coinvolga i tabulati, in quanto consentono di ricostruire sia i contatti telefonici sia di localizzare il detentore dell'apparecchio; confermando, che per ogni cittadino, il ricorso a tale strumento di indagine deve necessariamente essere soggetto alle garanzie previste dall'art. 15 Cost.

traverso l'analisi di tali dati è quindi possibile riscostruire il flusso di traffico telefonico e telematico relativo a una determinata utenza[4].

Raccolta di informazioni nata per esigenze amministrative in capo ai gestori telefonici, quali fatturazione e contabilità, oggi l'acquisizione dei dati sul traffico costituisce un mezzo di ricerca della prova largamente utilizzato che non è privo di problematiche anche sul piano tecnico, in particolare in tema di acquisizione, gestione, fruizione, interscambiabilità, integrità e attendibilità[5].

In tema di *data retention*[6] la normativa vigente prevede in capo ai fornitori di servizi di comunicazione specifici obblighi temporali di conservazione dei dati sul traffico telefonico e telematico[7].

In particolare, l'art. 132 comma 1 d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (cosiddetto codice privacy) prevede i seguenti termini di conservazione:

- i dati relativi al traffico telefonico devono essere conservati per ventiquattro mesi dalla data di comunicazione;
- i dati relativi al traffico telematico devono essere conservati per dodici mesi dalla data di comunicazione;
- i dati relativi alle chiamate senza risposta devono essere conservati per trenta giorni dalla data di comunicazione.

In deroga alle disposizioni testé illustrate, l'art. 24 l. 20 novembre 2017, n.167[8] «al fine di garantire strumenti efficaci in considerazione

[4] Cfr. A. Ricciardi, *Dati esteriori delle comunicazioni e tabulati di traffico, Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore,* in Diritto Penale Contemporaneo, n. 3, 2016, p. 157.

[5] In tema di attendibilità dei tabulati si v. Cass. Pen. Sez. III, 23 agosto 2019, n 36380; Cass. Sez. un. Pen., 28 gennaio 2019, n. 14426; United States vs. Marquette Tibbs. Case No. 2016 CF1 19431, Superior Court of the District of Columbia, Criminal Division. September 5, 2019.

[6] Per approfondimenti si rimanda al contributo di S. Signorato, *Data retention, tra diritto alla protezione dei dati personali ed esigenze di accertamento dei reati*; S. Marcolini, *L'istituto della data retention dopo la sentenza della corte di giustizia del 2014*, in S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, UTET Giuridica, 2019, pp. 1579-1597; S. Signorato, *Novità in tema di data retention. La riformulazione dell'art. 132 codice privacy da parte del d.lgs. 10 agosto 2018, n. 101*, in Diritto Penale Contemporaneo, Fascicolo xi, 2018, pp. 153-161.

[7] Sul tema si segnala la "Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico" del 22/07/2021 (Docweb n.9685978) inviata dal Garante Privacy al Parlamento e al Governo con la quale chiede di valutare l'opportunità di una riforma in tema di *data retention*.

[8] «Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea».

delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3 *quater*, e 407, comma 2, lett. *a*) […]» estende il periodo di conservazione a settantadue mesi per tutti i tipi di dati (telefonico, telematico nonché chiamate senza risposta); di fatto obbligando i fornitori a estendere tale periodo di conservazione a tutti i dati esteriori delle comunicazioni, attesa l'impossibilità di conoscere a priori la loro finalità di utilizzo. Pertanto, solo al momento della richiesta di acquisizione, cioè quando i gestori verificheranno se poterne dare corso oppure no, opererà il "doppio binario" previsto dalla normativa[9].

I gestori telefonici devono inoltre necessariamente conservare specifiche categorie di dati[10] previste espressamente nell'art. 3 d.lgs. 30 maggio 2008, n. 109[11]. Tra i dati essenziali troviamo[12]:

- anagrafica dell'abbonato;
- numeri telefonici chiamanti e chiamati;
- IMSI (*International Mobile Subscriber Identity*) del chiamato e del chiamante, ossia il numero che identifica univocamente ogni utenza, *rectius*, il contratto di telefonia mobile[13];

[9] Sul punto merita di essere segnalata l'ordinanza di ingiunzione del Garante Privacy nei confronti di TIM S.p.A. dell'8 luglio 2021 (www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9693464). Il Garante, ritenendo ammissibile il reclamo presentato dall'interessato con il quale veniva chiesto di accertare la violazione del diritto di accesso a dati di traffico telefonico e di ordinare alla medesima Società di soddisfare la richiesta di esercizio di tale diritto entro un termine congruo con le esigenze difensive invocate, ai sensi dell'art. 58, par. 2, lett. c) del Regolamento, ha ordinato al gestore di fornire al reclamante i dati richiesti, trattandosi di dati tempestivamente richiesti da questi, ben prima della scadenza del termine di 24 mesi contemplato dall'art. 132 del Regolamento, colpevolmente lasciato decorrere dal gestore. Il Garante, quindi, ha ordinato la consegna dei tabulati richiesti, nonostante fosse scaduto il termine dei ventiquattro mesi.

[10] Volendo svolgere un confronto, si segnala che, a differenza delle leggi sulla conservazione dei dati vigenti nell'Unione Europea e di altri paesi che prevedono la memorizzazione dei soli dati esteriori delle conversazioni, la legislazione russa prevede in capo ai gestori telefonici l'obbligo di conservare anche il contenuto delle stesse comunicazioni, sia esse telefoniche sia esse telematiche. Sul tema, v. M.S. ZHURAVLEV, T.A. BRAZHNIK, *Russian data retention requirements: Obligation to store the content of communications*, in Computer law & Security review, vol. XXXIV, 2018, pp. 496-507.

[11] "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (G.U. n. 141 del 18/06/2008)".

[12] Per l'elenco completo si rimanda alla norma citata.

[13] Tale numero è memorizzato all'interno di ogni SIM Card e il suo scopo è quello di identificare in modo univoco un abbonato all'interno della rete mobile.

- IMEI (*International Mobile Equipment Identity*) del chiamato e del chiamante, ossia il numero univoco associato al dispositivo mobile utilizzato;
- etichetta di ubicazione (Cell ID) all'inizio della comunicazione, ossia la "cella", *rectius* antenna BTS[14] (*Base transceiver station*), agganciata all'inizio della comunicazione.

Sotto il profilo acquisitivo[15], il novellato art. 132 comma 3 del d. lgs. 30/06/2003, n. 196[16] impone che i dati, ove rilevanti per l'accertamento dei fatti[17], siano acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato[18] su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private[19]; prevedendo al nuovo comma 3 *bis* – sulla falsariga di quanto previsto in tema di intercettazioni – casi eccezionali in cui il pubblico ministero può disporre direttamente l'acquisizione dei dati a cui dovrà seguire, da parte del giudice, la decisione sulla convalida. L'acquisizione dei dati in violazione di tali disposizioni comporta l'inutilizzabilità degli stessi (comma 3 *quater*).

[14] Antenna che realizza la copertura e che permette al dispositivo di connettersi alla rete e copre una specifica area geografica. L'insieme di più BTS formano un sito cellulare.

[15] Per un confronto sul tema si v. Carpenter v. United States, No. 16-402, Supreme Court of United States, June 22, 2018.

[16] La norma è stata modificata dall'art. 1 «Disposizioni in materia di acquisizione dei dati di traffico telefonico e telematico per fini di indagine penale» del d.l. 30 settembre 2021, n. 132 recante «*Misure urgenti in materia di giustizia e di difesa, nonché in tema di referendum, assegno temporaneo e IRAP*», convertito, con modificazioni, dalla l. 23 novembre 2021, n. 178 entrata in vigore dal 30 novembre 2021. Per approfondimenti, G. Pastelli, *Convertito in legge il D.L. 132/2021: le modifiche apportate* (*e quelle mancate*) *in materia di tabulati*, in il Quotidiano Giuridico, Wolters Kluwer, 18 novembre 2021; Relazione n. 55/2021 Corte Suprema di Cassazione, "*Relazione su novità normative – art. 1 d.l. 30 settembre 2021, n. 132*", Relazione n. 67/2021 Corte Suprema di Cassazione, "*Relazione su novità normativa – Conversione in legge, con modificazioni, del d.l. 30 settembre 2021, n. 132 (l. 23 novembre 2021, n. 178)*". Si segnala inoltre il parere del Garante Privacy sullo schema di decreto-legge consultabile all'URL www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9704851.

[17] L'espressione estende l'applicazione della norma in ogni stato e grado del procedimento.

[18] Sarà quindi direttamente il soggetto istante, a seguito dell'ottenimento del decreto autorizzativo, a fare richiesta di acquisizione al fornitore; la norma però non chiarisce il *quomodo* in cui la parte richiedente dovrà provvedere a tale acquisizione.

[19] Alla stregua del pubblico ministero, quindi, viene eliminata *tout court* la previsione contenuta nella normativa previgente che attribuiva al difensore dell'imputato o della persona sottoposta alle indagini la possibilità di richiedere – direttamente al fornitore – i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'art. 391 quater c.p.p. (richiesta di documentazione alla pubblica amministrazione).

In sede di conversione è stata altresì introdotta una disciplina transitoria – fonte di forti perplessità[20] – relativa ai tabulati già acquisiti in data anteriore all'entrata in vigore del d.l. che prevede che i relativi dati possano essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova e per l'accertamento di reati specifici.

La novella, che ha l'obiettivo di porsi in linea con il diritto comunitario e la sentenza della Corte di Giustizia dell'Unione Europea del 2 marzo 2021[21], sta destando pareri contrastanti tra gli addetti ai lavori. Da una parte i pubblici ministeri – prima detentori del monopolio in materia – lamentano un possibile rischio di rallentamento delle indagini, dall'altro invece, i processualpenalisti che sottolineano come tale previsione bilanci i rapporti tra accusa e difesa, in ossequio al principio di parità delle parti, e renda sempre più omogenei i sistemi giudiziari europei.

2. L'analisi forense dei tabulati di traffico: criticità, ripercussioni pratiche e soluzioni auspicabili

Come noto, oltre alle classiche attività, quali l'assunzione di informazioni testimoniali o la raccolta di elementi di prova, i tabulati di traffico sono divenuti un importante strumento investigativo nell'accertamento di un fatto. Da una parte, infatti, tale strumento permette alla polizia giudiziaria di venire a conoscenza di elementi rilevanti per l'indagine in corso, come ad esempio accertare dove si trovasse il sospettato in un dato periodo temporale, individuare gli ultimi contatti della vittima, ricostruire gli spostamenti, e così via; dall'altro, può essere rilevante per la verifica delle prospettazioni difensive, circa l'incompatibilità – in tesi difensiva – col *locus commissi delicti* o all'attribuzione di condotte. L'analisi dei tabulati di traffico presenta però diverse criticità che meritano di essere affrontate, atteso che, se non tenute in considerazione, potrebbero minare l'attendibilità dei risultati emersi.

[20] Cfr. G. Pastelli, *op. cit.*
[21] Cfr. C. Giust., 2 marzo 2021, C-746/18.

2.1. *L'integrità dei dati dei tabulati di traffico*

La prima criticità attiene all'integrità dei dati contenuti nei tabulati di traffico. Un recente e innovativo studio statunitense[22] ha intrapreso una ricerca per verificare il grado di attendibilità dei tabulati prodotti dai gestori telefonici individuando – appurata la loro natura quali dati digitali e quindi assoggettati allo standard ISO/IEC 27037[23]– in un metodo basato sulla *blockchain*[24]*,* una possibile soluzione per garantire l'integrità dei suddetti elementi di prova; integrità che dipende dalla metodologia di estrazione dal *repository* adottata dall'operatore e dalla successiva gestione dei dati. La ricerca ha appurato l'esistenza delle seguenti criticità[25]:

- assenza della catena di custodia[26] che documenti la storia del reperto;
- assenza della stringa risultante dalla funzione di *hash*[27] per i dati originari e per i dati prodotti;
- produzione dei tabulati in una varietà di formati digitali e con contenuti difformi;
- alterazione dei metadati[28] relativi ai file di origine e di destinazione;

[22] Cfr. J.B. Minor, *Forensic Cell Site Analysis: Mobile Network Operator Evidence Integrity Maintenance Research*, in Journal of Digital Forensics, Security and Law, vol. XIV, n. 2, Art. 5, 2019, pp. 59-85.

[23] In argomento si v. R. Brighi, M. Ferrazzano, *Digital forensics: best practices and perspective*, in Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations, CEDAM, 2021, pp. 13-48.

[24] Sul tema, cfr. R. Brighi, V. Ferrari, *Digital evidence e tutele processuali: potenzialità della tecnologia blockchain*, in Ragione Pratica, n. 2, il Mulino, 2018. pp. 329-342.

[25] Cfr. J.B. Minor, *Forensics Cell Site Analysis: Mobile* Operator Evidence Research, cit., p. 72 ss.

[26] Sul tema v. L. Bartoli, C. Maioli, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in M.A. Biasiotti, M. Epifani, F. Turchi (a cura di), *Trattamento e scambio della prova digitale in Europa*, Edizioni Scientifiche Italiane, 2016, pp. 139-151.

[27] «L'*hash* è una funzione matematica che prende in input una sequenza di bit di qualsiasi lunghezza e produce in output una stringa di bit di dimensione fissa (la cui lunghezza dipende dall'algoritmo prescelto), solitamente espresso in formato più leggibile come stringa di caratteri esadecimali (0123456789ABCDEF). Quando l'output della stringa di *hash* applicata al reperto originario o alle copie forensi è il medesimo, si ha la garanzia di integrità dei dati. MD5, SHA-1, RIPEMD-160 sono alcuni degli algoritmi più comuni che possono essere utilizzati per la creazione dell'impronta». Così in, M. Ferrazzano, *Aspetti metodologici, giuridici e tecnici nel trattamento di reperti informatici nei casi di pedopornografia*, Aracne, 2018. In argomento, E. Casey, *Digital Evidence and Computer Crime*, in Waltham Academic Press, 2011, p. 22 s.

[28] Insieme di dati (informazioni) che corredano ogni file digitale (quale, ad esempio, file audio, file video, documento, ecc.) e che consentono di risalire a importanti informazioni, come la data di creazione, la data di ultima modifica, la data di ultimo accesso ecc.

– perdita irrecuperabile dei dati esteriori conservati nel *repository* che quindi non sono stati inseriti nel file di destinazione;
– accesso agli elenchi relativi ai siti delle celle da parte di chiunque.

Dalla ricerca svolta su dei tabulati a campione è emerso che i fornitori non adottano metodologie atte a preservarne l'integrità; mancando peraltro linee guida che dettino protocolli per uniformare la loro estrazione e produzione.

Lo scenario italiano non si discosta più di tanto da quello illustrato. Ogni fornitore, infatti, come sarà illustrato *infra,* produce tabulati in diverso formato e contenuto, senza i relativi valori di *hash* e catene di custodia[29]. È giocoforza che tale agire si ripercuota poi sull'attendibilità degli esiti che emergeranno dall'analisi forense svolta sui dati stessi.

Il progetto di ricerca menzionato ha quindi individuato nell'uso della tecnologia *Blockchain*, basata sull'utilizzo di un registro distribuito in accordo con le architetture *Distributed Ledger Technology* (DLT), una possibile soluzione per mantenere l'integrità di tali fonti di prova; le fasi sommariamente sono le seguenti:

1. il tabulato di interesse come evidenza documentale viene inserito in un DL e crittato con chiave pubblica;
2. esso viene inserito nella struttura *blockchain* che è prevista da quel DL e che viene utilizzata come catena di custodia, inoltre vengono calcolati i valori di *hash* per tale elemento e per il blocco in cui viene inserito;
3. informazioni sull'elemento di prova di cui al punto 1) sono inseriti in un portale destinato a essere utilizzato da chi svolge indagini, cioè da soggetti autorizzati, dotati di opportune chiavi private, ad accedere alla catena di custodia;
4. il portale fornisce un affidabile sistema di controllo e di verifica della integrità delle prove (grazie al fatto di basarsi sulla struttura *blockchain*) ai soggetti autorizzati.

[29] Ai gestori telefonici sono prescritte da parte del Garante Privacy delle misure tecniche organizzative al fine di garantire un elevato livello di protezione dei dati. Tali misure di sicurezza attengono all'accesso ai dati e ai locali, il tracciamento dell'attività del personale incaricato, alla conservazione separata dei dati in base alla loro finalità, alla cancellazione dei dati, ai controlli interni e ai sistemi di cifratura.

L'uso di tale tecnologia – che potrebbe essere la base di partenza per creare standard comuni per la gestione dei record e protocolli di trasmissione – garantirebbe la produzione di dati integri e attendibili.

2.2. *La struttura e il contenuto dei tabulati di traffico*

Ulteriore criticità riguarda la struttura e il contenuto dei tabulati di traffico. Se da una parte il Garante Privacy prescrive ai gestori telefonici misure tecniche e organizzative al fine di garantire un elevato livello di protezione dei dati e il legislatore prevede quali categorie di dati debbano essere conservati e per quanto tempo, dall'altro, invece, non è dettata alcuna modalità attraverso la quale questi dati debbano essere trasmessi alle parti che ne fanno richiesta[30].

Invero, ogni fornitore produce tabulati di traffico telefonico e telematico in formati di file differenti (*pdf*, *csv*, *txt*), con un contenuto e una rappresentazione grafica ed elettronica difforme tra di loro[31]. Ad esempio, alcuni fornitori includono nello stesso tabulato le chiamate entranti e uscenti, mentre altri le riportano in due diversi tabulati[32]; lo stesso evento (chiamata entrante, uscente, ecc.) viene registrato dai gestori con identificativi e voci differenti; lo stesso accade anche per la durata delle chiamate, dove in alcuni casi viene espressa in secondi e in altri in ore, minuti e secondi senza spaziature tra i caratteri[33]. Ancora, alcuni operatori forniscono sia l'ID delle celle di inizio e fine chiamata, altri solo di inizio[34]. Alcuni poi, riportano direttamente nel tabulato l'indirizzo in cui è installato il sito cellulare.

È vero che ogni tabulato è corredato da una legenda che attribuisce a ogni voce indicata il corretto significato, ma ciò non è sufficiente, con

[30] Cfr. M. Ferrazzano, P. Reale, *Una proposta di progetto open source per l'analisi di tabulati telefonici in risposta a problematiche ed errori ricorrenti*, in M.A. Biasiotti, M. Epifani, F. Turchi (a cura di), *op. cit.*, pp. 373-389, p. 373.

[31] Per approfondimenti v. P. Reale, *I dati telefonici e telematici per l'autorità giudiziaria: la necessità di convergere su modelli di dati e procedure condivise*, in M.A. Biasiotti, M. Epifani, F. Turchi (a cura di), *op. cit.*, pp. 333-344, p. 335 s.

[32] Tale circostanza fa sì che la richiesta di acquisizione dei dati sul traffico rivolta al gestore debba necessariamente contenere la richiesta sia per le chiamate entranti che uscenti, altrimenti il rischio è quello di avere dati parziali.

[33] Cfr. P. Reale, *I dati telefonici e telematici per l'autorità giudiziaria,* cit., p. 338 s.

[34] Cfr. M. Tart, *et al.*, *Historic cell site analysis – Overview of principles and survey Methodologies,* in Digital Investigation, vol. VIII, issues 3-4, 2012, pp. 185-193, p. 185.

la conseguenza che si rende spesso necessario chiedere chiarimenti al gestore per poter formulare una corretta interpretazione dell'evento registrato.

Generalmente, i tabulati delle utenze mobili contengono i seguenti dati esteriori[35]:

- data dell'evento;
- ora di inizio e fine della chiamata;
- durata della chiamata (quando non è indicata la fine);
- tipo di evento[36] (chiamata entrante, uscente, senza risposta, SMS, ecc., connessione IP se si tratta di tabulati telematici);
- cell ID (BTS) e LAC (Location Area Code[37]) all'inizio della chiamata[38];
- nome del sito cellulare o coordinate[39];
- codice IMEI[40] del dispositivo;
- codice IMSI della scheda SIM.

La mancanza di uniformità tra i tabulati fa sì che chiunque analizzi i dati ivi contenuti, magari anche attraverso l'utilizzo di software specifici, dovrà porre molta attenzione nell'interpretare correttamente le informazioni e dovrà quindi individuare le differenze tra i diversi formati per scongiurare eventuali errori[41] che andrebbero ad inficiare la ricostruzione dei fatti.

Se un consulente informatico si trova di fronte a un caso in cui le utenze appartengono alla stessa rete, avrà sicuramente meno problemi rispetto al caso in cui si trovi di fronte a tabulati acquisiti da gestori diversi, poiché ragionevolmente nel primo caso i tabulati avranno il medesimo formato, rendendo relativamente più semplice l'analisi. Diversamente, invece, l'accertamento sarà molto complesso.

[35] Sul tema, cfr. J. HOY, *Forensic Radio Survey Techniques for Cell Site Analysis*, John Wiley & Sons, Incorporated, 2015, p. 265 s.

[36] Si badi che ad ogni evento è attribuito un numero il cui significato è desumibile dalla legenda allegata.

[37] Il LAC è il numero univoco assegnato a ciascuna area dell'ubicazione all'interno della rete. Si tenga infatti presente che l'area servita di una rete di accesso radio cellulare è solitamente suddivisa in aree di localizzazione, costituite da una o più celle radio.

[38] Tali dati permettono di capire in quale area geografica è stata localizzata l'utenza al momento dell'evento.

[39] Tale dato indica dove è installata la BTS agganciata.

[40] Sulla struttura del codice IMEI, si v. J. HOY, *op. cit.*, p. 55 s.

[41] In tema di errore di interpretazione dei dati del tabulato telefonico si rimanda al *case study* illustrato *infra*.

Ecco, quindi, che – prima di procedere con qualsiasi analisi – è necessario operare una "normalizzazione" dei dati grezzi forniti dal gestore in un formato comune al fine di rendere più semplice l'interrogazione della base dati[42]. La complessità di tale operazione, pertanto, richiede in capo a chi opera delle specifiche competenze sull'uso e l'interpretazione corretta dei dati, il corretto utilizzo dei software specifici, la sensibilità di comprendere se vi sia la necessità di richiedere ulteriori informazioni al fornitore e quale tipologia di documentazione richiedergli per svolgere eventualmente una più approfondita attività di analisi del sito cellulare. Si badi infatti che l'errata conversione dei dati presenti sul tabulato e l'errata interpretazione degli stessi non è una probabilità così remota.

A tal proposito, si pensi ad esempio allo scandalo scoppiato in Danimarca nel 2019 sui dati delle comunicazioni mobili errati e utilizzati a fini investigativi[43]; in tal caso, i dati erano stati alterati (alcuni furono scartati e di altri venne modificata la posizione di geolocalizzazione delle BTS fino a 200 metri) da un software utilizzato dalla polizia danese per convertire in un formato comune i dati grezzi forniti dai diversi gestori. Oppure, si pensi al caso in cui sia stata attribuita ad una cella la localizzazione sbagliata. In questa seconda circostanza, sarà utile svolgere un'attività di misurazione sul territorio (anche detta "misurazione del campo di copertura") al fine di verificare la compatibilità tra il dato indicato sul tabulato e quanto ricostruito dalla polizia giudiziaria o da una delle parti.

In tema di errata interpretazione dei dati, si vuole di seguito illustrare un caso di analisi svolto dal consulente di parte su tabulati telefonici al fine di verificare la ricostruzione operata della pubblica accusa, poi dimostratasi errata.

La vicenda

L'imputata Tizia veniva tratta in giudizio per rispondere *ex* art. 575 c.p. della morte di Caia. Tra gli elementi di prova prodotti in sede dibattimentale dal pubblico ministero per corroborare la ricostruzione accusatoria, venivano versati in atti altresì i tabulati telefonici relativi

[42] Sul tema, cfr. J. Hoy, *op. cit.*, p. 285 s. e p. 338 s.

[43] Per approfondimenti v. G. Nazzaro, *Danimarca: Aggiornamento sullo scandalo dei dati delle comunicazioni mobili errati e utilizzati per le indagini*, in Sicurezza e Giustizia, II, 2020, pp. 46-49.

all'utenza in uso alla vittima. In particolare, tramite la lettura dei dati del traffico acquisito dal fornitore, il pubblico ministero giungeva alla conclusione che alle 10.05 Caia fosse già deceduta per mano dell'imputata, posto che le due telefonate ricevute dalla vittima, rispettivamente alle ore 10.05 e alle ore 10.06, non avevano mai ricevuto risposta. In particolare, il pubblico ministero riteneva che tali telefonate fossero meri "tentativi di chiamata" e "telefonate terminate in segreteria telefonica", dopo le quali il cellulare risultava essere spento. La difesa, dal canto suo, alla luce dell'accertamento tecnico svolto dal proprio consulente tecnico di informatica forense sui tabulati in parola, argomentava invece che Caia a quell'ora fosse ancora viva perché emergeva *per tabulas* che quelle due chiamate avevano ricevuto risposta. Elemento questo che, letto congiuntamente agli esiti dell'accertamento autoptico e sul contenuto gastrico della vittima, facevano risalire l'epoca del decesso almeno un'ora dopo rispetto all'ora indicata dalla pubblica accusa.

L'analisi forense dei tabulati

Tenuto conto delle conclusioni a cui giungeva il pubblico ministero durante l'istruttoria dibattimentale, il consulente della difesa aveva avuto mandato di procedere all'analisi dei tabulati, in particolare di accertare se le due chiamate (delle ore 10.05 e 10.06) fossero – come sostenuto dal pubblico ministero – tentativi di chiamate terminate in segreteria telefonica o, invece, telefonate al quale era stata data risposta.

Il consulente provvedeva quindi a una disamina *de visu*[44] e, atteso che ogni riga del tabulato[45] si componeva di due parti, ciascuna delle quali conteneva un dato diverso[46], il consulente provvedeva a inserire dei segni grafici che permettevano di non confondere tra loro le righe e quindi i dati riportati, giungendo al seguente risultato[47].

[44] Come descritto *supra*, la difficoltà nell'analizzare un tabulato deriva dal fatto che ogni fornitore adotta differenti formati di rappresentazione dei dati; pertanto, per svolgere una corretta analisi, si rende necessario adottare strategie (talvolta attraverso l'utilizzo di software specifici e altre volte attraverso uno studio analitico *de visu*) che permettano l'esatta interpretazione dei dati.

[45] C.d. "cartellino" di traffico.

[46] In particolare, si veda la Figura 1 dove emergono i seguenti riferimenti: Centro Sms (parte in alto della colonna sinistra); Cod. Conv (parte in basso della colonna sinistra); Tipo Chta (parte in alto della colonna centrale); Tentativo (parte in basso della colonna centrale); Nota (parte in alto della colonna di destra); Del (parte in basso della colonna di destra).

[47] Il riquadro di colore rosso contiene gli eventi di interesse.

Ricerca: 5513048 CONSULTAZIONE TRAFFICO RADIOMOBILE Telecom Italia S.p.A.

DATA NCR/Call ID	ORA Conf ID	Durata	Telefono Chte Telefono Chto	Telefono Deviante Imsi Deviante	Imsi Chte Imsi Chto	Imei Chte Imei Chto	MSC Opest	NAZ	Cellid Cellid end	CGI/ECGI/LocNumber CGI end	Centro Sms Cod Conv	Tipo Chta Tentativo	Nota Dei
15[redacted]	20:19:35	000000	33988[redacted]				VRN1		[redacted]45U3	222-01-6[redacted]-17[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]45U3	222-01-61[redacted]-17[redacted]	14	CSR3	
16[redacted]	06:17:17	000000	32029[redacted]				VRN1		[redacted]2AU3	222-01-6[redacted]-50[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]2AU3	222-01-61[redacted]-50[redacted]	14	CSR3	
16[redacted]	06:25:58	000000	32029[redacted]				VRN1		[redacted]45U3	222-01-6[redacted]-17[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]45U3	222-01-61[redacted]-17[redacted]	14	CSR3	
16[redacted]	06:27:03	000000	32029[redacted]				VRN1		[redacted]45U3	222-01-6[redacted]-17[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]45U3	222-01-61[redacted]-17[redacted]	14	CSR3	
16[redacted]	06:34:01	000000	32029[redacted]				VRN1		[redacted]2AU3	222-01-6[redacted]-50[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]45U3	222-01-61[redacted]-17[redacted]	14	CSR3	
16[redacted]	06:37:41	000000	32029[redacted]				VRN1		[redacted]45U3	222-01-6[redacted]-17[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]45U3	222-01-61[redacted]-17[redacted]	14	CSR3	
16[redacted]	06:42:49	000000	32029[redacted]				VRN1		[redacted]45U3	222-01-6[redacted]-17[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]45U3	222-01-61[redacted]-17[redacted]	14	CSR3	
16[redacted]	10:05:32	000006	05[redacted]				VRN1		[redacted]05W2	222-01-6[redacted]-63[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]05W2	222-01-61[redacted]-63[redacted]	14		
16[redacted]	10:06:05	000018	05[redacted]				VRN1		[redacted]05W2	222-01-6[redacted]-63[redacted]		G	
			335522[redacted]		222016[redacted]	3556880[redacted]			[redacted]05W2	222-01-61[redacted]-63[redacted]	14		
16[redacted]	12:53:37	000013	33944[redacted]	335522[redacted]			JVE71					K	
			335522[redacted]	222016[redacted]							40		

Figura 1. Stralcio del tabulato telefonico «in ingresso» relativo all'utenza telefonica in uso alla vittima.

Ebbene, già da una preliminare disamina, emergeva che le due telefonate di interesse avevano una durata l'una di 6" e l'altra di 18", circostanza questa che forniva al consulente dei primi riscontri sulla possibile avvenuta risposta alle stesse da parte della vittima. Fermo restando ciò, al fine di comprendere come fossero qualificati i due eventi, l'esperto procedeva quindi a individuare con precisione quali identificativi fossero stati attribuiti alle due chiamate di interesse. Dall'analisi del tabulato emergeva che le due telefonate oggetto di disamina avevano entrambe lo stesso identificativo "14 G", dove il numero "14" era riconducibile a "Cod. Conv", ossia "codice conversazione" (cfr. Figura 1, colore blu), mentre la lettera "G" atteneva a "Tipo Chta", cioè al "tipo chiamata" (cfr. Figura 1, colore verde). Dopo aver correttamente individuato gli identificativi in parola, il consulente ne verificava il significato con l'aiuto delle rispettive legende. Dalla disamina di queste, in particolare la "legenda decodifica codici conversazioni" e la "legenda tipo chiamata" emergeva che l'identificativo "14" indicava "traffico terminato", mentre l'identificativo "G" indicava "Fonia UMTS". Pertanto, contrariamente a quanto ricostruito dal pubblico ministero, gli eventi registrati con identificativo "14 G" non erano da individuarsi come semplici "tentavi di chiamata" o "telefonate terminate in segreteria telefonica", ma in chiamate in entrata al quale era stata data risposta e vi era stata una conversazione.

Dopo aver appurato che dall'analisi del tabulato emergeva pacificamente che le due telefonate in parola avevano ricevuto risposta e, altresì, vi era stata conversazione, il consulente procedeva a verificare quale fosse stato il motivo dell'errata interpretazione da parte della

pubblica accusa dei due eventi di interesse al fine di convalidare la propria ricostruzione. A tale scopo, prendeva in esame il verbale di udienza[48] nella quale, durante l'esame testimoniale dell'agente di polizia giudiziaria impegnato nelle indagini, il pubblico ministero illustrava alla Corte d'Assise cosa emergesse dai dati presenti sul tabulato telefonico di interesse, nei seguenti termini[49]:

> Qui c'è il tabulato inerente all'utenza della vittima Caia. E ci sono queste due chiamate delle 10.05 e 10.06 da un numero fisso. Ora, leggendo la leggenda del tabulato, qui si vede che in fondo c'è un numero 14 e una lettera G. Se noi andiamo a vedere cosa significa, vediamo che G viene indicata in legenda, […] allora con la lettera G si intende colloquio con 119, che è il numero della segreteria telefonica. Perché infatti la lettera G c'è scritto fonia al primo foglio, dopodiché si legge cos'è questa fonia, cioè questo colloquio, te lo spiega nel dettaglio, colloquio con 119. Il codice 14 vuol dire telefonata terminata, cioè telefonata terminata in G, cioè telefonata che fluisce, termina in segreteria telefonica, vuol dire che nessuno ha risposto alla telefonata delle 10.06.

Da tale ricostruzione emergeva che il pubblico ministero attribuiva correttamente all'identificativo "14" il significato di "telefonata terminata" (*rectius* "traffico terminato"), mentre attribuiva erroneamente all'identificativo "G" il significato di "colloquio con 119". Tale errore derivava quindi da un'errata interpretazione dei dati riportati sul tabulato telefonico in parola. Infatti, la pubblica accusa, anziché attribuire correttamente l'identificativo "G" alla voce "Tipo Chta", l'attribuiva alla voce "Nota", la quale colonna – in realtà – non presentava alcun evento registrato, infatti appariva vuota (si v. Figura 1, colore arancione) e pertanto, consultando la legenda sbagliata, concludeva nell'identificare erroneamente l'evento come "Colloquio con 119".

Tenuto conto della ricostruzione operata dalla pubblica accusa – che si rivelò errata a causa di una non corretta interpretazione dei dati – il consulente documentava nella propria relazione altresì come sarebbe apparso il tabulato – e quindi quali identificativi avrebbero dovuto esserci – se le chiamate in parola fossero state effettivamente "tentativi di chiamata" o "telefonate terminate in segreteria telefonica". Nel caso di "tentativi di chiamata", le due chiamate non avrebbero avuto come

[48] Verbale di udienza redatto con il sistema della fonoregistrazione e successiva trascrizione.

[49] Si sono volutamente riportate le parole esatte del pubblico ministero al fine di comprendere il percorso logico alla base delle sue conclusioni.

identificativo "14 G", bensì un identificativo del tipo "14 G CSR1" e durata della chiamata pari a zero, dove "CSR1" si riferisce a uno dei codici attribuiti al "tentativo di chiamata". Mentre, se le chiamate fossero "terminate in segreteria telefonica" avrebbero avuto l'identificativo "40 K", dove il numero "40" significa "traffico *call forwarding*", ovvero trasferimento di chiamata e la lettera "K" significa "deviazione in STC", ovvero deviazione in segreteria telefonica, andando così a significare che la chiamata in entrata viene deviata in segreteria telefonica.

Concludendo, l'attività di accertamento svolta dal consulente informatico ha quindi permesso di interpretare correttamente i dati contenuti nel tabulato e quindi accertare che – contrariamente a quanto sostenuto dal pubblico ministero – Caia aveva risposto alle due telefonate in parola.

Tenuto conto di quanto sin qui detto, tra gli esperti del settore, tra cui i consulenti tecnici di parte, ciò che è auspicabile è che presto si possa giungere a una standardizzazione in tema di produzione dei tabulati[50] alla quale ogni operatore dovrebbe attenersi. E, allo stesso modo, che vengano sviluppati software basati su standard internazionali, piuttosto che utilizzare sistemi sviluppati privatamente che non possono essere certificati[51]. Ciò garantirebbe un'analisi più semplice e attendibile e minimizzerebbe gli errori causati da un'errata interpretazione dei dati.

2.3. *L'analisi delle celle telefoniche*

L'analisi del sito cellulare[52] ha la finalità di fornire degli elementi di prova su dove potrebbe essere stato localizzato un telefono cellulare quando sono accaduti determinati eventi registrati sul tabulato e quali celle possono ragionevolmente servire un dato luogo al momento dell'accertamento. Tale analisi presenta diversi limiti circa la sua accuratezza e attendibilità[53], motivo per il quale è bene basare questo tipo di accertamento sulla combinazione di due dati: i dati contenuti nel tabulato relativi alla cella agganciata dall'utenza[54] durante le sessioni di co-

[50] Cfr. M. Ferrazzano, P. Reale, *op. cit*.

[51] Cfr. G. Nazzaro, *op. cit*., p. 49.

[52] Sul tema, D.E. Caccavella, M. Ferrazzano, *L'accertamento di reati attraverso l'analisi di tabulati telefonici*, in Diritto di Internet, n. 4, 2020, pp. 751-758.

[53] Cfr., J. Hoy, *op. cit.*, p. 361.

[54] I tabulati forniscono i dettagli delle celle agganciate dall'utenza per ogni sessione di chiamata, SMS o connessione Internet e includono ID della cella, la sua posizione e la direzione del settore specifico utilizzato (cosiddetto azimut).

municazioni attive e quelli risultanti dall'indagine di misurazione del campo di copertura radioelettrica[55].

Scopo di tali indagini è quello, infatti, di verificare la compatibilità tra il dato indicato sul tabulato e la prospettazione offerta dalla pubblica accusa o quella offerta dalla difesa; tentando di determinare se il telefono oggetto di accertamento si potesse trovare oppure no nei dintorni del luogo di interesse. Sarà quindi necessario che il consulente che si appresti a svolgere un'analisi di questo tipo richieda al fornitore, tramite il difensore, l'ulteriore documentazione necessaria (oltre ai tabulati di traffico) al fine di valutare le possibili geolocalizzazioni delle utenze oggetto di accertamento. In particolare, dopo aver svolto un'analisi preliminare individuando gli eventi oggetto di accertamento, dovrà richiedere:

- l'elenco storico delle celle relative alla provincia in cui si trovano, complete di CGI[56], latitudine e longitudine (possibilmente espresse come coordinate WGS84), azimut[57], l'angolo di tilt[58] e la potenza del segnale, così come erano configurate nel giorno di interesse;
- mappe di copertura[59] storica individuale (cioè la massima copertura delle singole celle di interesse, senza tenere conto del contributo/interferenza delle celle adiacenti) relative allo stesso periodo, individuando separatamente (in *layers* separati) i livelli di intensità di campo.

Nonostante l'attività di misurazione aggiunga rigore empirico alla mera analisi delle celle attraverso i tabulati, anche questa presenta delle incertezze intrinseche a prescindere dalla metodologia di indagine[60] ap-

[55] Cfr., J. Hoy, *op. cit.*, p. 255.

[56] Il CGI (*Cell Global Identifier*) è l'identificativo univoco a livello mondiale di una singola cella. Si differenzia con il "Cell ID" che invece indica il codice adottato dal singolo operatore per identificare le proprie celle.

[57] L'asse di orientamento in cui quella cella sta dirigendo la copertura.

[58] L'inclinazione della BTS rispetto all'asse orizzontale.

[59] Mappe geografiche sviluppate dal gestore sulla base dei parametri di configurazione della cella e del territorio e sono, sostanzialmente, una rappresentazione simulata del grado di copertura territoriale di ogni singola BTS e del relativo campo. Così, in P. Reale, *Analisi delle celle telefoniche: limiti ed opportunità,* in Sicurezza e Giustizia, n. 4, 2011, pp. 8-9, p. 8.

[60] Sulle diverse metodologie di indagine applicabili, nonché sui loro vantaggi e svantaggi, si v. J. Hoy, *op. cit.;* M. Tart, *et al*., *Historic cell site analysis,* cit., p. 191 s. Sul grado di affidabilità dei metodi di indagine, si v. M. Tart., *et al*., *Cell site analysis; use and reliability*

plicata; motivo per il quale gli esiti emersi non possono essere usati singolarmente, ma devono essere usati a supporto di altri elementi di prova.

Un elemento dal quale non si può prescindere è che ogni attività di misurazione fornisce un'indicazione circa la copertura *nel momento in cui è stata condotta l'indagine* e non necessariamente fornisce dettagli *sullo stato di copertura cellulare*[61] *al momento in cui gli eventi oggetto di accertamento si sono verificati*[62]. Pertanto, l'unica conclusione che si può trarre da questo accertamento è che dato l'aggancio di un telefono a una determinata stazione base, quel telefono si trovava all'interno dell'area di copertura servita da quella antenna BTS nel momento in cui il dispositivo riceveva o trasmetteva.

Uno dei limiti più evidenti in tale analisi è dato dal fatto che le reti possono cambiare nel tempo; pertanto, potrebbero esserci differenze tra il momento in cui è avvenuto il fatto delittuoso e il momento in cui viene svolta l'indagine. Tali differenze possono ad esempio individuarsi in modifiche dell'ambiente (sono state aggiunte o rimosse delle antenne BTS) oppure nella presenza di guasti anche temporanei delle stesse apparecchiature[63]. Si tratta quindi di fattori che possono influire sul meccanismo di aggancio tra la cella e il terminale, andando così a fornire un esito diverso da quello che ci si aspettava.

Un modo per ridurre al mimino il potenziale cambiamento della rete è quello di svolgere le indagini in prossimità del fatto di interesse. Ciò dovrebbe avvenire idealmente entro poche ore o giorni[64], ma è evidente che questo sia obiettivamente impossibile. Pertanto, l'analisi non potrà mai essere svolta nelle stesse situazioni ambientali, atmosferiche e tecniche esistenti al momento dell'evento oggetto di accertamento.

Un ulteriore limite riguarda il dispositivo di rilevamento radio scelto. Esistono diversi strumenti di misurazione, tra i quali *Anite NEMO Handy*[65] e *TEMS*[66], ma non tutti offrono gli stessi servizi. Pertanto, sarà necessario prestare attenzione circa la scelta del dispositivo da utiliz-

of survey methods, in Forensic Science International: Digital Investigation, vol. XXXVIII, 2021, pp. 558-564.

[61] Per approfondimenti sul funzionamento della rete di telefonia mobile v. J. HOY, *op. cit.*

[62] Così in ivi, p. 278.

[63] Cfr. SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE), *Recommendations for Cell Site Analysis* (www.swgde.org/documents/published).

[64] Così in J. HOY, *op. cit.*, p. 279.

[65] www.keysight.com/it/en/product/NTH00000B/nemo-handy-handheld-measurement-solution.html.

[66] www.global-agents.com/contents.php?id=240.

zare, atteso inoltre che gli errori sistematici sono causati o da un malfunzionamento dello strumento o da un suo uso improprio[67]. Tenendo inoltre in considerazione che strumenti di misurazione diversi, potrebbero fornire risultati diversi[68].

Da quanto descritto, si comprende come l'analisi forense dei siti cellulari sia un'operazione complessa, che incorpora diverse tecnologie (della radio, di propagazione, ecc.) e che richiede quindi in capo a chi opera una conoscenza di tali materie, dell'infrastruttura delle reti mobili e di come queste si comportano, nonché una elevata capacità di interpretare i dati contenuti nei tabulati di ogni operatore telefonico.

3. Una panoramica in tema di *best practices*, standard e linee guida di riferimento

Se da un lato la natura dei dati esteriori delle conversazioni, quali dati digitali, impone che questi siano trattati nel rispetto dell'ISO/IEC 27037, dall'altro lato, allo stato attuale, non sono stati pubblicati standard internazionali *ad hoc* al fine di mantenere l'integrità di tali elementi di prova, in particolare prevedendo un'uniformità nel loro trattamento (acquisizione, gestione, produzione e trasmissione) e nella loro analisi.

Linee guide di riferimento non si trovano nemmeno nelle raccomandazioni di settore redatte dal NIST[69] (*National Institute of Standards and Technology*) in tema di trattamento di dispositivi mobili. In tali raccomandazioni sono illustrate le sole caratteristiche della rete cellulare, mentre è assente qualsiasi standard tecnico per il trattamento, analisi, convalida o attenuazione degli errori degli elementi di prova relativi ai record di chiamata (*Call Detail Record*) e ai record relativi alla localizzazione *(Cell Site Location Information)*.

Si individuano invece delle linee guida nazionali specifiche che meritano di essere citate auspicando che possano essere degli "apripista" nella formulazione di standard e protocolli nell'ambito in parola.

Si tratta, per esempio, del "*Codes of Practice and Conduct – For Forensics Science Providers and Practitioners in the Criminal Justice*

[67] Cfr. J.B. Minor, 2019*, cit.*, p. 64.
[68] Cfr. M. Tart, *et al.*, *Cell site analysis,* cit.
[69] www.nist.gov.

System"[70], a cui è allegato "*Appendix: Digital Forensics – Cell Site Analysis*"[71], codice vigente in Inghilterra e Galles (che può essere esteso o adottato anche da altre giurisdizioni previa approvazione degli organi preposti) emanato dal *Forensic Science Regulator,* figura che ha il ruolo di garantire che la fornitura dei servizi di scienze forensi in tutto il sistema di giustizia penale del Regno Unito sia conforme a un elevato standard di qualità scientifica. Il codice, che non si sostituisce alle ISO/IEC di riferimento, descrive in dettaglio gli standard e le linee guida che dovrebbero essere rispettate da tutti i professionisti delle scienze forensi, indipendentemente dal settore in cui sono impegnati e se l'incarico è stato commissionato dall'accusa o dalla difesa[72].

Le altre linee guida di interesse che meritano di essere citate sono *SWGDE Recommendations for Cell Site Analysis*[73] redatte dallo *Scientific Working Group on Digital Evidence* (SWGDE) gruppo di lavoro scientifico statunitense che riunisce le organizzazioni impegnate nel campo delle prove digitali con lo scopo di rafforzare la cooperazione tra gli enti e garantire la qualità e coerenza delle attività svolte dalla comunità forense.

Nello specifico, l'appendice al *Codes of Practice and Conduct* definisce:

- l'oggetto dell'analisi del sito cellulare (acquisizione, elaborazione dei dati, spesso in associazione con i riscontri emersi durante un'attività di misurazione della propagazione della radiofrequenza e presentazione dei risultati);
- i requisiti soggettivi in capo a chi compie l'attività (indipendenza, imparzialità e integrità);
- le garanzie in capo al cliente (deve essere informato circa i limiti dell'attività tecnica);
- cosa deve includere la procedura che definisce l'impostazione della strategia (circostanze del caso, dati disponibili su cui si baserà l'analisi, i limiti di tali dati, i requisiti del sondaggio, ecc.);

[70] www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2021-issue-7.

[71] www.gov.uk/government/publications/cell-site-analysis.

[72] In argomento v. G. TULLY, *et al.*, *Quality standards for digital forensics: Learning from experience in England & Wales*, in Forensic Science International: Digital Investigation, vol. XXXII, 2020.

[73] www.swgde.org/documents/published.

- un controllo dei record e dei risultati (o attraverso un processo di convalida o tramite un processo di revisione da parte di un secondo incaricato);
- le competenze di ogni analista nella gestione dei record e nell'esecuzione di un'indagine di misurazione delle propagazioni delle radiofrequenze;
- la procedura di convalida dei metodi utilizzati durante l'analisi;
- la valutazione del rischio dei metodi (utilizzata per sviluppare un piano di validazione), atteso che per ogni metodo applicato nell'analisi dei siti cellulari ci sono incertezze intrinseche;
- i requisiti di ogni report e relazione tecnica;
- infine, riporta un glossario di riferimento.

Il SWGDE fornisce delle raccomandazioni più prettamente di tipo tecnico sull'uso dei dati contenuti nei tabulati di traffico per una loro corretta interpretazione. In particolare:

- descrive la tipologia di documentazione che può essere utile richiedere al gestore per svolgere un'analisi dei siti cellulari più approfondita (elenco dei siti cellulari, mappe di copertura, ecc.);
- suggerisce al professionista di documentare il processo e le procedure utilizzate per condurre l'analisi;
- descrive i limiti e le problematiche che il tecnico potrebbe incontrare durante l'analisi dei tabulati (atteso che i formati prodotti dai gestori non sono uniformi tra di loro), motivo per il quale raccomanda che ciascun consulente debba possedere competenze specifiche;
- fornisce alcune definizioni utili da tenere in considerazione durante l'attività di misurazione;
- prevede un procedimento di convalida dei risultati;
- fornisce raccomandazioni per la redazione della relazione tecnica in merito all'elaborazione e presentazione dei dati.

Entrambe le linee guida citate, tra le diverse indicazioni fornite, prevedono la convalida[74] dei metodi di indagine e degli strumenti (quindi

[74] Cfr. J.B. Minor, *Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology*, in Journal of Digital Forensics, Security and Law, vol. I, n. 2, Article 7, 2017; M. Tart, *et al*., *Cell site analysis,* cit., p. 568. In tema di convalida, si discute sulla corretta previsione di

dell'attrezzatura scelta e il modo in cui viene utilizzata) e forniscono inoltre indicazioni sul contenuto della relazione tecnica[75].

La convalida, insieme alla mitigazione degli errori di un'analisi, è infatti fondamentali per assicurare risultati di analisi affidabili e ripetibili, rispondenti ai criteri di Daubert[76] in tema di prova scientifica.

Quanto alla redazione della relazione tecnica[77], la regola generale è che il consulente dovrà esprimersi in modo chiaro e comprensibile, tenuto conto che si rivolgerà a persone che non hanno conoscenze specifiche in quel determinato settore. Per tale ragione, sarà necessario spiegare i termini tecnici utilizzati tramite l'inserimento di un glossario e l'utilizzo di metafore o parallelismi con le conoscenze diffuse comuni all'uomo medio o derivate da altre scienze forensi più "conosciute", quali ad esempio la medicina legale[78]. Inoltre, la relazione dovrà contenere preliminarmente i criteri, gli strumenti e i metodi di indagine utilizzati, i quali potranno successivamente essere verificati dal giudice e dalle altre parti. Si proseguirà, poi, con l'esposizione dell'analisi svolta e degli esiti e/o riscontri emersi dalla stessa, documentando il tutto anche attraverso tabelle, immagini o mappe che mostrano ad esempio l'ubicazione delle BTS e dei dispositivi: ciò faciliterà la comprensione di quanto descritto. Infine, saranno riportate le conclusioni a cui si è giunti, alle quali seguirà la bibliografia a sostegno delle proprie valutazioni e il curriculum del consulente per presentarne qualifiche e competenze.

Quanto sin qui detto, è il cuore dell'elaborato tecnico, il quale però dovrà essere necessariamente corredato anche dagli eventuali allegati, che nel caso *de quo* risulteranno essere i tabulati di traffico di interesse,

applicare la ISO/IEC 17025 "*General requirements for the competence of testing and calibration laboratories*", sul punto si v. G. TULLY, *op. cit.*

[75] Una relazione tecnica esaustiva permette di far comprendere l'oggetto e gli esiti degli accertamenti svolti e ne garantisce la loro verificabilità.

[76] In argomento v. R. BRIGHI, C. MAIOLI, *Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologica*, in Informatica e diritto, 2016, XXIV, pp. 217-234.

[77] Sul tema si v. ISO/IEC 27042 "*Guidelines for the analysis and interpretation of digital evidence*"; J. HOY, *op. cit.* p. 279 s.; N. SUNDE, *What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices*, in Science & Justice, vol. LXI, Issue 5, 2021, pp. 586-596; G. HORSMAN, *The different types of reports produced in digital forensic investigations*, in Science & Justice, vol. LXI, Issue 5, 2021, pp. 627-634.

[78] Per esempio, si potrà portare a riflettere il lettore che l'adozione delle linee guida in materia informatica – spesso disattese – sono tanto fondamentali quanto quelle previste per svolgere un esame autoptico o degli accertamenti sul DNA.

gli eventuali verbali di attività di accertamento svolte (è il caso del verbale dell'attività di misurazione); eventuale documentazione di cui si è fatto riferimento nell'elaborato che servirà a corroborare la ricostruzione dei fatti (ossia la documentazione richiesta al gestore telefonico e utilizzata durante l'attività di misurazione); e comunque ogni documento che possa essere utile per supportare quando accertato. Attenzione, tuttavia, a che l'attività tecnica svolta dal consulente di parte non abbia in realtà le vesti di esperimento giudiziale[79]: in tal caso, potrebbe essere dichiarata inutilizzabile in giudizio.

Tramite la relazione tecnica, quindi, sarà possibile desumere l'intero percorso logico alla base dei riscontri emersi e della ricostruzione del fatto posto all'attenzione del giudice.

4. Considerazioni conclusive

I tabulati di traffico, se da un lato forniscono informazioni utili nell'accertamento di un fatto, dall'altro godono di diverse criticità che possono inficiare l'attendibilità dei risultati emersi dalla loro analisi.

Come illustrato, il processo di acquisizione, gestione e produzione dei dati operato dai fornitori non risponde alla ISO/IEC 27037 e, peraltro, manca di uniformità, compromettendo irrimediabilmente la qualità dei dati. Lo stesso vale in tema di analisi, dove i consulenti operano in un campo che gode di incertezze intrinseche a prescindere dalla metodologia di indagine applicata e che peraltro è privo di standard di settore, utili a garantire l'affidabilità di quanto accertato.

Per mitigare gli errori nelle conclusioni dei tecnici, si pone quindi l'esigenza di formulare una metodologia condivisa per il trattamento e l'analisi dei dati di traffico.

In tema di trattamento e integrità, una soluzione è stata individuata nell'uso della tecnologia *Blockchain*. Sul versante dell'analisi, invece, valide linee guida sono state individuate nell'appendice "*Digital Forensics – Cell Site Analysis*" al *Codes of Practice and Conduct* e nelle "*SWGDE Recommendations for Cell Site Analysis*".

[79] Mezzo di prova disposto dal giudice che consiste «nella riproduzione, per quanto è possibile, della situazione in cui il fatto si afferma o si ritiene essere avvenuto e nella ripetizione delle modalità di svolgimento dello stesso» (artt. 218 c.p.p. e s.).

La previsione di standard e linee guida però non è sufficiente. Il consulente incaricato a svolgere la analisi deve possedere specifiche competenze circa l'uso e l'interpretazione corretta dei dati, sul funzionamento della rete di telefonia mobile, sull'uso dei software e della strumentazione, nonché essere a conoscenza dei relativi limiti.

In definitiva, solo quando saranno fornite delle metodologie idonee a garantire il corretto trattamento dei dati esteriori delle conversazioni da parte di tutti gli attori coinvolti nelle indagini forensi, si potrà avere una maggiore accuratezza dei risultati e vedere assicurata la credibilità e l'attendibilità di tali prove digitali assunte nel processo che saranno poi valutate da parte del giudice.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464308
pp. 137-155 (gennaio 2022)

Il captatore che non c'è: ovvero perché il captatore potrebbe non entrare più nelle aule di tribunale

Alfonso Buccini[1], Donato Eugenio Caccavella[2]

1. Premessa

Negli ultimi anni lo sviluppo delle tecnologie di intercettazione a fini di individuazione degli elementi di prova per identificare gli autori di reati, nello specifico il captatore informatico, ha determinato da parte del legislatore una continua rincorsa per normare l'uso di questo insidioso strumento di ricerca della prova.

Ad un primo tentativo a fine 2017 con il cosiddetto "decreto Orlando" (d.lgs. 29 dicembre 2017 n. 216) mai entrato pienamente in vigore, ha fatto seguito nel 2019-2020 la "riforma Bonafede", (d.l. 30 dicembre 2019 n. 161 convertito, con modificazioni, dalla legge n. 7 del 28 febbraio 2020), anch'essa tuttavia mai pienamente attuata anche in ragione della mancata emanazione, ad oggi, di alcuni importanti decreti ministeriali attuativi. Ciò ha determinato, come anche la cronaca giudiziaria ha testimoniato, una serie di abusi e criticità nell'utilizzo di questo strumento di ricerca della prova che vanno a ledere la *privacy* e altri diritti fondamentali dei cittadini intercettati.

In questo contributo vengono ripercorsi i passi salienti dei due progetti di riforma attraverso l'analisi dei punti più controversi degli stessi, delle criticità non sanate e l'individuazione delle possibili soluzioni. Inoltre, saranno analizzati diversi aspetti tecnologici in contrapposizione con le *best practices* dell'informatica forense che porteranno a considerare i dati acquisiti da tali programmi scientificamente e giuri-

[1] Centro Studi Informatica Giuridica (CSIG) – Osservatorio di Bologna.
[2] Professore a contratto di Computer forensics, Università Statale di Milano; *Digital Forensics Expert*.

dicamente inutilizzabili, se non dovessero essere imposti e adottati rigorosi accorgimenti tecnici organizzativi di sicurezza informatica.

2. La riforma del sistema delle intercettazioni: dal decreto legislativo n. 216 del 2017 alla riforma "Bonafede"

2.1. *La delega legislativa nella legge di riforma del codice penale e del codice di procedura penale*

Dopo i vari tentativi di proposte di legge per regolare la materia andati a vuoto, fra cui la proposta nota come "proposta Quintarelli[3]" , fu con la legge delega di riforma del codice penale e del codice di procedura penale, meglio conosciuta come "delega Orlando", la legge 23 giugno 2017 n. 103 "Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario" – commi da 82 a 84 dell'art. 1 – pubblicata sulla Gazzetta Ufficiale Serie Generale n. 154 del 4 luglio 2017, che prese l'avvio il progetto governativo di riforma del sistema delle intercettazioni di conversazioni e comunicazioni; criteri di delega molto simili sia ad alcune circolari interne delle procure emanate negli anni 2015 e 2016 che ai principi espressi nella sentenza della Corte di cassazione a SS.UU. n. 26889 del 1° luglio 2016[4] che aveva legittimato l'uso del captatore informatico nelle attività di indagine per delitti di terrorismo e criminalità organizzata.

2.2. *Il decreto legislativo delegato: d.lgs. n. 216 del 2017*

A seguito della delega legislativa contenuta nella legge di riforma del codice penale e del codice di procedura penale e su iniziativa del Ministro della Giustizia allora in carica, Andrea Orlando, nel mese di novembre del 2017 il Consiglio dei Ministri provvide all'emanazione di una versione preliminare del decreto legislativo per l'ottenimento di tutti i pareri necessari fra cui quello delle competenti Commissioni Parlamentari Giustizia[5].

[3] Cfr. testo integrale al link: https://www.camera.it/leg17/126?idDocumento=4260.

[4] Cfr. testo integrale al link: https://archiviopenale.it/intercettazioni--cass-sez-un-1-luglio-2016-(cc-28-aprile-2016)-scurato/contenuti/6142.

[5] Per maggiori dettagli sul punto sia consentito di rimandare a, A. Buccini, M. Ferrazzano, *Il captatore come strumento di indagine: quali garanzie?*, in G. Costabile, A. Attanasio, M. Ianulardo (a cura di), IISFA Memberbook 2018, Edizioni InMagazine, 2018. pp. 131-142.

Acquisiti tutti i pareri e le necessarie autorizzazioni, il decreto legislativo 29 dicembre 2017 n. 216 fu infine pubblicato sulla Gazzetta Ufficiale n. 8 del giorno 11 gennaio 2018, con la previsione che le norme di cui agli articoli 1 e 6 del decreto legislativo sarebbero entrate in vigore trascorsi quindici giorni dalla pubblicazione, mentre le altre norme trascorsi 180 giorni, ovvero entro la seconda metà del mese di luglio, ciò per dare modo alle procure della Repubblica di adeguare i locali e gli impianti tecnologici delle procure medesime alle previsioni normative contenute nel decreto.

Ad integrazione e completamento dello stesso decreto legislativo, l'art. 7 prevedeva poi l'emanazione di due d.m. attuativi da parte del Ministero della Giustizia, il primo nel quale dovevano essere stabiliti i requisiti tecnici dei programmi informatici "funzionali all'esercizio delle intercettazioni mediante inserimento di captatore informatico su dispositivo elettronico portatile" e il secondo sui criteri attraverso i quali il Procuratore della Repubblica, sentito il Garante Privacy, avrebbe dovuto disciplinare l'accesso all'*archivio riservato* (novità introdotta dall'anzidetto decreto) dove dovevano essere conservate tutte le intercettazioni acquisite.

I due suddetti decreti furono poi condensati nel d.m. Giustizia del 20 aprile 2018 pubblicato sul Bollettino Ufficiale del 31 maggio, decreto che tuttavia si è rivelato quanto mai generico e non ha risolto i molti dubbi degli addetti ai lavori, in particolare per quanto riguarda le specifiche tecniche dei captatori.

L'*archivio riservato* a cui si è accennato è uno degli aspetti, non l'unico del provvedimento, che evidenzia come la questione della "riservatezza" [6] sia la caratteristica principale sia della delega legislativa che del decreto delegato.

Fra le criticità del provvedimento rilevate vanno segnalate l'eccessiva discrezionalità concessa alla polizia giudiziaria nella fase di selezione delle intercettazioni fra intercettazioni rilevanti, intercettazioni non rilevanti e intercettazioni contenenti dati definiti "sensibili" e le scarse tutele difensive, evidenti sia nei tempi ristretti concessi alle difese per l'esame e l'ascolto delle intercettazioni una volta depositate nell'*archivio riservato* e per eventualmente proporne di nuove a tutela del proprio assistito e sia dal divieto, per il difensore, di farsi assistere in questa sede da un consulente tecnico o di ammettere all'ascolto dei

[6] Sul punto si veda, C. Conti, *La riservatezza delle intercettazioni nella delega Orlando*, in *Diritto penale contemporáneo*, 2017, 3.

brani l'imputato, imputato la cui presenza avrebbe consentito al difensore una maggiore comprensione dei contenuti intercettati e quindi di riflesso una maggiore tutela delle esigenze difensive[7].

2.3. *Dai rinvii dell'entrata in vigore del "decreto Orlando" alle modifiche introdotte dalla legge 9 gennaio 2019, n. 3*

Nel periodo intercorrente fra la pubblicazione in Gazzetta Ufficiale del "decreto Orlando" e l'entrata in vigore di tutto l'articolato, prevista per la fine del mese di luglio del 2018, si tennero le elezioni politiche che determinarono un cambio di maggioranza governativa ed un conseguente cambio della titolarità del Ministero della Giustizia.

In ragione di ciò, l'entrata in vigore delle ulteriori norme del d.lgs. n. 216 del 2017 fu più volte differita, i differimenti furono ufficialmente motivati dalle stesse ragioni che avevano disposto il primo rinvio contenuto nell'art. 9, comma 1, del "decreto Orlando", ovvero la necessità di adeguare le infrastrutture delle procure alle previsioni normative del decreto medesimo, pur se da parte del Guardasigilli in carica le motivazioni erano soprattutto quelle di intervenire sul provvedimento in maniera incisiva.

Non solo, già il "decreto Orlando" fu oggetto di una rilevante modifica da parte della legge n. 3 del 2019, modifica poi rimasta nella normativa vigente, legge avente ad oggetto "Misure per il contrasto dei reati contro la Pubblica Amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici", meglio nota come "legge Spazzacorrotti", caratterizzata da un taglio fortemente "repressivo" del fenomeno della corruzione e che, fra le altre previsioni normative, è intervenuta a modificare l'art. 6 del "decreto Orlando", articolo che disciplinava l'uso del captatore informatico per l'individuazione dei reati contro la Pubblica Amministrazione, modifica che ha equiparato i reati stessi ai più gravi reati di mafia e terrorismo e quindi autorizzando l'uso *senza limiti* del captatore informatico nelle attività di indagine[8].

[7] Per una approfondita analisi di tutti gli aspetti e le criticità del decreto legislativo n. 216 del 2017 si vedano: G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni, Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Giappichelli, 2018; L. Filippi, *Le nuove norme su intercettazioni e tabulati,* Pacini Giuridica, 2017.

[8] Riguardo l'impatto della legge n. 3 del 2019 sul decreto n. 216 del 2017 si veda, S. Signorato, *Intercettazioni di comunicazioni*, in R. Orlando, S. Seminara (a cura di), *Una nuova legge contro la corruzione*, Giappichelli, 2019, p. 245-259.

Sulla base di quanto sopra, la modifica apportata ha perciò abrogato il comma 2 dell'art. 6 del d.lgs. n. 216 del 2017 come originariamente formulato in sede di prima pubblicazione del "decreto Orlando" ed ha altresì implementato il comma 2-bis dell'art. 266 c.p.p., implementazione in base alla quale il comma 2-bis dell'art. 266 c.p.p. è ora il seguente:

> L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4.

2.4. *Il decreto legislativo n. 161 del 30 dicembre 2019*

In concomitanza con la scadenza dell'ultima proroga fissata dall'art. 9, comma 2 del decreto legge n. 53 del 2019 al 31 dicembre 2019, fu pubblicato il decreto legge n. 161 del 30 dicembre 2019 "Disposizioni urgenti in materia di intercettazioni" sulla Gazzetta Ufficiale n. 305 del 31 dicembre 2019, decreto che si è caratterizzato, come vedremo, per un intervento molto incisivo sulla precedente disciplina anche se questa non era mai entrata nel pieno della sua vigenza.

Lo stesso decreto legge n. 161 è stato poi convertito, con modifiche anche abbastanza rilevanti, dalla legge n. 7 del 28 febbraio 2020: legge e testo coordinato sono stati pubblicati sulla Gazzetta Ufficiale n. 50 del 28 febbraio 2020.

Le modifiche rispetto alla normativa precedente sono particolarmente incisive: ad uno sguardo d'insieme si assiste ad un ritorno ad alcune previsioni normative antecedenti al d.lgs. n. 216 del 2017, pur se tuttavia si rilevano anche opportuni interventi volti a sanare le criticità che la dottrina e gli addetti ai lavori avevano avuto modo di evidenziare nei contenuti del precedente provvedimento.

Soffermandoci sugli elementi di novità del nuovo decreto preme evidenziare che, accogliendo un suggerimento da parte dei procuratori della Repubblica, l'operatività delle norme del decreto legge n. 161 non è più da collegare come a suo tempo previsto dal "decreto Orlando" alla data del provvedimento che dispone le intercettazioni, ma alla data di

iscrizione dello stesso nel *registro*, in modo da evitare che nel passaggio da una norma ad un'altra (nello specifico dal d.lgs. n. 216 del 2017 al dl n. 161 del 2019 ed alla sua legge di conversione) si potesse verificare il caso di trovarsi di fronte a regole differenti per lo stesso procedimento. Proseguendo, gli altri interventi correttivi apportati dal decreto legge n. 161 possono essere così sinteticamente riassunti:

1. ampliamento della categoria dei delitti per i quali è consentito procedere alle intercettazioni tra presenti con captatore informatico, includendo anche i delitti commessi dagli "incaricati di pubblico servizio" per i reati commessi contro la Pubblica Amministrazione e puniti con la pena della reclusione non inferiore nel massimo a cinque anni. La definizione di "incaricato di pubblico servizio" la rinveniamo nell'articolo 358 del codice penale;
2. con riferimento ai suddetti delitti commessi dai pubblici ufficiali e dagli incaricati di pubblico servizio contro la P.A., l'estensione della regola, già valevole per i delitti di cui all'art. 51 commi 3-*bis* e 3-*quater* c.p.p. secondo cui nel decreto autorizzativo delle intercettazioni tra presenti con captatore informatico non è necessario indicare i luoghi ed il tempo in relazione ai quali è consentita l'attivazione del microfono;
3. l'introduzione di un più ampio regime di utilizzabilità i fini della prova dei delitti di criminalità organizzata e di quelli dei pubblici ufficiali e degli incaricati di pubblico servizio contro la P.A. dei risultati delle intercettazioni disposte con riferimento a delitti diversi (art. 270, comma 1, c.p.p.);
4. nuove tempistiche e modalità per la trasmissione di verbali e delle registrazioni dalla polizia giudiziaria al Pubblico Ministero e per il trasferimento di detto materiale all'*archivio digitale* (non più all'*archivio riservato* come nella precedente disciplina del "decreto Orlando" a sottolineare la minore attenzione alla questione della *riservatezza*) e lo snellimento della procedura per l'acquisizione delle intercettazioni rilevanti e il trasferimento al suddetto archivio, procedura che era risultata alquanto farraginosa nella parte "decreto Orlando" ad essa dedicata.

Oltre ai suddetti elementi di novità, quello che a nostro avviso è da considerare come il principale punto di forza dell'attuale normativa in vigore è il fatto di aver riportato tutta l'attività di selezione delle inter-

cettazioni fra quelle rilevanti, quelle non rilevanti e quelle contenenti dati cosiddetti "sensibili" sotto il controllo del Pubblico Ministero, come sottolineato anche dal Governo e dal Ministro allora in carica nel momento della presentazione alla stampa dei contenuti del decreto legge, a conferma che quanto più volte evidenziato dalla dottrina e dagli addetti ai lavori circa le criticità del "decreto Orlando" sul ruolo subalterno del Pubblico Ministero nei confronti della polizia giudiziaria relativamente all'attività di selezione delle intercettazioni fra intercettazioni rilevanti, intercettazioni non rilevanti e intercettazioni contenenti dati sensibili era una critica fondata.

Il rappresentante dell'accusa per quanto riguarda questa importante fase dell'attività di selezione delle intercettazioni rilevanti ai fini della formazione del fascicolo processuale torna ora infatti a rivestire una duplice veste: quella di fornire indicazioni e direttive alla polizia giudiziaria sulla selezione delle intercettazioni e allo stesso tempo vigilare sulla corretta esecuzione da parte della polizia giudiziaria delle direttive impartite.

La stessa polizia giudiziaria continua, tuttavia, ad avere un ruolo importante per quanto riguarda le attività di ascolto prima e selezione poi del materiale intercettato, solo che il Pubblico Ministero viene ora a ricoprire quel ruolo di direzione e controllo che la precedente normativa non gli riconosceva anche se i pubblici ministeri, in risposta alle critiche provenienti dalla dottrina e dagli addetti ai lavori, avevano sempre ribadito di esercitarla in ogni caso.

Infine, per quanto riguarda un'altra rilevante modifica apportata dal decreto legge 161 del 2019 rispetto al "decreto Orlando", questa è costituita dal ripristino della cosiddetta *udienza stralcio* per l'acquisizione degli atti delle intercettazioni al fascicolo processuale, udienza che il decreto legislativo precedente aveva sostituito con una procedura ben più complessa e farraginosa che aveva sollevato molti rilievi e molte critiche.

Se l'attuale normativa vigente presenta i punti di forza sopra richiamati, non è tuttavia esente da critiche in quanto fra gli interventi attuati essa ha cancellato, fra le altre previsioni, la permanenza del segreto sulle comunicazioni intercettate dopo l'attività di *discovery* a favore della difesa e fino alla conclusione della procedura selettiva.

Le criticità in sede di tutele difensive a suo tempo evidenziate dagli addetti ai lavori[9] nella precedente normativa, seppure in qualche modo parzialmente sanate in sede di conversione del d.l. n. 161/2019 in legge,

[9] Si veda al riguardo, G. Giostra, R. Orlandi (a cura di), *op. cit.*

relativamente alla possibilità per i difensori stessi di estrarre copia delle intercettazioni e dei verbali una volta che questi saranno stati depositati alla conclusione delle indagini (possibilità non prevista in sede di emanazione del decreto legge n. 161/2019, ma introdotta in sede di conversione in legge dello stesso dopo le giuste rimostranze di alcune Camere Penali), non eliminano tuttavia i rilievi critici su tale punto[10] in quanto, le pur limitate facoltà concesse alla difesa di ascoltare le registrazioni ed eventualmente proporne di nuove da acquisire al fascicolo a tutela del proprio assistito, andranno esercitate in un tempo di venti giorni non soggetto ad ulteriore proroga, tempo che appare assai limitato, in modo particolare per ciò che riguarda quei procedimenti, perlopiù relativi a reati di criminalità organizzata, contenenti numerosissime intercettazioni spesso da comprendere e da tradurre con l'aiuto di un interprete in quanto contenenti espressioni dialettali di difficile comprensione.

Rimane inoltre aperta con la normativa vigente la questione della tutela delle conversazioni fra difensore e assistito in quanto, pur se non utilizzabili a fini probatori, queste conversazioni possono essere captate e il Pubblico Ministero ne può avere cognizione, situazione che determina per il titolare dell'accusa un considerevole vantaggio nella definizione della strategia processuale.

Successivamente alla emanazione del decreto legge e della sua legge di conversione, il Ministero della Giustizia è intervenuto, con circolari e decreti attuativi reperibili sul sito del Ministero[11] su varie questioni, fra le quali anche sulla questione relativa alla determinazione dei soggetti legittimati all'accesso alle sale d'ascolto: per quanto riguarda la difesa è stato ribadito che quali soggetti legittimati all'accesso vengono indicati esclusivamente gli "interpreti" e non i consulenti tecnici e meno che mai gli imputati, figure che, come già rilevato in sede di analisi della precedente normativa, avrebbero consentito al difensore di comprendere al meglio alcuni passaggi delle conversazioni intercettate e di esercitare in maniera più incisiva il proprio mandato.

L'auspicio è che, non essendo tale presa di posizione del Ministero sul punto una posizione "tassativa" e auspicando che il problema sull'accesso alle sale di ascolto degli interpreti e dell'imputato venga

[10] Sugli aspetti critici della riforma delle intercettazioni relativamente alle tutele difensive si veda F.S. Maisano, C.M. Piazza, *La nuova riforma delle intercettazioni: il fine giustifica i mezzi*?, contributo consultabile al seguente link: https://www.bolognaforense.net/2020/12/la-nuova-disciplina-delle-intercettazioni-il-fine-giustifica-i-mezzi/.

[11] *Cfr.* testo integrale al link: https://www.giustizia.it/giustizia/it/mg_2_9_19.page.

risolto dalla "prassi", si arrivi in futuro a consentire l'accesso alle suddette sale di ascolto anche al consulente tecnico e all'imputato per garantire così al meglio il diritto di difesa.

Va segnalato infine, sulla riforma nel suo complesso, un esaustivo intervento del Consiglio Superiore della Magistratura che con una delibera del 28 luglio 2021[12] ha approvato una risoluzione avente ad oggetto "Ricognizione di linee guida e buone prassi in materia di intercettazioni a seguito della entrata in vigore della riforma della disciplina delle intercettazioni di conversazioni e di comunicazioni" nella quale, fra le altre, vengono affrontate le problematiche derivanti dalla coesistenza di un archivio informatico e di un archivio digitale, la mancanza di "comunicazione" fra i diversi archivi in dotazione alle procure, invitando il Ministero della Giustizia ad intervenire sul punto per quanto riguarda le problematiche di sua competenza e a fornire assistenza ai magistrati alle prese con l'uso degli applicativi.

2.5. *L'uso del captatore in procedimenti diversi*

Fra gli aspetti della riforma che si sono rivelati più controversi e che ancora oggi sono oggetto di pronunce da parte della giurisprudenza di merito, va segnalata la questione relativa alla utilizzabilità delle intercettazioni in procedimenti diversi, disciplinata dall'art. 270 c.p.p., articolo che ha subito rilevanti modifiche sia ad opera del decreto legge n. 161 del 2019 che della sua legge di conversione. Fra le modifiche, in particolare, al comma 1 è stato stabilito che:

> I risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'articolo 266, comma 1.

Inoltre, la norma è intervenuta introducendo una previsione specifica per disciplinare l'utilizzo delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile, previsione specifica di cui al comma *1-bis* dell'art. 270 c.p.p. in base al quale

[12]Cfr. testo integrale al link: https://sistemapenale.it/pdf_contenuti/1630856282_csm-risoluzione-intercettazioni-delibera-28-luglio-2021.pdf.

> Fermo restando quanto previsto dal comma 1, i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione qualora risultino indispensabili per l'accertamento dei delitti indicati dall'articolo 266, comma 2-*bis*.

Questa nuova formulazione dell'art. 270 c.p.p. nella quale i concetti di "rilevanza", "necessarietà" ed "indispensabilità" acquistano particolare importanza ai fini della utilizzabilità dei risultati delle intercettazioni in procedimenti diversi, fanno comprendere come nelle aule di tribunale l'interpretazione degli stessi sarà alla base delle contrapposizioni fra accusa e difesa e delle decisioni dei Giudici.

Successivamente all'entrata in vigore della riforma, sull'utilizzabilità dei risultati delle intercettazioni in procedimenti diversi si sono registrati vari interventi della giurisprudenza di merito: a titolo esemplificativo e non esaustivo citiamo fra tali interventi la recente sentenza della VI sezione penale della Corte di Cassazione del 14 giugno 2021 n. 23244 [13] la quale esclude l'applicabilità del principio di diritto fissato nella precedente sentenza n. 51 del 2020[14] in materia di utilizzazione dei risultati delle intercettazioni in procedimenti diversi, sentenza emessa prima dell'entrata in vigore della riforma e nella quale la Cassazione a Sezioni Unite assunse una posizione garantista sulla questione, quando, dopo l'attività di captazione, l'imputazione venga riqualificata in altra non annoverata nello specifico elenco di cui all'art. 266 c.p.p.[15].

[13] Cfr. testo integrale al link*:* https://www.giurisprudenzapenale.com/wp-content/uploads/2021/07/cass-pen-2021-23244.pdf.

[14] Cfr. testo integrale al link*:* https://www.giurisprudenzapenale.com/2020/01/03/depositata-la-sentenza-delle-sezioni-unite-sullutilizzazione-in-altri-procedimenti-dei-risultati-delle-intercettazioni-art-270-c-p-p/.

[15] Sulla utilizzabilità delle intercettazioni in procedimenti diversi si veda anche, M. Grifo, *Quale connessione per l'utilizzabilità delle intercettazioni in procedimenti diversi ? Inevitabile una nuova investitura delle Sezioni Unite*, in Sistema Penale, contributo consultabile al seguente link: https://www.sistemapenale.it/it/sentenza/cassazione-37407-2020-connessione-utilizzabilita-intercettazioni-procedimenti-diversi-270-cpp.

3. Questioni tecniche sul captatore

3.1. *Il lato oscuro del captatore*

Effettuato l'inquadramento giuridico e giurisprudenziale dello "strumento captatore" si entra ora nel merito degli aspetti tecnici analizzandoli in chiave critica. In via preliminare però si rende necessario sinteticamente illustrare le caratteristiche e le funzionalità tecniche che caratterizzano un captatore[16].

Un captatore informatico è un software che è in grado di installarsi e di porsi in esecuzione su un sistema informatico all'insaputa del suo utilizzatore, utilizzando vulnerabilità di sicurezza. Nello specifico, è corretto classificare il captatore informatico quale *trojan*[17], ovvero software installato su un sistema informatico (personal computer, smartphone, tablet) che lo trasformano in una sorta di "cimice" mobile[18].

I captatori informatici sono quindi software che, previa installazione e attivazione sul dispositivo *target*, consentono di intercettare e inviare a terzi i dati di interesse che difficilmente potrebbero essere raccolti in altri modi in quanto spesso i dati informatici vengono trasmessi in maniera cifrata, casi in cui il traffico dati non è intellegibile, con la conseguenza che pur entrando in possesso di tali dati informatici senza la relativa chiave di decifratura non è possibile in alcun modo rilevarne il patrimonio informativo.

Va inoltre precisato che i captatori informatici permettono un numero particolarmente significativo di ulteriori operazioni: la possibilità di consultare i dati presenti sul supporto realizzando una perquisizione informatica da remoto con la sostanziale possibilità di estrarre copie di dati consultati; la possibilità di registrare audio e video locali mediante attivazione di microfono e videocamera; la possibilità di carpire password utilizzando una modalità *keylogger*; la possibilità di creare *screenshot* o generare un filmato di ciò che vede a schermo l'utilizzatore[19]. Tuttavia,

[16] M. Ferrazzano, *Considerazioni sul captatore informatico",* in R. Brighi, M. Palmirani, M. Sanchez Jordan (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza*, Aracne, 2018, p. 283-296.

[17] M. Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017.

[18] A. Buccini, M. Ferrazzano, *op cit*.

[19] R. Brighi, *Requisiti tecnici, potenzialità e limiti del captatore informatico. Analisi sul piano informatico-forense*, in G. Giostra, R. Orlandi (a cura di), op.cit., pp. 231-56.

la libertà di azione presuppone anche la possibilità che si possano alterare e/o distruggere dati informatici, in maniera colposa, quanto dolosa: a titolo esemplificativo, creazione di nuovi dati, alterazioni di metadati (ultima lettura, ultima modifica, creazione), cancellazione di contenuti.

3.2. *L'installazione del captatore informatico*

Un captatore informatico può essere inoculato in un sistema informatico in modi diversi[20]:

- la tecnica senza dubbio più evoluta prevede di sfruttare delle vulnerabilità non ancora note (cosiddette *0-day*) che possono essere presenti nel sistema operativo o in software applicativi di terzi parti installati. Il processo di installazione avviene solitamente aprendo un eseguibile (ad esempio, un allegato a un'email che sembra essere un documento o un'immagine e che invece è l'installer del malware) oppure tramite una porzione di codice *javascript* eseguito durante la consultazione di una pagina web;
- l'altra modalità altamente diffusa prevede l'inserimento del captatore all'interno di un altro software; il malware così rimane silente nel sistema sino a quando la persona che ha interesse a utilizzarlo non lo attiva;
- altra tecnica diffusa prevede il mascheramento del malware con un nome di un processo noto, oppure modificando parti di un software normalmente utilizzato dall'utente;
- anche solo disponendo fisicamente del dispositivo per poter effettuare direttamente l'inoculazione.

3.3. *Funzionalità*

Nello specifico, le principali operazioni che possono essere eseguite da un captatore dalle potenzialità assimilabili a quelle di un captatore a seguito della sua attivazione sono le seguenti:

- *attivazione remota del microfono*: il sistema infettato si comporta come una microspia ambientale;

[20] A. Buccini, M. Ferrazzano, *op. cit.*, p. 139.

- *attivazione remota della fotocamera*: il sistema infettato invia fotografia e/o video al soggetto che controlla il captatore;
- *condivisione dello schermo*: il soggetto che controlla il captatore è in grado di visionare la stessa schermata in visione all'utilizzatore;
- *consultazione dei dati presenti*: il sistema infettato permette al soggetto che controlla il captatore di consultare ogni tipo di dato (fotografie, video, chat, email, contatti, elenco chiamate, cronologia, file di tipo documentale, ecc.);
- *keylogger*: il sistema infettato trasmette al soggetto che controlla il captatore i tasti digitati dall'utilizzatore sulla tastiera, in modo così da rivelare dati che di norma non vengono salvati come le password;
- *geolocalizzazione*: il sistema infettato comunica al soggetto che controlla il captatore la posizione GPS del dispositivo (al netto del margine di errore della tecnologia);
- *interazione*: il soggetto che controlla il sistema infetto può eseguire delle operazioni, comandi e applicazioni da remoto, sia in maniera occulta che mostrando l'azione alla vittima;
- *alterazione dei dati*: il soggetto che controlla il sistema infetto può modificare, creare, cancellare, distruggere, cifrare dati presenti in esso[21].

Pertanto, alla luce di quanto esposto, senza farsi distrarre da una concezione analogica del captatore come mero e semplice strumento di acquisizione di contenuti audio, si può concludere che il captatore è di fatto uno strumento di acquisizione forense di dati informatici presenti sul dispositivo *target*[22].

Infatti, il captatore, oltre a permettere l'acquisizione di dati informatici "ordinari" presenti sul sistema *target*, consente di acquisire anche immagini, conversazioni audio e posizioni geografiche; quindi, effettua una acquisizione di dati informatici. Le stesse conversazioni audio che sono analogiche in quanto fisiche, una volta captate diventano dati digitali e quindi acquisite e inviate in forma di dato digitale. Motivo per il quale va doverosamente precisato che il captatore deve rispondere ai principi dell'informatica forense secondo le indicazioni dello standard

[21] R. Brighi, *op. cit.*

[22] M. Griffo, *ll captatore informatico e la filosofia del doppio binario*, Editoriale Scientifica, 2019.

ISO/IEC 27037 e secondo le modalità previste dal Codice di Procedura Penale e, in particolare, da quanto previsto dalla L. 48/2008[23].

I dati informatici acquisiti dal captatore, a causa della loro natura intangibile e volatile, sono facilmente soggetti a rischi di alterazione, contraffazioni e malfunzionamento del sistema che li tratta[24]. Ne consegue che il trattamento del dato informatico deve seguire precisi protocolli tecnici nel rispetto del quadro normativo su indicato. Dal punto di vista tecnico, infine, un corretto approccio metodologico impone l'esigenza di garantire l'immodificabilità dei dati oggetto di raccolta, la loro integrità rispetto ai dati originari, la completezza dei dati acquisiti e la corretta conservazione.

Pertanto, il captatore come strumento software, ma anche tutta l'infrastruttura informatica che tratta e conserva i dati acquisita da tale strumento, ovvero l'intero "sistema captatore" inteso come insieme di tecnologia e organizzazione deve fornire tutte le garanzie che l'informatica forense prevede sia in termini scientifici che giuridici.

Sul punto preme richiamare la Sentenza della Corte Costituzionale n.113/2015 che per fattispecie estremamente meno gravi di quelle che prevedono l'utilizzo del captatore, quale la violazione dei limiti di velocità, ha esposto il seguente principio giuridico-scientifico di cui riportiamo uno stralcio utile per successivi riferimenti:

> È evidente che, al fine di dare effettività ai meccanismi repressivi delle infrazioni ai limiti di velocità, la disposizione realizza in modo non implausibile e non irragionevole un bilanciamento tra la tutela della sicurezza stradale e quella delle situazioni soggettive dei sottoposti alle verifiche. È vero, infatti, che la tutela di questi ultimi viene in qualche modo compressa per effetto della parziale inversione dell'onere della prova, dal momento che è il ricorrente contro l'applicazione della sanzione a dover eventualmente dimostrare – onere di difficile assolvimento a causa della irripetibilità dell'accertamento – il cattivo funzionamento dell'apparecchiatura. Tuttavia, detta limitazione trova una ragionevole spiegazione nel carattere di affidabilità che l'omologazione e la taratura dell'autovelox conferiscono alle prestazioni di quest'ultimo.
> In definitiva il bilanciamento realizzato dall'art. 142 del codice della strada ha per oggetto, da un lato, interessi pubblici e privati estremamente rilevanti quali la sicurezza della circolazione, la garanzia dell'ordine pubblico, la preservazione dell'integrità fisica degli individui, la conservazione dei beni e,

[23] C. Maioli (a cura di), *Questioni di informatica forense*, Aracne, 2015.

[24] S. Aterno, P. Mazzotta, *La perizia e la consulenza tecnica – con approfondimento in tema di Perizie Informatiche* (analisi e schede tecniche di D. Caccavella), CEDAM, 2006.

> dall'altro, valori altrettanto importanti quali la certezza dei rapporti giuridici ed il diritto di difesa del sanzionato. Detto bilanciamento si concreta attraverso una sorta di presunzione, fondata sull'affidabilità dell'omologazione e della taratura dell'autovelox, che consente di non ritenere pregiudicata oltre un limite ragionevole la certezza della rilevazione e dei sottesi rapporti giuridici. Proprio la custodia e la conservazione di tale affidabilità costituisce il punto di estrema tensione entro il quale la certezza dei rapporti giuridici e il diritto di difesa del sanzionato non perdono la loro ineliminabile ragion d'essere.
> Il ragionevole affidamento che deriva dalla custodia e dalla permanenza della funzionalità delle apparecchiature, garantita quest'ultima da verifiche periodiche conformi alle relative specifiche tecniche, degrada tuttavia in assoluta incertezza quando queste ultime non vengono effettuate.
> In definitiva, se «il giudizio di ragionevolezza [di questa Corte], lungi dal comportare il ricorso a criteri di valutazione assoluti e astrattamente prefissati, si svolge attraverso ponderazioni relative alla proporzionalità dei mezzi prescelti dal legislatore nella sua insindacabile discrezionalità rispetto alle esigenze obiettive da soddisfare o alle finalità che intende perseguire, tenuto conto delle circostanze e delle limitazioni concretamente sussistenti» (sentenza n. 1130 del 1988) e se la prescrizione dell'art. 142, comma 6, del codice della strada nella sua astratta formulazione risulta immune dai richiamati vizi di proporzionalità, la prescrizione dell'art. 45 del medesimo codice, come costantemente interpretata dalla Corte di cassazione, si colloca al di fuori del perimetro della ragionevolezza, finendo per comprimere in modo assolutamente ingiustificato la tutela dei soggetti sottoposti ad accertamento.

La Corte costituzionale ha quindi ritenuto fondamentale che l'agente accertatore segua scrupolosamente una metodologia che permetta di considerare verificabile l'accertamento dell'infrazione, stante la sua natura irripetibile, nel senso di non riproducibilità altrove e con altri strumenti di quanto in quel momento constatato.

Applicando quanto fin qui brevemente considerato al principio scientifico giuridico al captatore, va rilevato che essendo gli accertamenti in parola irripetibili, rientrano in quei casi in cui è dovuto il rispetto dei principi e delle garanzie enunciate dalla Corte costituzionale. Ne deriva, pertanto, che anche nel caso del captatore è necessaria l'osservanza di una scrupolosa metodologia che permetta di verificare l'operato dell'agente accertatore.

La conseguenza di quanto fin qui esposto è giocoforza sillogistica: se per la rilevazione del superamento del limiti di velocità di un veicolo viene richiesto un rigore scientifico e tecnico estremamente elevato, obbligando l'ente accertatore ad adottare strumenti e metodologia opportunamente adeguati a tal fine, in virtù del principio del "bilanciamento

dei valori in gioco[25]", le indagini di natura tecnica svolte con l'uso del captatore devono necessariamente richiede l'adozione di adeguate metodologie e strumenti, al fine di verificare e controllare successivamente l'oggetto delle indagini e quanto ivi accertato. Garanzie che consistono nel permettere alla difesa di poter verificare il corretto funzionamento del "sistema captatore", ovvero del programma inoculato e della relativa infrastruttura tecnologica, in ottemperanza ai principi metodologici dell'informatica forense e della normativa in parola.

Detta in altri termini, la difesa deve poter verificare il corretto funzionamento del captatore e la correttezza dei trattamenti adottati per la gestione dei dati acquisiti, aspetto questo che impone che la stessa debba poter disporre del captatore con il relativo codice sorgente e di tutta la documentazione tecnica e organizzativa della relativa infrastruttura. Quindi, andrebbe data facoltà alla difesa di poter disporre dei seguenti dati:

- copia forense del captatore inoculato per le intercettazioni di cui si chiede l'inutilizzabilità;
- copia forense dei dati generati dal captatore e dati utili per documentare le caratteristiche di integrità e autenticità degli stessi, nonché la riconducibilità del dispositivo oggetto di intercettazione e relativo sigillo elettronico e marcatura temporale;
- copia della documentazione in essere presso l'affidatario del servizio di intercettazione utile per apprezzare il corretto trattamento delle intercettazioni e in generale dei servizi tecnico e organizzativi di supporto.

In ragione di ciò, alla luce di quanto esposto, si può sostenere che la diretta conseguenza dell'impedimento di poter verificare la correttezza del funzionamento del captatore utilizzato comporta certamente una inutilizzabilità scientifica, ma anche giuridica, degli esiti di tutte le acquisizioni ottenute dal captatore. Tenendo sempre bene presente che il captatore è uno strumento di acquisizione forense di dati, cosa ben diversa e molto più complessa di un banale registratore ambientale, per

[25] E. Lestini, *Captatore informatico: tra "tortura digitale" ed esigenze investigative*, in *Ius in Itinere*, 2021.

inconfrontabilità tecnica non è possibile far riferimento all'attuale giurisprudenza relativa a fattispecie di "semplici intercettazioni audio"[26].

Per comprendere come la rilevanza della correttezza della acquisizione dei dati, in termini di integrità, sia fondamentale per garantire giuste indagini è sufficiente immaginare il caso in cui attraverso un captatore venga acquisita, in una intercettazione ambientale, l'espressione *"eliminalo!"* espressione generica, che con il supporto della geolocalizzazione trova certamente una più rilevante interpretazione se detta sul luogo di un omicidio o invece presso un *coiffeur*, riferendosi ad esempio ad un difetto del taglio dei capelli. Questo semplice esempio fa comprendere come l'acquisizione dei dati effettuata con il captatore deve fornire le massime garanzie di autenticità e integrità ed essere scevra da qualsiasi pregiudizio di alterazione, anche solo colposa, da parte degli inquirenti e/o dai fornitori dei servizi informatici[27].

3.4. *L'esigenza delle garanzie: il captatore che non c'è*

Alla luce di quanto esposto, quindi, è quanto mai doveroso permettere l'esercizio del diritto di difesa consentendo la verifica del "sistema captatore", però aspetto che va tenuto in considerazione risulta essere che in questo modo il funzionamento di ogni specifico tipo di captatore sarà inevitabilmente di dominio pubblico circostanza che permetterà inevitabilmente la diffusione e la commercializzazione di prodotti software "anti captatore", per certi versi come sta già accadendo per i navigatori satellitari che avvisano della prossimità di un autovelox o come per gli antivirus.

Motivo per il quale si cerca di impedire la diffusione di informazioni in merito al funzionamento dei captatori sia per esigenze relative alla riservatezza di proprietà intellettuale o industriale, ma anche per impedire tecniche di *anti forensics*[28] finalizzate a evitare l'inoculazione di captatori su sistemi informatici che limiterebbero la diffusione e l'utilizzo di un così potente strumento di indagine.

[26] M. Daniele, *L'illusione di domare il captatore informatico*, in La legislazione penale, 2020.

[27] G. Ziccardi, *Il captatore informatico nella "Riforma Orlando": alcune riflessioni informatico-giuridiche*, suppl. a AP, 2018.

[28] L'*Anti forensics* è l'insieme di strumenti, metodi e processi che permettono di rendere inefficaci o comunque limitare attività di acquisizione e analisi tipiche dell'informatica forense. Ad esempio realizzando programmi che riconoscono il captatore e lo rimuovono, oppure semplicemente ne inibiscono il funzionamento.

Pertanto, alla luce di quanto esposto, è molto difficile che un captatore utilizzato in una attività di indagine possa entrare nell'aule di tribunale al fine di permettere l'esercizio di difesa della prova di resistenza, anche solo per il fatto che questi strumenti si sono dimostrati in alcune situazioni fallaci, come alcuni casi di cronaca hanno palesato e le aziende affidatarie dei servizi poco affidabili, sia non permettendo *ex post* di poter avere adeguate e documentate garanzie che i dati acquisiti siano rimasti effettivamente integri e autentici, aspetto questo che estremamente critico in dibattimento, fino ad arrivare come in alcuni casi noti alle cronache di veri e propri casi di acquisizioni o (mal) trattamenti di dati illegittimi o in palese violazione di legge.

Seguendo il *fil rouge* dell'autovelox, una alternativa ad una analisi diretta del captatore potrebbe essere quella di istituire un organo che verifichi la adeguatezza dei "sistema captatore" offerti all'Autorità Giudiziaria, quindi nello specifico: il corretto funzionamento dei captatori utilizzati, garantendone le funzionalità di acquisizione e trasmissione dei dati garantendone l'integrità e l'autenticità, ma che verifichi anche i livelli di affidabilità del fornitori di servizi di intercettazione in modo che siano garantiti adeguati se non addirittura i massimi, livelli di protezione dei dati e delle informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni finalizzato ad una corretta gestione dei dati sensibili.

Infatti, come per l'autovelox l'efficacia dello strumento di misurazione viene garantito da una periodica attività di verifica del dispositivo, analogamente anche per il captatore andrebbe effettuata una continua attività di controllo di funzionamento per ogni versione rilasciata e allo stesso tempo andrebbe periodicamente effettuata una verifica di affidabilità del fornitore di servizi di intercettazione dei dati (*auditing*)[29].

Va però evidenziato che mentre per l'autovelox le verifiche di funzionamento sono estremamente semplici, atteso che il dispositivo deve solo misurare la velocità del veicolo, nel caso del captatore la verifica di funzionamento dello stesso è estremamente complessa e onerosa attesa la continua evoluzione tecnologica e eterogeneità di modelli dei

[29] L. Filippi, *Chi e come usa il captatore informatico? La Cassazione non ammette controlli*, 2020, https://www.quotidianogiuridico.it/documents/2020/12/03/il-captatore-informatico-riflessioni-sulla-recente-sentenza-della-cassazione.

dispositivi sui cui inoculare il captatore, circostanza questa che potrebbe portare ad avere fasi di collaudo estremamente lunghe. Mentre certamente è più facilmente percorribile la strada della verifica della correttezza dei dati effettuata dal fornitore di servizi che potrebbero assolvere, come spesso già alcune fanno, ottenendo la certificazione ISO 27001.

Quindi, a sommesso parere degli scriventi, in questa prospettiva andrebbe istituito un organo tecnico di controllo che dovrebbe vigilare sulla corretta erogazione dei servizi di intercettazione e collaudare le versioni di captatori che vengono di volta in volta realizzati, organo che alla luce dei diversi episodi noti alle cronache avrebbe dovuto già essere costituito e la cui costituzione risulterebbe alquanto complessa atteso anche il rilevante ruolo di controllo che dovrebbe avere.

Motivo per il quale, allo stato attuale, l'unica garanzia processuale che rimane per la verifica dell'attendibilità probatoria dei dati acquisiti da un captatore informatico è l'esame diretto dello strumento, l'organizzazione del fornitore di servizi e l'analisi dei dati acquisiti con lo specifico strumento. Per cui, si ribadisce l'estrema improbabilità che in un processo si puntino i riflettori sul captatore e sul relativo fornitore: ovvero il captatore che non c'è.

4. Conclusioni

Alla luce di quanto illustrato e della mancata emanazione di alcuni decreti di attuazione, emerge come sia ancora molto lunga la strada da percorrere per giungere al consolidamento normativo in merito all'uso del captatore informatico, così come le esigenze di verifica tecnica del corretto funzionamento presentano criticità scientifiche e giuridiche rilevanti. Allo stesso tempo, tale strumento si è dimostrato estremamente pervasivo e risolutivo nella attività di indagine, motivo per il quale il suo utilizzo non potrà essere certamente abbandonato.

Andrà, a parere degli scriventi, svolto da parte del legislatore, un attento lavoro di valutazione e individuazione di misure legislative, organizzative e tecniche che possano maggiormente garantire il diritto di difesa, partendo però da un imprescindibile presupposto tecnico: il "sistema captatore" è uno strumento di acquisizione di dati e non un mero registratore di voci e su tale presupposto si dovranno basare tutte le iniziative, legislative, regolamentari e tecniche volte al miglioramento dell'attuale disciplina esistente.

Parte II

IOT, *CRYPTO* E SOCIAL MEDIA: NUOVE SFIDE PER LA *FORENSICS*

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464309
pp. 159-186 (gennaio 2022)

La "Qualità dell'Informazione" nella IoT Forensics: dal modello IQA all'ontologia forense

FAUSTO GALVAN, FEDERICO COSTANTINI,
MARCO ALVISE DE STEFANI, SEBASTIANO BATTIATO[1]

1. Introduzione: Qualità dell'Informazione nella IoT forensics

La sfida rappresentata dall'analisi delle prove digitali[2] in ambiente c.d. "Internet of Things"[3] (d'ora in poi, IoT), è ormai nota agli esperti forensi e alla comunità scientifica internazionale[4]. Le difficoltà sono date

[1] Fausto Galvan, *Digital Forensics Expert*; Federico Costantini, Dipartimento di Scienze giuridiche, Università degli Studi di Udine; Marco Alvise De Stefani, Synaptic; Sebastiano Battiato, Dipartimento di Matematica e Informatica, Università di Catania.

[2] La *Digital forensics* è la scienza forense che si occupa delle prove elettroniche. Una delle più autorevoli ed esaustive definizioni è la seguente: «*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*» G. PALMER, *A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS)*, New York, 2001, p. 23. In Italia di recente sul tema cfr. M. FERRAZZANO, *L'Informatica forense: profili giuridici, tecnici e metodologici nel trattamento della digital evidence*, in *Diritto e tecnologie informatiche: questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, T. Casadei e S. Pietropaoli (a cura di), Milano, Wolters Kluwer; Comp.Lex - Diritto, computazione, complessità), 2021, pp. 151-161; G. COSTABILE, A. ATTANASIO E M. IANULARDO (a cura di), *IISFA Memberbook 2021 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter*, IISFA Educational, 2021.

[3] Il termine *Internet of Things* fu coniato nel 1999 relativamente ai dispositivi RFID (Radio-Frequency Identification) e presto si diffuse comprendendo anche altre tecnologie. Attualmente è definito come «*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*», secondo una definizione data nel 2012 dalla International Telecommunication Union (ITU), M. FRIEDEWALD E O. RAABE, *Ubiquitous Computing: An Overview of Technology Impacts*, in «Telematics and Informatics», 28 n. 2 (2011), pp. 55-65.

[4] R. HEGARTY, D. J. LAMB E A. ATTWOOD, *Digital Evidence Challenges in the Internet of Things*, in *Proceedings of the Tenth International Network Conference (INC) 2014*, Plymouth, School of Computing & Mathematics Plymouth University, 2014, pp. 163-172; *FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger*, 2018 IEEE

da diversi fattori: i dati sono sparsi in un insieme di dispositivi di cui, a priori, non si conoscono le specifiche (tipo, numero e posizionamento)[5]; le macchine in molti casi presentano diverse vulnerabilità in termini di sicurezza informatica; le comunicazioni possono non essere sufficientemente protette, oppure consentire ai dati di viaggiare su rete aperta, così permettendo l'intromissione – ed eventualmente la successiva manomissione – da parte di terzi; le unità di archiviazione dei dati spesso non sono al riparo da accessi indesiderati; a causa dell'alta interdipendenza che caratterizza dispositivi di una stessa rete, quand'anche estesa, ogni anomalia può espandersi indeterminatamente ovvero fluire all'esterno, contaminando altri sistemi. Crimini molto seri, pertanto, possono essere commessi senza lasciare alcuna traccia ovvero rischiano di non poter essere efficacemente perseguiti perché l'approccio attualmente più comune, fondato sulla "catena di custodia"[6], non sempre si rivela fruttuoso.

In questo contributo intendiamo trattare il problema della Qualità dell'Informazione (d'ora in poi, IQ) nell'ambito di un ecosistema IoT, delineando un approccio teorico che prevede la formalizzazione del processo inerente alla valutazione della prova informatica estratta da tale contesto. In particolare, intendiamo proporre un modello idoneo a calcolare la IQ – denominato IQA (*Information Quality Assessment*) includendo una molteplicità di componenti eterogenee che condizionano l'acquisizione forense e quindi l'integrità della "catena di custodia". Tali fattori riguardano tre aspetti molto differenti tra loro:

International Congress on Internet of Things (ICIOT), pp. 33-40; S. Zawoad, A. Kumar Dutta e R. Hasan, *SecLaaS: secure logging-as-a-service for cloud forensics*, Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, 2484342, ACM, 2013, pp. 219-230; C. Meffert, D. Clark, I. Baggili e F. Breitinger, *Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition*, Proceedings of the 12th International Conference on Availability, Reliability and Security, 3104053, ACM, 2017, pp. 1-11.

[5] M. Sharjeel Zareen, A. Waqar e B. Aslam, *Digital Forensics: Latest Challenges and Response*, 2013 2nd National Conference on Information Assurance (NCIA), 2013, pp. 21-29.

[6] Il termine "catena di custodia" indica l'insieme delle procedure funzionali a garantire l'integrità della prova. Questa nozione comprende diverse fasi e procedure, richiedendo tra le alter cose, la registrazione degli accessi alla prova al fine di garantire la massima trasparenza sull'affidabilità della prova. Cfr. a tal proposito la Convenzione sul Cybercrime sottoscritta nel 2001 a Budapest (n. 185 CoE).

1) l'aspetto "oggettivo". Si pone il problema della qualità delle risultanze dell'acquisizione, ossia la qualità del dato (d'ora in poi, DQ)[7],
2) l'aspetto "soggettivo". Ciò riguarda la gestione dei dati da parte dell'analista e quindi la capacità di analisi impiegata dall'esperto nel caso specifico[8],
3) l'elemento "transattivo". Esso concerne l'influenza dell'aspetto comunicativo e retorico-processuale sull'impatto della prova rispetto alla decisione della controversia[9].

La presente trattazione si compone dei seguenti passaggi argomentativi:

1) in via preliminare introduciamo il tema con una panoramica sui concetti di DQ e IQ, concentrandoci sulle questioni che più rilevano in uno scenario IoT;
2) ci soffermiamo sul concetto di IQ che intendiamo approfondire in questo contributo, collocandolo in un più ampio quadro concettuale dato dalla "Filosofia dell'Informazione";
3) analizziamo le questioni pratiche emergenti all'interno del contesto IoT evidenziando come in esso possono trovare riscontro le istanze teoriche sopra individuate;
4) esponiamo il modello per valutare la IQ nell'ambiente IoT e lo rappresentiamo in una formulazione che, come si vedrà, può essere coniugata in tre diverse varianti;
5) prospettiamo l'inserimento del modello teorico così esemplificato all'interno delle attuali ontologie legali più rappresentative in ambito forense.

In conclusione, esprimiamo le nostre valutazioni finali e offriamo alcune indicazioni per ricerche future.

[7] In generale, maggiore è la quantità di fonti di prova, minore fiducia si può riporre nella loro qualità. In altri termini, se ci sono diversi tipi di dispositivi interconnessi, è probabile che essi debbano essere analizzati con diverse metodologie e, per converso, è improbabile che i risultati dell'analisi possano essere aggregati in modo efficiente.

[8] In generale, maggiore è la quantità di dati disponibile, più difficile è analizzarli. Infatti, la prova informatica dipende dalla capacità computazionale richiesta per l'acquisizione, l'elaborazione e la selezione del materiale rilevante. Raccogliere le prove dopo il termine di scadenza per la presentazione in giudizio è del tutto inutile.

[9] In generale, più sono avanzate le tecnologie, maggiore è il grado di competenza richiesto per il loro utilizzo e la comprensione dei risultati della loro applicazione. Ciò significa anche che maggiore è la complessità di una tecnologia, minore è la comprensione da parte di un non esperto.

2. Presupposti teoretici: DQ e IQ tra "teoria dell'informazione" e "filosofia dell'informazione"

In via preliminare è utile tenere presente che vi sono diverse concezioni intorno ai concetti di "dato" e "informazione"[10]. Secondo una prospettiva che, per semplicità, possiamo ritenere più legata alla "teoria dell'informazione"[11], i dati sono definiti come una categoria specifica di "informazione", mentre quest'ultima è concepita come una particolare forma di "conoscenza"[12]. Una ricostruzione alternativa, discendente dalla "Filosofia dell'Informazione"[13] – su cui di seguito si forniscono alcuni chiarimenti ulteriori – qualifica l'informazione come "dato significativo", mentre la "conoscenza" è concepita come "informazione qualificata"[14]. Questa seconda ricostruzione è preferibile ai fini della presente trattazione in quanto consente di ancorare il nostro modello teorico alle più recenti conquiste dell'epistemologia contemporanea[15] sfruttandolo come collegamento tra questa e le possibili applicazioni pratiche che ne possono derivare.

La discussione tra "dato" e "informazione" si riflette in ambito giuridico rispetto al rapporto tra "realtà" e "conoscenza", problema che riguarda direttamente tutte le misure che devono essere adottate per mantenere la "catena di custodia", e indirettamente la teoria della prova

[10] R. Brighi, *Il ruolo dei dati informatici nella costruzione della realtà*, Aracne, 2016.

[11] Cfr. per tutti C. E. Shannon e W. Weaver, *The Mathematical Theory of Communication*, Urbana, University of Illinois Press; 27), 1949.

[12] In questo senso il "dato" è definito come: «*reinterpretable representation of information in a formalized manner suitable for communication, interpretation and processing*», mentre l'"informazione" è: «*information processing knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context have a particular meaning*» C. Batini e M. Scannapieco, Dat*a and Information Quality: Dimensions, Principles and Techniques,* Springer International Publishing (Data-Centric Systems and Applications, 2016.

[13] Cfr. la "quadrilogia" L. Floridi, *The philosophy of information*, Oxford-New York, Oxford University Press, 2011; Id, *The Ethics of Information*, Oxford, Oxford University Press, 2013; Id, *The 4th Revolution. How the infosphere is reshaping human reality*, Oxford, Oxford University Press, 2014; Id, *The logic of information. A theory of philosophy as conceptual design*, Oxford-New York, Oxford University Press, 2019.

[14] Per un approfondimento sugli aspetti epistemologici, cfr. in Id, *The logic of information. A theory of philosophy as conceptual design*, cit. nonché la versione ridotta in lingua italiana Id, *Pensare l'infosfera. La filosofia come design concettuale*, Milano, Cortina, 2020.

[15] Cfr. per tutti E. Gettier, *Is Justified True Belief Knowledge?*, in «Analysis», 23 n. 6 (1963), pp. 121-123.

su cui esse devono fondarsi[16]. Infatti, se si prende come riferimento il procedimento penale secondo il modello accusatorio – l'esempio più notevole in questo senso – si può osservare come le fonti di prova devono essere raccolte secondo specifiche modalità per poter essere oggetto di contraddittorio e quindi costituire il fondamento della decisione giudiziale[17]. Affinché ciò possa avvenire a prescindere dal tipo di supporto – fisico o informatico – in cui le prove sono incorporate si rende necessario un notevole sforzo di astrazione concettuale. Un ulteriore elemento da tenere in considerazione – e che costituisce altresì argomento favorevole alla seconda impostazione – è dato dal fatto che, grazie ad essa, "realtà" e "conoscenza" diventano concetti che possono essere applicati a diversi tipi di entità – esseri umani o agenti artificiali – ed essere oggetto tanto di elaborazione da parte del singolo agente quanto di condivisione tra una pluralità di operatori.

La contrapposizione tra l'approccio basato sul "dato" e quello basato sulla "informazione" si ripresenta anche rispetto alla qualità. A tal proposito è utile premettere che, se la prova può essere considerata come una sorta di "informazione", si può osservare come per garantirne la qualità sia essenziale che si stabiliscano non solo regole giuridiche processuali, ma anche standard tecnologici trasparenti e condivisi sull'acquisizione e sull'ammissione delle prove.

È stato detto molto efficacemente che i dati sono l'anello di congiunzione tra il mondo reale e quello digitale[18], nel senso che dal "mondo reale" avviene, attraverso sensori o algoritmi, l'acquisizione di dati, i quali poi sono rappresentati nel "mondo digitale" per essere successivamente processati di nuovo e re-introdotti nel contesto originario.

Rispetto a ciò, la DQ viene definita dal punto di vista tecnologico "il grado in cui le caratteristiche dei dati soddisfano i bisogni dichiarati e impliciti quando usati in condizioni specificate"[19].

[16] Specificamente sugli aspetti teoretici della teoria della prova, G. TUZET, *Filosofia della prova giuridica*, Torino, Giappichelli (Recta ratio. Testi e studi di Filosofia del Diritto. Sesta Serie; 117), 2013.

[17] Il riferimento privilegiato è agli artt. 244, 247 e 360 C.P.P.

[18] A. KARKOUCH, H. MOUSANNIF, H. AL MOATASSIME E T. NOEL, *Data quality in internet of things: A state-of-the-art survey*, in «Journal of Network and Computer Applications», 73 (2016), pp. 57-81.

[19] «*the degree to which the characteristics of data statisfy stated and implied needs when used under specified conditions*», Cfr. ISO/IEC 25012:2008 (ISO/IEC 2008). Come affermato in C. BATINI E M. SCANNAPIECO, *Data and Information Quality: Dimensions, Principles and Techniques*, cit., la qualità in generale è stata definita come la "*totalità delle caratteristiche di un prodotto che incidono sulla sua capacità di soddisfare bisogni dichiarati o impliciti*" ISO

Sulla nozione di DQ e sulle sue componenti vi sono diverse tesi. Di seguito si riporta una tabella che contempla le posizioni più significative ai fini della nostra trattazione[20]. La classificazione contenuta in Tabella 1 è essenziale per lo sviluppo del nostro modello[21].

Rispetto alla IQ occorre tenere presenti due ulteriori aspetti, che dipendono dal fatto che l'analisi viene svolta – e successivamente influenza – la visione del mondo, le decisioni e la condotta di un essere umano. Questi aspetti sono la c.d. "*complatency*"[22] e il "consenso"[23]. Il primo elemento concerne la valutazione in merito all'ignoranza sulla qualità dell'informazione disponibile, con il rischio di generare un eccessivo affidamento sull'informazione disponibile. Il secondo elemento invece riguarda il fatto che su ciò che l'informazione rappresenta ci sia condivisione all'interno di un gruppo sociale: ciò dipende da fattori preesistenti ed estrinseci rispetto all'informazione stessa, come le convinzioni dell'agente, oppure elementi occasionali come vincoli o limitazioni di diversa natura[24]. Entrambi i fattori, come si può facilmente notare, sono caratteristici degli esseri umani.

9000:2015. cfr. anche la definizione di "qualità dei dati" in ISO/TS 8000-1:2011. La DQ è definita sinteticamente anche «*fitness for the (intended) use of data*» W. H. DeLone e E. R. McLean, *Information Systems Success: The Quest for the Dependent Variable*, in «Information Systems Research», 3 n. 1 (1992), pp. 60-95; Id, *The DeLone and McLean Model of Information Systems Success: A Ten-Year Update*, in «Journal of Management Information Systems», 19 n. 4 (2003), pp. 9-30; C. Batini, C. Cappiello, C. Francalanci e A. Maurino, *Methodologies for data quality assessment and improvement*, in «ACM Computing Surveys», 41 n. 3 (2009), pp. 1-52; P. Woodall, A. Borek e A. Kumar Parlikad, *Data quality assessment: The Hybrid Approach*, in «Information & Management», 50 n. 7 (2013), pp. 369-382, cfr. anche in precedenza "*fitness for (intended) use*" J. M. Juran, *Juran on Planning for Quality*, New York; London, Free Press ; Collier Macmillan, 1988. In senso diverso si definisce come "conformance to requirements" P. B. Crosby, *Quality is Free: the Art of Making Quality Certain*, New York, McGraw-Hill, 1979, o "user satisfaction" S. Wayne, *Quality Control Circle and Company Wide Quality Control*, in «Quality Progress», October (1983), pp. 14-17.

[20] Sono state individuati ben 159 componenti della qualità dei dati, Karkouch et al., *Data quality in internet of things: A state-of-the-art survey*, cit., p. 60.

[21] Si può osservare come le diverse classificazioni coincidano in parte.

[22] Si preferisce utilizzare il termine in lingua inglese per precisione concettuale. Esso si definisce come «*the degree to which information on IQ is ignored*» Batini e Scannapieco, *Data and Information Quality: Dimensions, Principles and Techniques*, cit.

[23] Si definisce come «*the level of agreement within a group with respect to a preferred choice*», ivi.

[24] Qui si può collocare l'eventualità che lo scopo per cui l'informazione è stata originariamente prodotta (*P-purpose*) sia difforme dallo scopo – o dagli scopi – per cui essa viene utilizzata o meglio consumata (*C-purpose*), L. Floridi, *Information Quality*, in «Philosophy & Technology», 26 n. 1 (2013), pp. 1-6.

Table 1. Corrispondenza tra le versioni del concetto di "informazione"[25].

Classificazioni menzionate in Batini and Scannapieco 2016				
(Batini, Palmonari, and Viscusi 2012)	**(Wand and Wang 1996)[26]**	**(Wang and Strong 1996)[27]**		**(Shamala et al. 2017)[28]**
Accuratezza	Accuratezza	Intrinseco	Accuratezza	Accuratezza
-	-		Credibilità	Credibilità
-	-		Oggettività	-
-	-		Reputazione	-
Completezza	Completezza	Contestuale	Completezza	Completezza
-	-		Rilevanza	Rilevanza
-	Tempestività		Tempestività	Tempestività
-	-		Valore aggiunto	-
Ridondanza	-		-	-
-	-		Appropriatezza nella quantità di dati	Quantità di dati

[25] Altri modelli sono discussi in BATINI E SCANNAPIECO, *Data and Information Quality: Dimensions, Principles and Techniques*, cit. ma non sono affrontati qui M. BOVEE, R. P. SRIVASTAVA E B. MAK, *A Conceptual Framework and Belief-function Approach to Assessing Overall Information Quality*, in «International Journal of Intelligent Systems», 18 n. 1 (2003), pp. 51-74; L. LIPING E L. N. CHI, *Evolutional Data Quality*, in *7th International Conference on Information Quality*, Cambridge, MIT, 2002, pp. 292-304; F. NAUMANN, *Quality-Driven Query Answering for Integrated Information Systems*, Berlin Heidelberg, Springer-Verlag (Lecture Notes in Computer Science, 2002; THOMAS C. REDMAN, *Data Quality for the Information Age*, 1st ed., Norwood, MA, USA, Artech House, Inc., 1997.

[26] Si tratta di un approccio di carattere più teoretico, cfr. Y. WAND E R. Y. WANG, *Anchoring data quality dimensions in ontological foundations*, in «Communications of the ACM», 39 n. 11 (1996), pp. 86-95.

[27] Questo approccio ha una caratterizzazione di tipo empirico, cfr. RICHARD Y. WANG E DIANE M. STRONG, *Beyond Accuracy: What Data Quality Means to Data Consumers*, in «Journal of Management Information Systems», 12 n. 4 (1996), pp. 5-33.

[28] P. SHAMALA, R. AHMAD, A. ZOLAIT E M. SEDEK, *Integrating information quality dimensions into information security risk management (ISRM)*, in «Journal of Information Security and Applications», 36 (2017), pp. 1-10.

Classificazioni menzionate in Batini and Scannapieco 2016				
(Batini, Palmonari, and Viscusi 2012)	**(Wand and Wang 1996)[26]**	**(Wang and Strong 1996)[27]**		**(Shamala et al. 2017)[28]**
-	-	Rappresentazionale	Interpretabilità	-
-	-		Facilità di comprensione	-
-	-		-	Obiettività
-	-		Concisione nella rappresentazione	Concisione nella rappresentazione
Coerenza	Coerenza		Coerente rappresentazione	Coerente rappresentazione
Utilità	-		-	-
Fiducia	-		-	-
-	Affidabilità		-	Affidabilità
Accessibilità	-	Accessibilità	Accessibility	
-	-			Disponibilità
-	-		Sicurezza nell'accesso	-
Leggibilità	-		-	-
-	-		-	Comprensibilità
-	-		-	Verificabilità

3. IQ e "Filosofia dell'Informazione"

È noto che la "Filosofia dell'Informazione" si è sviluppata nel corso degli ultimi venti anni come una visione fondata su una metafisica costruzionistica[29] il cui concetto di fondo – appunto, l'idea di "informazione" – rappresenta essenzialmente la minima entità di essere che può essere isolata all'interno di un determinato contesto. Sotto questo pro-

[29] ID, *The logic of information. A theory of philosophy as conceptual design*, cit., specialmente il capitolo 3.

filo è estremamente importante che in questa prospettiva si riprendano tre diverse concezioni di "informazione" che erano state elaborate prima dalla cibernetica e, successivamente, dalle riflessioni sulla tecnologia: "informazione come realtà", "informazione sulla realtà", "informazione per la realtà". Ciascuna versione ha delle particolarità.

Table 2. Corrispondenza tra le versioni del concetto di "informazione".

Weaver 1949[30]	**Borgman 1999**[31]	**Floridi 1999**[32]	**Esempio**
Technical information	Technological	Informazione come realtà	Segnale elettrico, il cui processo di trasmissione avviene a prescindere dal contenuto veicolato.
Semantic information	Natural	Informazione sulla realtà	Descrizione di fenomeni naturali, soggetti alla valutazione di conformità con la realtà (valore aletico).
Influential information	Cultural	Informazione per la realtà	Istruzioni operative, comandi o algoritmi destinati a uno o più destinatari.

Il problema della qualità si esprime in modo diverso a seconda della versione del concetto di informazione che si prende in considerazione.

Per quanto concerne l'Informazione come realtà, il problema è presente sin dalle origini della stessa teoria dell'informazione, che si preoccupa di ridurre il rumore, le distorsioni e la perdita di qualità nel segnale. Qui la IQ misura l'affidabilità delle misure adottate per salvare dall'entropia l'informazione trasferita.

Rispetto all'"informazione sulla realtà", invece, si pone il problema della discrepanza tra mondo naturale e mondo digitale. Questo concetto è connesso a quello di "significato" dell'informazione e quindi alle questioni connesse alla semantica. Qui, in altri termini, la IQ misura l'affidabilità delle informazioni ottenute nel rappresentare gli eventi esterni al mondo digitale, e quindi il grado di plausibilità dell'attribuzione del valore aletico, ossia il "vero" o il "falso".

[30] «*In communication there seem to be problems at three levels: 1) technical, 2) semantic, and 3) influential*», W. WEAVER, The Mathematics of Communication, in «Scientific American», 181 n. 1 (1949), pp. 11-15.

[31] A. BORGMANN, *Holding on to Reality. The Nature of Information at the Turn of the Millennium*, Chicago, University of Chicago Press, 1999.

[32] L. FLORIDI, *Philosophy and computing. An introduction*, London-New York, Routledge, 1999.

Rispetto all'"informazione per la realtà" il problema della qualità si pone invece nel momento in cui si verifica la sussistenza di conflitti o lacune. Questo concetto riguarda il fatto che l'informazione acquisita potrebbe essere processata ulteriormente una volta condivisa con altri soggetti. Di conseguenza, qui si pone il problema dell'affidabilità degli agenti che ricevono l'informazione da condividere.

Per quanto concerne l'ambito forense, l'IQ si coniuga differentemente a seconda del contesto, come si può osservare nello schema riportato.

Per quanto concerne la qualità dell'"informazione come realtà" si pongono le questioni concernenti specificamente la "catena di custodia", comprendendo in esse anche gli standard tecnologici e le c.d. *best practices* adottate dalla comunità degli esperti.

In merito alla qualità dell'"informazione sulla realtà" si può prendere in considerazione l'affidabilità della rappresentazione degli eventi avvenuti nel "mondo naturale" ossia la questione della validazione alla luce del confronto con altre fonti di prova.

La terza tipologia, ossia l'"informazione per la realtà" riguarda la discussione delle prove in giudizio (in generale: accusa, difesa degli imputati e delle parti civili, giudici, testi, consulenti). Ovviamente questa discussione deve avvenire secondo le regole processuali, che prevedono specifici requisiti per l'ammissibilità e l'onere della prova. In questo ambito possono essere comprese anche variabili che rilevano rispetto all'efficacia della prova, ossia le competenze professionali degli esperti, *soft-skills* (capacità argomentativa, strategie processuali), i costi degli strumenti di analisi e il tempo a disposizione per l'indagine.

Per quanto concerne in particolare l'ambito specifico della IoT forensics, si possono ulteriormente dettagliare le questioni attinenti l'IQ.

La qualità concernente l'"informazione come realtà" riguarda l'integrità delle informazioni raccolte, ossia la possibilità di isolare il dispositivo e cristallizzare il singolo frammento di informazione. Rispetto a questo tema si segnala come sia difficile individuare il confine di rilevanza dei dati.

La qualità relativa all' "informazione sulla realtà" si pone rispetto al problema di individuare una specifica sorgente, tracciare la catena delle interazioni, misurare l'influenza di un singolo elemento all'interno del contesto che rappresenta l'evento effettivamente accaduto. Da questo punto di vista, la correlazione più che il rapporto di causalità costituisce al chiave per comprendere l'incertezza epistemica che regna in questo contesto.

La qualità relativa all' "informazione per la realtà", da ultimo, fa emergere il problema intrinseco nel fattore umano, che comunque deve essere tenuto in considerazione al pari di quelli tecnologici, e pertanto si pone i termini di "responsabilizzazione" degli operatori, ossia nel definire degli approcci che consentano, a coloro i quali assumono posizioni di carattere fiduciario, di provare il rispetto degli standard di condotta attraverso l'esposizione delle ragioni ad essa sottese.

Table 3. Corrispondenza delle questioni concernenti l'IQ.

Filosofia dell'Informazione	**Qualità dell'informazione, livello di analisi**	**Qualità dell'informazione nella digital forensics**	**Qualità dell'informazione nella IoT Forensics**
Informazione come realtà	Teoria tradizionale della comunicazione	"Catena di custodia"	Rilevanza
Informazione sulla realtà	Coerenza con i fatti rappresentati	Convalida esterna con altre fonti di evidenza	Incertezza
Informazione per la realtà	Coerenza le altre informazioni	Regole sugli aggettivi (ammissione e onere della prova)	Accountability

4. Problemi pratici nella IoT Forensics

Dopo aver fornito una breve definizione della qualità delle informazioni, intendiamo ora sottolineare che con il passare degli anni è diventato chiaro che l'utilizzo di dispositivi IoT – che sono stati concepiti per aumentare l'efficienza dei servizi, a beneficio di utenti privati e industrie – genera un "ambiente virtuale" contenente un'enorme quantità di informazione che, se necessario, può essere utilizzata come fonte di prova in uno scenario forense. In questo capitolo analizziamo come uno dei compiti principali dell'IoT Forensics, ovvero la raccolta di prove, sia particolarmente impegnativo per diversi motivi.

Innanzitutto, l'estrema varietà di dispositivi IoT, con protocolli proprietari o non documentati, spesso privi di interfacce fisiche, ostacola l'estrazione diretta delle prove dai dispositivi.

In secondo luogo, i dispositivi IoT inviano costantemente informazioni ai "propri" fornitori di servizi *Cloud*, ma ottenere queste prove da un servizio *Cloud* comporta altre sfide, sia tecniche (*Cloud Forensics*) che legali (interazione con società straniere con ordinamenti giuridici diversi).

In terzo luogo, le prove potrebbero essere manipolate dai fornitori di servizi *Cloud*: i dati "grezzi" inviati dai dispositivi IoT vengono analiz-

zati, interpretati e archiviati, aggiungendo ulteriori livelli di interpretazione. Tali processi possono aggregare i dati ma anche deteriorarli, peggiorando così la qualità delle informazioni acquisite.

Un esempio può essere utile per chiarire le questioni emergenti. Supponiamo di voler acquisire la cronologia completa della geolocalizzazione di un determinato utente che usa un account Google.

Un primo approccio potrebbe essere quella di acquisire con modalità forensi i dati estraendoli direttamente da tutti i dispositivi IoT coinvolti (ad esempio lo smartphone, lo smartwatch, una fitband, un computer fisso privato, un computer portatile aziendale, i dati della centralina dell'auto, ecc.). Questa metodologia si scontra però con le problematiche prima esposte (difficoltà ad estrarre e a interpretare i dati estratti, senza considerare che i dati potrebbero non essere memorizzati nei dispositivi stessi).

Una seconda possibilità consiste nell'utilizzare le informazioni messe a disposizione del provider stesso, estraendo i dati presenti nella "*Google Timeline History*"[33]. Supponiamo quindi di possedere le credenziali dell'account (username e password): attraverso un applicativo forense (es. *Oxygen Forensic Cloud Extractor*[34]) siamo in grado di acquisire lo storico della geolocalizzazione[35]. Dopo di ciò, analizzando i dati raccolti potremmo trovare un insieme di informazioni molto chiaro e dettagliato, concernenti anche fatti avvenuti anni prima[36]. La varietà e l'organizzazione dei dati può portarci a supporre che la qualità dei dati sia molto alta, tuttavia manca un dettaglio fondamentale, dato dall'origine delle informazioni. Infatti, il fornitore di servizi potrebbe acquisire le informazioni di geolocalizzazione da una vasta gamma di fonti relative a quell'account: il GPS di uno smartphone; i dati EXIF delle immagini; le torri radio della rete cellulare; le reti WiFi note; le app per il fitness e bracciali; l'utilizzo di servizi di spostamento come Uber o l'utilizzo di biglietti del trasporto pubblici; la geolocalizzazione dell'IP; i dati forniti da uno smartwatch; le app di navigazione; le re-

[33] https://www.google.com/maps/timeline.

[34] https://www.oxygen-forensic.com/en/oxygen-forensic-cloud-investigator-ofci.

[35] Si presume che il software forense sia conforme a tutte le procedure e gli standard della digital forensics.

[36] La tipica interfaccia utente del software forense per questo tipo di dati è costituita da una mappa del mondo con punti e linee colorate che rappresentano informazioni di geolocalizzazione e probabili movimenti: mediante comodi filtri temporali, la possibilità di ingrandire e l'utilizzo di ricerche geografiche possiamo agevolmente individuare i dati di interesse.

censioni di negozi o ristoranti; l'utilizzo di dispositivi smart home e molte altre fonti IoT. La timeline inoltre potrebbe essere stata manipolata dall'utente attraverso l'interfaccia web del servizio *Cloud* (ad esempio in Google Timeline possiamo facilmente aggiungere una nuova geolocalizzazione o modificare o eliminare un vecchio record).

Se ci concentriamo su un giorno specifico, abbiamo solo la presunta cronologia della geolocalizzazione: alcuni punti (costituiti da longitudine, latitudine e *timestamp*) e linee che collegano quei punti per ipotizzare movimenti, ma non siamo in grado di scoprire da dove proviene il dato relativo ad ogni singolo punto. Anche se in alcuni *metatag* sono presenti informazioni sulla fonte delle informazioni, possiamo accedere solo ai dati interpretati e metabolizzati dal service provider; non sappiamo se la fonte è affidabile o se i dati sono stati manipolati, compromessi o non interpretati correttamente. I dati originali potrebbero non essere nemmeno archiviati o accessibili[37].

5. Esposizione del modello IQA

Abbiamo visto, nell'esempio precedente, come la valutazione dell'IQ in un insieme di dati eterogenei non sia un compito banale, soprattutto nel momento che al processo di estrazione si possono utilizzare diverse metodologie. Le varie fasi della valutazione dipendono sempre da fattori diversi, molti dei quali possono essere solo stimati[38]. Oltre alle difficoltà illustrate nelle sezioni precedenti e caratteristiche di un ambiente IoT, in uno scenario forense vi sono ulteriori condizioni da rispettare relativamente all'IQ: il fatto che l'informazione acquisita sia anche ammissibile sotto il profilo processuale.

[37] La stessa problematica si presenta – con riferimento a Google – qualora si acquisiscano gli stessi dati tramite la procedura di Google Takeout, grazie alla quale si possono ottenere due formati differenti: JSON e KML. Dal confronto di queste tre fonti (Timeline e JSON/KML Takeout) e interpretando i risultati con l'esperienza e il *reverse engineering* in casi simili possiamo migliorare la nostra comprensione sulla provenienza dei dati, ma rimarrebbero ipotesi e non informazioni certe. Ad esempio, vedere la stessa geolocalizzazione ripetuta in giorni diversi (centrata nello stesso punto ma con un ampio intervallo di incertezza), significa probabilmente che lo smartphone era connesso a una torre radio cellulare mentre il GPS non era in funzione, ma è una deduzione data dall'esperienza e da test pratici, e non da metadati a corredo della geolocalizzazione.

[38] Non possiamo dimenticare il rumore che arriva con il flusso di dati, che deve essere accuratamente identificato e rimosso. Naturalmente, tale processo deve essere eseguito con molta cautela poiché potrebbe causare la perdita definitiva di dati preziosi.

Un possibile approccio a tale questione dovrebbe essere basato sulla verifica separata dell'IQ, nel senso che, per essere ammissibili ai fini forensi, le informazioni acquisite devono essere, allo stesso tempo, ammissibili come prove processuali (quindi correttamente acquisite secondo gli standard previsti e conservate secondo le più recenti e migliori pratiche del settore[39]) e affidabili dal punto di vista qualitativo (a bassa rumorosità, leggibili, comprensibili, salvati in un formato noto, ecc.). Il metodo che prevede esclusivamente questa duplice serie di controlli, sebbene utile, è caratterizzato da due rischi principali: (1) la perdita di tempo in cui si incorre quando la negatività dell'esito di uno dei due controlli obbliga a scartare dati che sarebbero stati ammissibili seguendo le altre specifiche di ammissibilità; (2) il rischio di veder rifiutare l'ammissibilità per prove chiave che, per qualche motivo, non abbiano ottenuto un livello di qualità sufficiente sotto il profilo meramente informatico (es. viene scartata un'immagine che, considerata insieme ad altre evidenze, potrebbe avere un significato importante, perché affetta da troppo "rumore").

5.1. *Il modello teorico di determinazione dell'IQ nella IoT Forensics*

Sulla base di quest'ultima osservazione si può il quadro teorico delineato nella sezione precedente con un approccio in cui caratteristiche delle informazioni estratte (allo stesso tempo "dati grezzi" ed "evidenze") vengono processate contemporaneamente, andando a comporre gli addendi di una sommatoria. Per motivi di chiarezza, consideriamo solo le categorie delle caratteristiche del'IQ mostrate in Wang e Strong (1996)[40].

Nel nostro scenario investigativo immaginario, le prove digitali raccolte provengono da un insieme di *n* dispositivi IoT. Il modello considera diversi fattori per stabilire l'IQ delle informazioni estratte da ogni fonte, giungendo a computare un coefficiente percentuale che abbiamo chiamato IQA (valutazione della qualità delle informazioni), definito come segue:

$$\text{IQA} = \frac{\sum_{i=1}^{n}(DTC_i + DST_i + CS_i + CM_i + SR_i + PC_i + TDA_i + OT_i + OS_i)}{9n} \times 100. \quad (1)$$

[39] ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.

[40] WANG E STRONG, *Beyond Accuracy: What Data Quality Means to Data Consumers*, cit.

dove:

- *i* = i-esimo dispositivo;
- DTC = stato del dispositivo dal punto di vista tecnico[41];
- DST = livello di sicurezza del dispositivo[42];
- CS = livello di sicurezza del servizio *Cloud* a cui è connesso il dispositivo[43];
- CM = manipolazione dei dati spuri da parte di apposito servizio presente nel *Cloud*[44];
- SR = affidabilità della fonte[45];
- PC = privacy dei dati con riferimento al GDPR[46];
- TDA = accessibilità delle specifiche tecniche del dispositivo[47];
- OT = livello tecnico dell'osservatore[48];
- OS = capacità dell'osservatore[49];
- i valori ammessi sono tutti i decimali, con due cifre dopo la virgola, compresi tra 0 = "pessimo" ed 1 = "ottimo".

Anche per quest'ultimo modello, sebbene più completo e simile alla realtà operativa rispetto a quello descritto nella Figura 2, è possibile sollevare obiezioni sia pratiche che teoriche:

[41] Il fatto che il dispositivo funzioni correttamente (hardware e software) e la valuta del software.

[42] Il livello di protezione implementato nel dispositivo (confidenza, integrità, disponibilità, ecc.) sia dal punto di vista dell'*hardware* che del *software*.

[43] Il livello di protezione informatica del *cloud* in cui sono archiviati i dati, anche temporaneamente, e della trasmissione dei dati da e verso il *cloud*. Nel caso in cui il dispositivo sia caratterizzato da funzionamento "*stand alone*" il valore di questo termine sarà considerato massimo.

[44] La possibilità che nel *cloud* i dati vengano elaborati e modificati in qualche modo.

[45] La possibilità che l'osservatore possieda informazioni aggiuntive sulla fonte che origina i dati, ovvero il livello di IQ ottenuto in una precedente indagine sui dati provenienti dalla stessa fonte.

[46] Il rispetto delle normative sulla protezione dei dati, ad esempio in termini di protezione dei dati per impostazione predefinita o per progettazione. Questo requisito è legato al GDPR nell'UE, ma ovviamente dipende dal fatto che nell'ordinamento giuridico preso in considerazione esiste una normativa specifica.

[47] La disponibilità di specifiche tecniche riguardanti il dispositivo e il formato.

[48] Gli strumenti analitici utilizzati dall'osservatore per raccogliere ed elaborare le evidenze.

[49] Il grado di esperienza, abilità e abilità raggiunto dall'osservatore prima dell'osservazione.

1) Potrebbe non essere possibile definire ogni fattore per tutti i tipi di dispositivi IoT. Ad esempio, quello denominato CS sembra implicare che il dispositivo sia sempre connesso, ma sappiamo bene che alcuni dispositivi possono essere utilizzati anche (o esclusivamente) offline.
2) I dati necessari per definire queste variabili potrebbero non essere accessibili, non solo tecnicamente, ma a causa dei vincoli imposti dalle società che le possiedono. Ad esempio, supponiamo che un'indagine in Italia richieda dati relativi a un viaggio di un'auto prodotta da un'azienda straniera. Pensiamo che, per qualche motivo, l'unica copia di questi dati sia conservata in un server situato nel paese in cui ha sede l'azienda: potrebbe essere molto complicato raggiungere una tale fonte e raccogliere dati da essa.
3) I termini di (1) sono la traduzione numerica di aspetti eterogenei, alcuni tecnici, altri per lo più legati al fattore umano, o dipendenti da concetti astratti o modificabili dal legislatore. Pertanto, è arbitrario stimare le loro mutue interazioni, in quanto potrebbero sorgere domande come: è giusto che un aumento di 0,1 nello stato tecnico del dispositivo abbia la stessa influenza su (1) dell'aumento di 0,1 nella conformità alla privacy[50]? Cosa significa aumentare di 0,15 una delle voci? L'idea di un OS "buono" è la stessa in Italia e in Olanda? E, non ultimo, chi decide questi valori?
4) In alcuni casi può essere utile impostare un valore di soglia IN/OUT per l'IQA, un valore al di sotto del quale qualsiasi dato può essere scartato. Si tratta di una scelta investigativa che va attentamente valutata e spiegata con chiarezza. Infatti, tutti gli aspetti dei dati acquisiti meritano di essere approfonditi, senza essere mescolati, o magari confusi o sottovalutati, a prescindere dalla loro qualità.

Possiamo ritenere che la questione sollevata al punto 3) possa essere affrontata con le seguenti precauzioni:

a) Ponderare ogni elemento da aggiungere nella formula, valutando attentamente l'interazione con gli altri addendi;

[50] Il riferimento ovvio è al Regolamento (UE) 679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati), in GUCE L 119, 4.5.2016, p. 1–88.

b) Separare gli elementi in aree diverse. Di conseguenza, per ogni gruppo di prove IoT avremmo tag diversi, ma i punteggi possono rimanere separati.

Riguardo a quest'ultima osservazione, possiamo suddividere gli addendi della formula con due diversi tipi di tassonomie, la cui adozione dipende dall'utilità che risulta più opportuna nella prova. Naturalmente, la scelta di una non esclude necessariamente l'altra, poiché nel processo ogni aspetto può essere utilizzato nell'argomentazione. Possiamo infatti evidenziare i tipi di informazioni ("come", "riguardo la" o "per la" realtà) o gli strati coinvolti, come spiegato nei paragrafi seguenti.

I due diversi tipi di tassonomie ci permettono di mettere a punto il modello fornito sopra in due direzioni opposte.

5.2 *Modello IQA e triplice declinazione del concetto di "informazione"*

Table 4. Corrispondenza tra le due formulazioni del modello IQA.

Tipi di informazione	**Formula (1)**	**Formule (2), (3), (4)**
Intrinseca	DTC	Informazione *come* realtà (rilevanza)
Contestuale	DST	
	CS	
Rappresentazionale	CM	Informazione *sulla* realtà (incertezza)
	SR	
Accessibilità	PC	Informazione *per la* realtà (accountability)
	TDA	
	OT	
	OS	

Nella prima possiamo aggregare i fattori IQA nelle quattro categorie illustrate (cfr. Tab. 4), potendo così suddividere (1) in tre formule, ognuna delle quali prende in considerazione una diversa categoria della Filosofia dell'informazione:

$$\mathrm{IQA_I} = \frac{\sum_{i=1}^{n}(DTC_i + DST_i + CS_i)}{3n} \times 100. \quad (2)$$

$$\mathrm{IQA_{II}} = \frac{\sum_{i=1}^{n}(CM_i + SR_i)}{2n} \times 100. \quad (3)$$

$$\mathrm{IQA_{III}} = \frac{\sum_{i=1}^{n}(PC_i + TDA_i + OT_i + OS_i)}{4n} \times 100. \quad (4)$$

dove:

- $\mathrm{IQA_I}$ = informazione *come* realtà
- $\mathrm{IQA_{II}}$ = informazione *sulla* realtà
- $\mathrm{IQA_{III}}$ = informazione *per la* realtà

5.3 *Modello IQA declinato a seconda del livello tecnologico*

Si nota come (1) può essere modellata considerando che un ambiente IoT è caratterizzato dalla presenza di diversi "livelli": (1) *percezione fisica*, che include l'attività di sensori e attuatori; (2) *livello di rete*, che comprende elaborazione e trasmissione; (3) *livello applicativo*, che corrisponde ai servizi forniti[51]. Questo approccio si può ulteriormente dettagliare, prendendo in considerazione questi tre aspetti per ciascuno dei fattori. Ad esempio, DST – la sicurezza tecnologica del singolo dispositivo – può essere valutata sotto l'aspetto fisico (es. protezione), la sicurezza di rete (es. trasmissione crittografata), e il livello applicativo (es. interfaccia protetta da password).

[51] KARKOUCH et al., *Data quality in internet of things: A state-of-the-art survey*, cit. Tali livelli sono definiti come segue: «*a physical perception layer that perceives physical environments and human social life, a network layer that transforms and processes perceived environment data and an application layer that offers context-aware intelligent services in a pervasive manner*», Z. YAN, P. ZHANG E A. V. VASILAKOS, *A survey on trust management for Internet of Things*, in «Journal of Network and Computer Applications», 42 (2014), pp. 120-134, p. 120.

Table 5. Schema di analisi distribuita per livello[52].

	Requirements (distinti per livello)		
Categorie di informazione	**Livello di percezione fisica**	**Livello di rete**	**Livello applicativo**
Intrinseca	DTCp	DTCn	DTCa
Contestuale	DSTp	DSTn	DSTa
	CSp	CSn	CSa
Rappresentazionale	CMp	CMn	CMa
	SRp	SRn	SRa
Accessibilità	PCp	PCn	PCa
	TDAp	TDAn	TDAa
	OTp	OTn	OTa
	OSp	OSn	OSa

È quindi possibile delineare un ulteriore schema (cfr. Tab. 5), che ci conduce verso la definizione di altre tre formule che ci permettono di prendere in considerazione questo diverso approccio:

$$\mathrm{IQA_p} = \sum_{i=1}^{h} \left(\frac{\sum_{j=1}^{m_{p_i}} f_{p_j}}{m_{p_i}} \right) \tag{5}$$

$$\mathrm{IQA_n} = \sum_{i=1}^{h} \left(\frac{\sum_{j=1}^{m_{n_i}} f_{n_j}}{m_{n_i}} \right) \tag{6}$$

$$\mathrm{IQA_a} = \sum_{i=1}^{h} \left(\frac{\sum_{j=1}^{m_{a_i}} f_{a_j}}{m_{a_i}} \right) \tag{7}$$

dove:

- *h* rappresenta il numero dei dispositivi che sono tenuti in considerazione nell'attività forense;

[52] Naturalmente, OT e OS dipendono dall'osservatore, che è un essere umano. Ciò significa che i fattori rappresentano l'apparato tecnico utilizzato dal consulente e le competenze acquisite in ciascun campo. Ad esempio, un consulente potrebbe avere uno strumento molto avanzato per l'analisi dei dispositivi (OTp), ma non la stessa capacità di garantire la sicurezza della connessione (OTn) o le competenze per valutare come vengono erogati i servizi (OTa).

- i = i-mo dispositivo;
- m_{p_i}, m_{n_i} e m_{a_i}rappresentano il numero di fattori che possono essere considerati, rispettivamente, nel mondo fisico, a livello di rete o di applicazione, per il l'i-mo dispositivo. Ciò perché, come sopra chiarito, non tutti i fattori della tabella 3 devono necessariamente essere presenti nella formula.
- f_{p_j}, f_{n_j} e f_{a_j} rappresentano i singoli fattori che devono essere valutati (i.e. DTC_p).
- IQA_p= qualità dell'informazione del livello – percezione del mondo fisico;
- IQA_n = qualità dell'informazione del livello – rete;
- IQA_a = qualità dell'informazione del livello – applicazioni.

Nella prossima sezione esporremo un caso di studio che permette di apprezzare come i termini definiti astrattamente in (1), e riutilizzati in (2), (3) e (4), possano essere valutati e sfruttati in pratica[53].

6. Dal modello alle indagini reali: caso di studio

Come applicazione di tutte le suddette formule ad uno scenario reale, di seguito proponiamo una situazione operativa riguardante la questione dell'Information Quality Assessment nel caso di un insieme eterogeneo di dispositivi digitali.

Poniamo che sulla scena del crimine sia stato sequestrato un set di dispositivi digitali IoT. Nello specifico:

1) uno smartphone;
2) la SIM Card al suo interno;
3) un drone;
4) uno smartwatch;
5) un computer portatile;
6) una smartTV.

Un esperto di Digital Forensics, prima di analizzare in profondità queste fonti di evidenza, deve valutare l'IQ di ogni singolo dispositivo e del gruppo di evidences acquisite.

[53] Solo per ragioni di spazio non prendiamo in considerazione le formule (5), (6) e (7).

Confrontare i QI dei dispositivi e valutare il QI complessivo prendendo in considerazione tutti i termini che compongono (1) potrebbe essere un compito difficile. Infatti, i produttori di dispositivi potrebbero non rendere (o non aver reso ancora) pubbliche le informazioni tecniche richieste e, anche se rilasciati, tali dati potrebbero non essere dettagliati quanto necessario. Inoltre, le informazioni all'interno di ciascun dispositivo potrebbero essere organizzate e archiviate in modi diversi, a seconda delle politiche del rispettivo marchio. Il livello di queste valutazioni dovrebbe essere simile a quanto esposto in autorevole letteratura sull'argomento[54], dove il file system, la forma e il formato dei file di log e altri utili indizi forensi sono esposti in caso di drone, smartTV e smartwatch. Dopo questo tipo di analisi approfondite, potremmo riempire una tabella come la tabella sottostante (Cfr. Tab. 6)[55], quindi implementare (1), (2), (3) e (4), e generare così una serie di grafici che permettano di comprendere meglio il QI delle fonti di evidenza esaminate. Per il test abbiamo considerato i seguenti dispositivi:

1. Smartphone Huawei modello ALE-L21 (P8 Light), con Android 6.0, 2 Gb RAM, CPU Octa-core 1.2 GHz, versione Kernek 3.10.86-g33ff982;
2. Nano SIMCard 4G Telecom Italia anno 2017;
3. Drone[56];
4. Smart TV[57];

[54] D. R. Clark, C. Meffert, I. Baggili e F. Breitinger, *DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III*, in «Digital Investigation», 22 (2017), pp. S3-S14; A. Boztas, A. R. J. Riethoven e M. Roeloffs, *Smart TV forensics: Digital traces on televisions*, in «Digital Investigation», 12 (2015), pp. S72-S80; N. R. Odom, J. M. Lindmar, J. Hirt e J. Brunty, *Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices*, in «J Forensic Sci», 64 n. 6 (2019), pp. 1673-1686.

[55] Il valore numerico inserito in questo esempio per ogni voce non è indicativo. Si tratta di valori esemplificativi inseriti esclusivamente ai fini di questo lavoro. Essi sono stati calcolati dopo una valutazione fatta dagli autori, e potrebbero essere soggetti a variazioni significative a seconda di molte ragioni, ad es cambiamenti nelle leggi, miglioramenti tecnici, capacità tecniche migliorate e così via. Il loro scopo è consentire il calcolo dei QI richiesti e la rappresentazione grafica dei risultati.

[56] Clark et al., *DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III*, cit.

[57] Boztas et al., *Smart TV forensics: Digital traces on televisions*, cit.

5. IBM Thinkpad Edge E30, o.s. Windows 10, 8 GB di RAM, processore Intel i5;
6. Smartwatch[58].

Table 6. Valori numerici dei termini in (1) per i dispositivi 1 – 6[59].

Dispositivo 1 Smartphone		Dispositivo 2 SIMCard		Dispositivo 3 drone		Dispositivo 4 smartTV		Dispositivo 5 pc laptop		Dispositivo 6 Smartwatch	
DTC	0,56	DTC	0,93	DTC	0,97	DTC	0,91	DTC	0,39	DTC	0,89
DST	0,62	DST	0,12	DST	0,48	DST	0,16	DST	0,30	DST	0,82
CS	0,47	CS	1,00	CS	0,69	CS	0,91	CS	0,48	CS	0,44
CM	0,34	CM	0,17	CM	0,76	CM	0,80	CM	0,58	CM	0,85
SR	0,48	SR	0,76	SR	0,50	SR	0,98	SR	0,56	SR	0,18
PC	0,77	PC	0,82	PC	0,77	PC	0,80	PC	0,00	PC	0,98
TDA	0,55	TDA	0,60	TDA	0,21	TDA	0,99	TDA	0,26	TDA	0,65
OT	0,84	OT	0,07	OT	0,89	OT	0,80	OT	0,07	OT	0,89
OS	0,26	OS	0,88	OS	0,45	OS	0,95	OS	0,79	OS	0,31

Applicando (1), (2), (3) e (4) a tutti i dispositivi, con i dati esposti in Tab.7 come input, si ottengono i seguenti interessanti risultati: l'IQA dell'insieme di tutti i dispositivi sequestrati è di circa 62%, il dispositivo nr.4 è quello che ottiene il miglior risultato in termini di Information Quality, mentre il dispositivo nr.5 ha le peggiori prestazioni:

Table 7. Risultati degli indici IQA.

IQA_I	IQA_{II}	IQA_{III}			IQA_{tot}
61,96 %	56,30 %	54,74 %			62,04 %
$IQA_{device1}$	$IQA_{device2}$	$IQA_{device3}$	$IQA_{device4}$	$IQA_{device5}$	$IQA_{device6}$
54,37 %	59,49 %	63,73 %	89,79 %	38,19 %	66,68 %

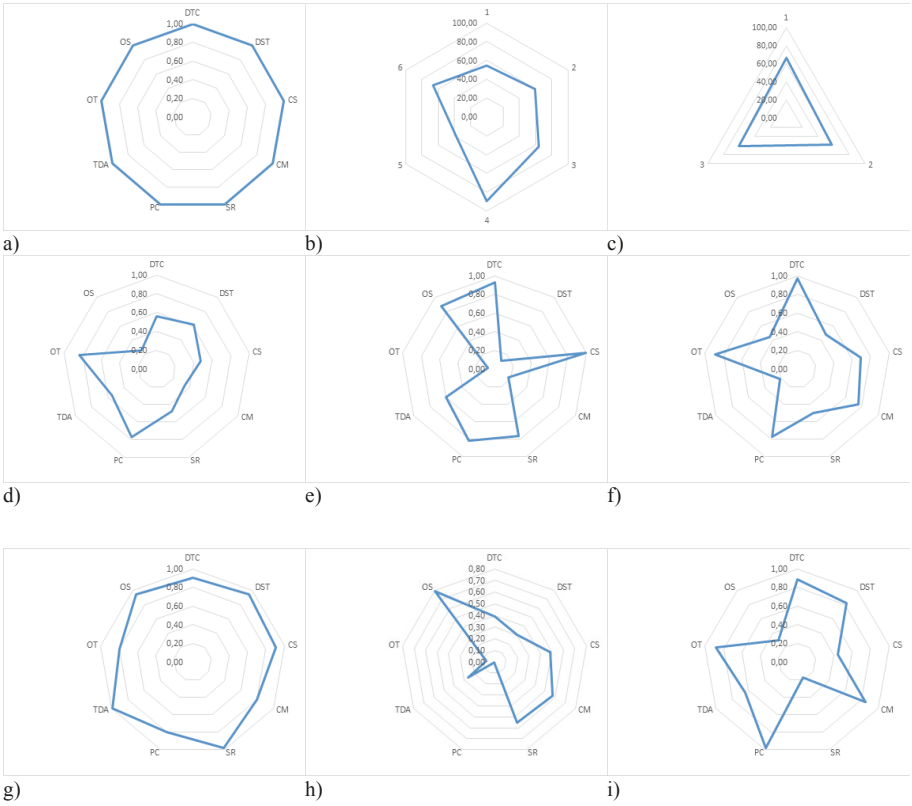
La QI può essere chiaramente visualizzata anche da un insieme di diagrammi come quelli esposti nello schema seguente (cfr. Tab. 8), in cui è mostrato un insieme di valutazioni, considerando il totale degli apparati acquisiti, ed ogni dispositivo valutato singolarmente. La lettera a) rappresenta il miglior risultato che si può ottenere: tutti gli elementi

[58] ODOM et al., *Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices*, cit.

[59] Naturalmente, OT e OS dipendono dall'osservatore, che è un essere umano. Ciò significa che i fattori rappresentano l'apparato tecnico utilizzato dal consulente e le competenze acquisite in ciascun campo. Ad esempio, un consulente potrebbe avere uno strumento molto avanzato per l'analisi dei dispositivi (OTp), ma non la stessa capacità di garantire la sicurezza della connessione (OTn) o le competenze per valutare come vengono erogati i servizi (OTa).

che compongono la valutazione hanno i valori più alti, ed infatti il poligono è completamente circondato dalla linea blu. La lettera b) mostra contemporaneamente l'IQA di tutti i dispositivi esaminati, e permette di apprezzare immediatamente il miglior risultato dato dal dispositivo 4 già evidenziati. La lettera c) mostra insieme il calcolo dell'IQA con (2), (3) e (4), mentre ogni lettera da d) a i) rappresenta le prestazioni di ogni singolo dispositivo. Anche dal confronto tra questi ultimi set di immagini, si individuano facilmente le migliori prestazioni del dispositivo 4.

Table 8. Rappresentazione grafica degli indici risultanti dal caso di studio.



7. Ulteriore implementazione del modello

L'utilità dell'IQA (valutazione della qualità delle informazioni) implica che tale valore sia comunicato assieme alle prove analizzate. Ciascuna prova potrebbe quindi essere accompagnata da una serie di file contenenti metadati che descrivano le informazioni critiche (il processo di acquisizione utilizzato, l'output ottenuto, hash, codec e software necessari per fruire) e l'IQA. Abbiamo ipotizzato due possibili sviluppi, non mutualmente escludibili, utili a favorire l'elaborazione automatica della qualità del dato forense.

La prima implementazione riguarda il DFXML (Digital Forensics XML, un linguaggio XML utilizzato per automatizzare i processi di digital forensics, sviluppato da Simson Garfinkel[60]. Il DFXML contiene informazioni sia riguardo il risultato del processo sia gli strumenti utilizzati, è citato dal NIST[61] (National Institute of Standards and Technology) ed è adottato all'interno di software commerciali e open source[62]. Il suo schema è liberamente consultabile in Github[63].

L'implementazione dell'IQA richiederebbe l'introduzione di alcuni elementi non attualmente presenti nel DFXML e quindi comporterebbe il rilascio di una nuova versione dello schema. Il risultato finale sarebbe simile all'esempio seguente, che ipotizza l'acquisizione di un file video scambiato su WhatsApp.

Table 9. Metadati IQA.

```
<?xml version="1.0" encoding='UTF-8' ?>
<dfxml version='1.1.0'>
  <metadata xmlns:dc='http://purl.org/dc/elements/1.1/' xmlns:usg="#usg">
    <dc:type>Video file</dc:type>
  </metadata>
  <creator>
    <program>XYZ WhatsApp iOS Extractor</program>
    <version>1.1.2</version>
    <execution_environment>
```

[60] S. Garfinkel, *Digital forensics XML and the DFXML toolset*, in «Digital Investigation», 8 n. 3-4 (2012), pp. 161-174
https://simson.net/clips/academic/2012.DI.dfxml.pdf.

[61] https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/technical-information/dfxml.

[62] https://forensicswiki.xyz/wiki/index.php?title=Category:Digital_Forensics_XML

[63] https://github.com/dfxml-working-group/dfxml_schema

```
        <start_time>2023-12-17T18:20:24Z</start_time>
        <username>user_AC1280</username>
      </execution_environment>
    </creator>
    <source>
      <device_model>Apple iPhone 19.2</device_model>
      <device_sn>Z7KNR012H4MR</device_sn>
         <os_version>25.3.1</os_version>
      <app_id>29162302_whatsappios</app_id>
      <app_version>512.640</app_version>
      <app_data>account:+39111222333</app_version>
    </source>
    <fileobject>
      <filename>VID-20231202-WA0117.mp4</filename>
      <filesize>13143968</filesize>
      <libmagic>video/mp4</libmagic>
                                                                <hashdigest
type='sha512'>e7c1fd0dfa0a240c1cb7cda71a49f2f146dead49c61e36f104d46351
7d3eb77046020efe2b50250af5529d075c5e768f834d0e5dec627eb8d66c6041b5b
b83df</hashdigest>
    </fileobject>
    <iqa><total>82.00%</total></iqa></dfxml>
```


Un ulteriore sviluppo, che riteniamo più promettente è l'implementazione dell'IQA nell'ontologia CASE[64]. Come è noto, CASE (Cyber-investigation Analysis Standard Expression) è un'estensione dell'Unified Cyber Ontology (UCO) che supporta le cyber investigazioni in ambito penale, aziendale e di intelligence, ambiti in cui l'IQA potrebbe essere estremamente rilevante. L'IQA può essere efficacemente introdotto nell'ontologia CASE come Facet[65], rappresentandolo come un attributo. Il Facet IQA applicato all'elemento prova finale è quindi in grado di fornire l'IQA complessivo. L'ontologia CASE risulta di particolare interesse in quanto prevede una gestione automatica della "Catena di Custodia" e in generale della provenienza di ciascun elemento, mediante le classi InvestigativeAction e ProvenanceRecord che permettono di risalire agli step precedenti che hanno portato all'*evidence* decisiva. La nostra proposta è quindi quella di accompagnare ciascuno

[64] E. Casey, S. Barnum, R. Griffith, J. Snyder, H. van Beek e A. Nelson, *Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language*, in «Digital Investigation», 22 (2017), pp. 14-45, https://caseontology.org/.

[65] CASE utilizza i Facet come attributi degli Observable Objects.

di questi step con il relativo IQA: questo permetterebbe all'esaminatore di valutare quali passaggi hanno influito sull'eventuale perdita di qualità dell'informazione.

8. Considerazioni finali

Se è vero che gli esiti dei procedimenti giudiziari dipendono in ultima analisi dalla valutazione del giudice, non si può negare che tutti gli attori del processo possono, in modo più o meno determinante, condizionarne le conclusioni. In questo scenario, il divario tra le competenze necessarie per affrontare e gestire le prove digitali e le competenze in materia da parte degli operatori ai vari livelli, è senza dubbio una delle cause più frequenti di errori di valutazione. È quindi fondamentale migliorare l'efficienza e l'efficacia dei procedimenti che riguardano l'acquisizione delle prove e sensibilizzare tutti i professionisti coinvolti sulla natura peculiare delle prove digitali.

Tra le numerose sfide affrontate attualmente dalla Digital forensics, gli ostacoli e le complessità introdotte dalle tecnologie IoT sono le più impegnative, per ragioni sia pratiche che teoriche.

Dal punto di vista teorico, si pone il problema della qualità delle risorse informative acquisite come fonti di prova, questione che dovrebbe essere presa in considerazione nella progettazione dei dispositivi e degli ecosistemi IoT. Non è un caso se il riferimento alla qualità del dato rappresenta un requisito previsto per ottenere la certificazione dei sistemi di intelligenza artificiale da parte della Proposta di Regolamento (UE) "Legge sull'Intelligenza Artificiale" attualmente in discussione nel Parlamento Europeo[66].

Da un punto di vista pratico, uno dei problemi principali nella IoT Forensics è bilanciare quantità e qualità dei dati acquisiti. Scartare a priori i dati di bassa qualità espone al rischio di cancellare dettagli importanti, ma un minimo livello di qualità è richiesta, ad esempio per poter eseguire in modo affidabile analisi su grandi quantità di dati utilizzando metodi automatici. Per questo motivo gli esperti, a monte delle fasi di analisi ed interpretazione delle evidenze raccolte, devono porsi

[66] Proposta di Regolamento del Parlamento Europeo, c.d. Legge Sull'intelligenza Artificiale, COM/2021/206 final.
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri= CELEX:52021PC0206.

il problema di quali tipi di dati sia necessario acquisire, e come possano essere manipolati senza violare il principio di pertinenza. In questa prospettiva la valutazione inerente la IQ potrebbe essere considerata una sorta di metadato: informazione sull'informazione.

In questo contributo abbiamo delineato, dopo aver descritto il quadro teorico di riferimento, un modello per valutare la IQ nella IoT Forensics, prima in una formula generale e successivamente in tre applicazioni. Per quanto a nostra conoscenza, questo è il primo tentativo di fornire un approccio analitico/matematico ad una questione puramente teorica come quella dell'argomentazione giuridica sottesa alla valutazione delle prove in giudizio provenienti da un ambiente IoT[67].

In futuro ci proponiamo di proseguire lungo questa via con ulteriori approfondimenti: implementare il nostro approccio esplorando la possibilità di creare ed alimentare con continuità un database per ogni tipo di dato, permettendoci così di ottenere statistiche "robuste"; tentare nuovi approcci che utilizzino teorie matematiche avanzate, ad esempio la teoria dei modelli di statistici gaussiani[68] o le Reti Neurali, o ancora integrando il livello di complessità ISO/OSI aggiungendovi ulteriori quattro livelli basati sull'interazione con il fattore umano, fondamentale in ogni contesto forense. Proprio quest'ultima osservazione ci conduce verso un ulteriore raffinamento della figura dell'osservatore, ora generalmente espresso come OS.

[67] La nostra ricerca si è sviluppata in diverse fasi, cfr. F. COSTANTINI, M. ALVISE DE STEFANI E F. GALVAN, *The «Quality of Information» Challenges in IoT Forensics: An Introduction*, in «Jusletter IT», n. 21 February 2019 (2019); F. GALVAN, F. COSTANTINI E S. BATTIATO, *A Case Study for an "Accountable" IoT Forensics*, in *Verantwortungsbewusste Digitalisierung / Responsible Digitalization. Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020 / Proceedings of the 23rd International Legal Informatics Symposium IRIS 2020*, Eric Schweighofer, Walter Hötzendorfer, Franz Kummer e Ahti Saarenpää (a cura di), Bern, Weblaw (Colloquium; II.28), 2020, pp. 533-542; F. COSTANTINI, F. GALVAN, M. ALVISE DE STEFANI E S. BATTIATO, *Assessing "Information Quality" in IoT Forensics: Theoretical Framework and Model Implementation**, in «Journal of Applied Logics — IfCoLog Journal of Logics and their Applications», 8 n. 9 (2021), pp. 2373-2406

[68] D. REYNOLDS, *Gaussian Mixture Models*, in *Encyclopedia of Biometrics*, Stan Z. Li e Anil Jain (a cura di), Boston, MA, Springer US, 2009, pp. 659-663; Traditional Forensic Voice Comparison with Female Formants: Gaussian Mixture Model and Multivariate Likelihood Ratio Analyses, Proceedings of the 13th Australasian International Conference on Speech Science and Technology, pp. 42-45; XINYI WANG, SHAOZHANG NIU E JIWEI ZHANG, *Digital Image Forensics Based on CFA Interpolation Feature and Gaussian Mixture Model*, in «IJDCF», 11 n. 2 (2019), pp. 1-12.

Infine, come ulteriore applicazione del modello proposto, riteniamo che in un futuro non troppo lontano potrebbe essere sviluppato un sistema di classificazione dei dispositivi digitali, simile a quello attualmente adottato per il consumo energetico, relativo al grado di sicurezza informatica ed all'affidabilità in caso necessità di analisi forense.

Riconoscimenti

Il contributo è il risultato di una ricerca congiunta compiuta dagli autori, tuttavia, i singoli paragrafi devono essere attribuiti come segue: 1-3 Federico Costantini, 4 e 7 Marco Alvise De Stefani, 5 e 6 Fausto Galvan, 8 Sebastiano Battiato.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643010
pp. 187-205 (gennaio 2022)

Cyberlaundering e *Blockchain Forensics*: aspetti giuridici e tecnici del riciclaggio di criptovalute

Pasquale Sammario[1], Raffaella Brighi[1]

1. Introduzione

La dematerializzazione del contante con la rapida ascesa e diffusione delle criptovalute nelle transazioni finanziarie – resa sempre più florida dagli emergenti *asset* della *distributed economy* – costituisce il substrato ideale per l'affermazione e lo sviluppo del fenomeno del *cyberlaundering*, una nuova frontiera del riciclaggio che combina le potenzialità delle reti informatiche alle peculiari caratteristiche tecniche delle *cryptocurrencies,* con l'obiettivo di dare nuova linfa ai proventi illeciti compendio di attività criminali.

Le *utilities* offerte dalle criptovalute nel garantire la totale riservatezza delle singole operazioni effettuate mediante la pseudonimizzazione e cifratura dei dati personali, con le indubbie difficoltà tecniche di un loro tracciamento frutto della virtualizzazione del processo di creazione, allocazione e gestione delle stesse, rendono il *cyberspace* il luogo perfetto ove si perfezioni l'intero ciclo di "ripulitura" delle risorse delittuose.

L'esigenza di offrire una disamina unitaria al fenomeno del *cyberlaundering,* nel contesto più ampio dei *cybercrimes,* impone una trattazione che tenga conto tanto delle principali implicazioni giuridiche sottese, quanto degli aspetti tecnici relativi alla tecnologia alla base del funzionamento delle criptovalute: la *blockchain*. In tal senso, la prima parte del contributo muoverà l'analisi dalla sussumibilità delle condotte prodromiche ed esecutive dell'attività di *cyberlaundering* negli schemi codicistici del diritto penale, tentando di collocare tale fenomeno nel contesto dei delitti contro il patrimonio – nello specifico dei delitti di riciclaggio, reimpiego ed autoriciclaggio di cui agli artt. *648-bis, 648-ter e 648-ter.1* del codice penale – analizzandone le fattispecie strumen-

[1] CIRSFID – Alma Human Artificial Intelligence, Università di Bologna.

tali e i delitti-presupposto che si inseriscono nell'ampia trama delle fasi del cybericiclaggio. Uno sguardo è rivolto alle possibili soluzioni in ottica di prevenzione del fenomeno, alla luce della recente legislazione di matrice europea in materia di antiriciclaggio. In seguito, passate brevemente in rassegna le principali caratteristiche relative all'infrastruttura e al funzionamento della *blockchain,* si esplorerà il perimetro della *Blockchain Forensics* per riferirsi al complesso delle attività di *forensics* applicate alla tecnologia *blockchain,* al fine di individuare e acquisire potenziali evidenze digitali ivi allocate, in particolare agli *artifacts* generati dall'utilizzo delle criptovalute, con un *focus* conclusivo sullo stato dell'arte delle migliori pratiche.

2. Nuove tecnologie per vecchi crimini: il *cyberlaundering*

Da quando le criptovalute sono approdate nel mondo dei mercati finanziari nel primo decennio degli anni duemila[2], si è assistito ad un costante e significativo aumento del volume delle transazioni generate in rete, con una capitalizzazione odierna di più di mille miliardi di dollari tra le oltre sei mila diverse tipologie in circolazione[3], divenendo di fatto la forma di pagamento *online* più versatile, veloce e sicura.

Una simile diffusione delle *cryptocurrencies* trova una propria *ratio* nell'ontologica natura delle stesse: un flusso di *bits* codificati per funzionare come mezzo di scambio in cui i singoli *record* di proprietà della monete sono archiviati in un registro distribuito, la *blockchain*, che utilizza una crittografia avanzata per proteggere i *record* delle transazioni, per controllarne la creazione di nuove monete e per verificare il trasferimento della proprietà delle stesse[4].

Il progresso della tecnica di crittografia e della tecnologia *blockchain*[5] ha reso la criptovaluta un mezzo di scambio alternativo alle

[2] Si fa riferimento alla nascita di *Bitcoin* con la pubblicazione nell'ottobre del 2008 del *paper* di Satoshi Nakamonto*, Bitcoin: A Peer-to-Peer Electronic cash system*, consultabile all'indirizzo https://bitcoin.org/bitcoin.pdf.

[3] Un elenco di 6714 criptovalute è su *CoinMarketCap.com* di ottobre 2021.

[4] S. Mahajan, A. Sharma, *The Era of Cryptocurrency,* in *International Journal of Innovative Science and Research Technology*, Volume 6, Issue 8, August 2021, p. 1190.

[5] L'interesse per la *Blockchain* è esploso negli ultimi anni. Il numero di pubblicazioni presenti in letteratura sull'argomento è aumentato da 2 nel 2013 (il primo anno in cui sono iniziate le pubblicazioni su *Blockchain*), a 4 nel 2014, a 21 nel 2015, a 118 nel 2016, al 521 nel 2017,

valute legali, ancorando tale successo alle quattro peculiari caratteristiche tecniche che la contraddistinguono:

1) la *decentralizzazione*, che implica l'assenza di un'autorità centrale che ne controlla e regola l'emissione[6];
2) l'*immutabilità* del registro ove vengono archiviate le transazioni, che elimina l'attuale sistema di controllo delle valute legali e di fiducia per riporla unicamente in un *network* di utenti[7];
3) lo *pseudo-anonimato*, basato su un sistema a crittografia a chiave pubblica, che elide la necessità per gli *users* di una previa identificazione su canali istituzionali, rendendo agevole la creazione di identità digitali anonime e portafogli virtuali per effettuare transazioni sul sistema decentralizzato con la garanzia di autenticarle in modo sicuro;
4) l'*offerta limitata* che, ricalcando lo schema dell'oro quale bene prezioso esauribile presente in natura, sottrae la valuta da un controllo diretto teso ad evitare, o quantomeno arginare, comportamenti inflazionistici.

Sviscerata, dunque, l'intrinseca natura delle valute virtuali, la rivoluzione tecnologica delle *cryptocurrencies*, come ogni rivoluzione legata allo sviluppo delle Tecnologie dell'Informazione e della Comunicazione *(TIC),* serba, tuttavia, il concreto pericolo di una deriva distopica del loro utilizzo[8], rappresentando un fertile terreno per il proliferare del *cybercrime,* intenso, in senso ampio, quale risultato dell'evoluzione della stessa tecnologia informatica[9]. È proprio in questa articolata trama dei *cybercrimes* che si colloca il recente fenomeno del *cyberlaundering*, definito come la *"nuova frontiera del riciclaggio"*[10], che – con-

al 1954 nel 2018, a 3667 nel 2019 e al 3945 nel 2020. A partire dal 29 giugno, sono stati pubblicati nel 2021 1569 articoli. Cfr. W. ZHAO *[et al], Blockchain Technology: Principles and Applications, Special issue,* IEEE Access, vol. 9, 2021.

[6] Come è noto, le transazioni sono registrate in un registro pubblico distribuito, la *blockchain*, e verificate dai nodi stessi della rete tramite crittografia.

[7] G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico,* Zanichelli, Bologna, 2019, pag. 269 ss.

[8] Sull'utilizzo delle crittomonete nelle attività illecite, si veda, *inter alias*, G. COSTABILE in *Le indagini digitali* in Aterno, Cajani, Costabile, Curtotti (a cura di) *Cyber forensics e indagini digitali*, Giappichelli, 2021, pp.124-125.

[9] L. FLORIDI, *La rivoluzione dell'informazione*. Codice Edizioni, Torino 2012.

[10] E. SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio*, in *Rivista trimestrale di Diritto penale dell'Economia*, 4, 2015.

densando al proprio interno un insieme eterogeneo di attività dirette ad occultare la provenienza delittuosa di capitali, beni, valori o altre utilità, mediante le potenzialità delle reti e dei sistemi informatici – va a inquadrarsi nel novero dei cd. *computer related crimes*[11] quale naturale progressione nell'era della dematerializzazione del tradizionale *money laundering*[12].

L'ampia nozione appena apprestata condensa il fenomeno in una duplice prospettiva inquadrandolo, da un lato, come un sottoinsieme dei *cybercrimes tout court* da collocare nelle maglie delle tradizionali fattispecie codicistiche positivizzate e, dall'altro, come procedura informatizzata strumentale alla tradizionale "ripulitura" del provento illecito che ricomprende un novero di condotte delittuose funzionalmente differenti e pertanto distinte dalla condotta pura del riciclaggio, eppur tuttavia idonee a fungere da presupposto ovvero da strumento per la sua realizzazione.

Riprova di condotte presupposto rivengono nelle classiche, e sempre in costante evoluzione, tecniche di *social engineering*, basate sullo studio e sulla manipolazione dei comportamenti delle persone, con l'obiettivo di raccogliere informazioni confidenziali e private. Si pensi al *phishing*, forse la tecnica più nota quanto efficace, con la quale viene veicolato un messaggio malevolo – tradizionalmente tramite *mail*, ma anche tramite sms (*smishing*) o chiamate (*vishing*) – che per fattura o contenuto inganna l'utente inducendolo a fornire credenziali di account personali (ad esempio quello dell'*home banking),* ovvero al *pharming*, che coinvolge un insieme di utenti indistinti tramite la contraffazione di un sito *Internet* affidabile sul quale l'ignaro utente immette i propri dati[13]. Tali tecniche di *social engeneering* vengono ricomprese nella

[11] Con tale espressione si suole riferirsi ai casi in cui i *computer*, ma in generale i sistemi informatici, siano strumento per la commissione di un reato, diversamente dai casi in cui gli stessi siano oggetto del reato, cd. *computer crime.* Cfr. N. Haynes, *Cyber Crime,* Editech, 2018, p. 76 ss.

[12] Per *money laundering* s'intende la forma classica del riciclaggio. Il termine (letteralmente "lavaggio di denaro") deriva dalla prassi utilizzata dal gangster Al Capone di mescolare i proventi illeciti della propria attività criminale con la liquidità proveniente dalle casse delle lavanderie automatiche (*laundrettes*) da lui possedute nella Chicago degli anni Venti, allo scopo di occultarne l'illecita provenienza e giustificarne l'esistenza. Cfr. G. Pogliani, N. Pecchiari, M. Mariani, *Frodi aziendali. Forensic accounting, fraud auditing e litigation,* Egea, 2016, p. 195 ss.

[13] P. Kalaharsha, B.M. Mehtre, *Detecting Phishing Sites - An Overview*, *ResearchGate,* all'indirizzo https://www.res earchgate.net/publication/350371788. Per un maggiore approfondimento sull'argomento si veda il contributo di *U. Bardari, Dal* Phishing *allo* SMiShing. *Strumenti di prevenzione e repressione delle frodi informatiche.*

fattispecie penale della frode informatica ex art. 640-ter c.p. la quale comprende un insieme eterogeneo di attività dirette ad intervenire sui sistemi informatici o telematici mediante accesso abusivo, per poi disporre, tra le diverse possibili condotte, bonifici, transazioni, alterazioni di coordinate iban e, a più ampio raggio, manipolazione di dati e programmi da cui consegua l'ingiusto profitto presupposto del successivo trasferimento od impiego dei proventi illeciti così conseguiti[14].

Non solo condotte presupposto, ma anche condotte strumentali si inseriscono nel complesso meccanismo di ripulitura informatica dei proventi illeciti, rimanendo, tuttavia, da essa separate, in una sorta di posizione 'servente' che, come tale, fa conseguire autonoma rilevanza penale. Ne costituiscono manifestazioni il furto d'identità digitale (art. 494 c.p.), che si realizza attraverso la falsificazione o sottrazione dei documenti identificativi degli utenti *target* al fine di procedere all'attivazione di carte di credito o conti bancari strumentali su cui far affluire il denaro 'sporco', così come l'accesso abusivo ai suddetti sistemi informatici (art. 615-ter c.p.) o, ancora, la clonazione delle carte di credito e di pagamento (art. 493-ter c.p.), condotte strumentali, talvolta indispensabili, per occultare almeno in una prima parte l'intricata catena del *laundering.*

3. Le fasi e le tecniche del riciclaggio "*via cripto*"

Un *file rouge* che da sempre lega trasversalmente i criminali di epoche differenti risiede nella predisposizione di tecniche, sempre più innovative quanto talvolta geniali, atte ad ostacolare la conoscenza del fatto di reato, al fine di conseguirne l'impunità. La diffusione delle criptovalute come sistema di scambio di valore completamente virtualizzato ha di fatto risolto uno dei più grandi ostacoli che si presentavano nel riciclaggio: il contante. Si è cosi assistito al passaggio dall'esportazione fisica del denaro illecito attraverso le frontiere al trasferimento dello stesso con un semplice *click*.

Se da un lato, dunque, la dematerializzazione del contante ha reso più agevole lo spostamento di enormi capitali illeciti, necessitando soltanto di una connessione a *Internet* per raggiungere la moltitudine delle *smart utilities* a tal fine funzionali, dall'altro, ha inciso significativa-

[14] L. Picotti, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio,* in *Rivista trimestrale di Diritto penale dell'Economia*, 3-4/2018, pp. 610 e ss.

mente sulle classiche tre fasi cui si articola il riciclaggio tradizionale che, nella versione informatica, tendono ad assumere una rilevanza distintiva sempre più labile.

1) Il *Placement* è la fase in cui i capitali o le altre utilità proventi di illeciti vengono collocati nell'economia legale; si verifica quando il denaro "sporco" viene convertito in criptovalute e utilizzato per acquistare beni e servizi col fine di ripulirlo o convertirlo in 'denaro legale'. Esso assume fondamentale importanza nel cd. *"riciclaggio digitale strumentale"*, ove il posizionamento nell'economia dei beni di provenienza delittuosa avviene con la loro smaterializzazione[15], attraverso appositi *exchange providers;* di contro, detta fase risulta superflua, come si vedrà, nel cd. *"riciclaggio digitale integrale"*, in cui i proventi illeciti si presentano già in forma dematerializzata (es. denaro su conti *online* ovvero in criptomonete). Quanto alle tecniche mediante le quali tale fase si estrinseca, si spazia dagli investimenti in azioni societarie lecitamente quotate all'acquisto di moneta legale o, ancora, attraverso il gioco *online* la cui vincita si riconverte in denaro pulito.
2) Il *Layering* è la fase di dissimulazione del provento illecito che si esplica attraverso una serie 'stratificata' di operazioni finanziarie atte ad occultare, facendo perdere le tracce, la reale provenienza del capitale illegale; anche in questo caso diverse sono le tecniche mediante le quali si esplica: dall'utilizzo di società di comodo virtuali[16] per il trasferimento *offshore* dei fondi, all'acquisto di beni *online* per futura rivendita, ovvero tramite *home banking* con l'apertura di conti virtuali fraudolenti, resi possibili da talune condotte presupposto che si è *supra* analizzato, quali il furto di identità digitale[17]. Una tecnica particolarmente insidiosa che si è sviluppata con l'avvento della tecnologia *blockchain* è quella del cd.

[15] GUTTMANN, *Cybercash: The Coming Era of Electronic Money,* Palgrave Macmillan, Basingstoke, 2003.

[16] «Le shell companies sono società che sostanzialmente non esercitano alcuna attività commerciale e vengono costituite col solo fine di farvi depositare il capitale illecito per essere poi reintrodotto nell'economia reale con l'accordo di un prestanome». Cfr. A. ROSATO, *Profili penali delle criptovalute*, in *Quaderni del Centro Ricerca Sicurezza e Terrorismo*, Pacini Giuridica, 2021, p. 70.

[17] Si parla a proposito di *money mule,* o testa di legno, per riferirsi appunto a quelle identità virtuali fittizie attraverso cui è possibile aprire un conto online senza sottostare ai controlli imposti alle banche al momento della registrazione di un nuovo cliente. Cfr. A. ROSATO, *ibidem*., p. 69.

mixing che consiste nell'occultare il *paper trail*[18] servendosi di appostiti soggetti, i cd. *mixers*, i quali, dietro commissione, 'mischiano' le criptovalute illecite in entrata con altre lecite restituendole in un formato pressoché anonimo solo dopo una lunga serie di transazioni strumentali a confondere gli indirizzi.

3) L'*Integration* è l'ultima fase e deriva dalla necessità di creare un'apparenza di legittimità del capitale illecito ripulito; se nella fase di stratificazione, dunque, l'obiettivo chiave del *cyberlaunderer* è quello di creare una rete di complessità al fine di eludere la tracciabilità del provento illecito da parte delle autorità di regolamentazione, in questa fase l'esigenza fondamentale è la reintroduzione del capitale illecito, ormai ripulito, nel circuito economico[19]. Tra le diverse tecniche all'uopo predisposte, per la peculiare ingegnosità del meccanismo cui si perfeziona, si annovera il cd. *loan back*[20]*:* una complessa operazione di finanziamento di capitali attraverso la quale un soggetto, nel nostro caso il *cyberlaunderer,* contrae un prestito con un istituto finanziario al fine di realizzare una determinata attività, il più delle volte fittizia, ponendo come garanzia dello stesso un *quantum* di criptovalute di illecita provenienza; alla scadenza del prestito, il mancato adempimento dell'obbligazione finanziaria determina l'escussione della garanzia in criptovaluta da parte della banca, così perfezionandosi il reinserimento dei capitali delittuosi nell'economia reale.

Ebbene, ripercorse analiticamente le fasi attraverso le quali si snoda l'intricata catena del riciclaggio, di prima evidenza si rileva come, differentemente dal tradizionale *money laundering* ove ciascuna delle suddette fasi assumeva autonoma e necessaria rilevanza per la proficua riuscita dell'attività delittuosa, nel *cyberlaundering* tale rigida triparti-

[18] Per *Paper Trail* si intende la catena di transazioni economiche e/o finanziarie che, al proprio apice, porta all'identificazione del soggetto titolare dei proventi illeciti. Cfr. F. BRIZZI, G. CAPECCHI, A. RINAUDO, *La reimmissione della liquidità illecita nel circuito economico ed il delitto di reimpiego tra prevenzione patrimoniale e giustizia penale: prospettive di future armonizzazioni*, in *Archivio Penale*, 2014, pp. 3 ss.

[19] F. POMES, *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*. in Diritto Penale Contemporaneo, 2-2019, p. 166.

[20] Cfr. G. PALUMBO, *Dal riciclaggio al cyberlaundering*, in Centro Studi Internazionali, consultabile in https://www.cesi-italia.org/articoli/145/dal-riciclaggio-al-cyberlaundering.

zione potrebbe risultare obsoleta a favore piuttosto di una sovrapposizione delle stesse. Ciò è reso maggiormente evidente nel cd. *"riciclaggio digitale integrale"*, considerato *"l'ultima vera frontiera del riciclaggio"*[21], in cui i capitali di provenienza illecita si presentano già *ab origine* allo stato digitale, collocati su *e-wallets*[22], poiché frutto, ad esempio, del prezzo pagato a terzi per l'acquisto di beni intrinsecamente illeciti sul *dark web* ovvero il corrispettivo versato per liberare un sistema informatico da un *ransomware*[23]. In tal caso, dunque, le varie fasi del processo di *recycling* perdono autonoma consistenza, sfumando in un meccanismo unitario e totalmente virtualizzato: se da un lato ciò consente di ridurre, di pari, i rischi connessi a tale attività[24], dall'altro rende tale forma di riciclaggio la più difficile da contrastare, stante l'assenza dei tradizionali istituti finanziari su cui incombe l'obbligo di segnalazione delle operazioni sospette.

3. La rilevanza penale del *cyberlaundering*

La disciplina fenomenologica del *cyberlaundering* solleva alcune riflessioni sulla natura giuridica delle condotte attraverso le quali esso si concretizza e la conseguente necessità di saggiare il grado di compatibilità con le speculari fattispecie incriminatrici previste nella parte speciale del codice penale. L'armamentario giuridico di repressione del fenomeno è infatti rimasto ancorato alle previsioni codicistiche di cui agli artt. *648-bis, 648-ter e 648ter-1* c.p., sebbene, come visto, la tecnologia delle criptovalute abbia notevolmente inciso sulle modalità tecniche di perfezionamento dell'intero ciclo di *recycling.*

La fattibilità di un'ermeneutica operazione di sussunzione delle condotte di riciclaggio tramite criptovalute nella fattispecie prevista

[21] E. Simoncini, *op. cit.*, p. 901.

[22] *E-wallet* o portafogli elettronici sono programmi *software* che archiviano i dati in modo sicuro; questi dati sono necessari per consentire al proprietario del portafoglio di effettuare pagamenti *online* o presso i punti vendita, utilizzando specifici dispositivi. Cfr. Kolandaisamy *[et al] The Impact of E-Wallets for Current Generation,* in *Journal of Advanced Research in Dynamical and Control Systems*, n. 12/2020, p. 751.

[23] M. Croce, *Cyberlaundering e valute virtuali. la lotta al riciclaggio nell'era della distributed economy*, in Sistema Penale, 4, 2021, p. 139. Per un diverso approccio si veda *G.* J. Sicignano*, L'acquisto di bitcoin con denaro di provenienza illecita,* in Archivio Penale, 2, 2020, p.16 nota 59.

[24] J. Alcini, *Mondi paralleli, bitcoin e reati virtuali*, in *La giustizia penale,* 2, 2018, p. 448.

dall'art. *648-bis* c.p. è difatti subordinata alla soddisfazione di tutti gli elementi tipici descritti da quest'ultima: il delitto di riciclaggio richiede che siano realizzate condotte di sostituzione o trasferimento di denaro, beni o altre utilità, ovvero altre operazioni idonee ad ostacolare l'identificazione della loro provenienza delittuosa. Si tratta, quindi, di comprendere se l'acquisto di valute virtuali possa integrare tale condotta. La strada più percorribile appare quella di inquadrare le criptovalute nel concetto di *"altre utilità"* di cui all'art. *648-bis* c.p., stante la possibilità che le stesse possano essere suscettibili di una valutazione economica[25]; si esclude, di contro, che possano essere qualificate come *"denaro",* non avendo le stesse corso legale in alcuno Stato, né possano rientrare nel concetto di *"beni"*, nei quali, secondo dottrina maggioritaria, rientrano le sole *res* tangibili, idonee a essere oggetto di diritti[26]. Ciò premesso, perché possa integrarsi il delitto di riciclaggio occorre che le criptovalute siano oggetto di sostituzione o trasferimento, ovvero che vengano realizzate altre operazioni in grado di ostacolare l'identificazione della loro provenienza delittuosa, tracciando un distinguo per le due tipologie di *cyberlaundering* suesposte.

Di certa compatibilità con la fattispecie *ex art. 648-bis* c.p. sono le condotte rientranti nel cd. *"riciclaggio digitale strumentale"*, laddove i proventi illeciti vengono smaterializzati attraverso transazioni in criptovalute, verificandosi quella "sostituzione" di cui al dato normativo idonea a generare una modifica qualitativa del provento illecito.

Alcuni dubbi sollevano, invece, le condotte rientranti nel cd. *"riciclaggio digitale integrale"*, ove i proventi degli illeciti si presentano già *ab origine* in forma dematerializzata su conti *online*[27]; in tali scenari, bisogna verificare se le operazioni di acquisto e scambio di criptovalute possano rientrare in quelle *"altre operazioni volte ad ostacolare l'identificazione della provenienza delittuosa"*. Ancorare l'analisi alla semplice considerazione che le transazioni via cripto siano intrinsecamente idonee ad ostacolarne l'identificazione delle stesse per il sol fatto di possedere caratteristiche tecniche come pseudo-anonimato e decentralizzazione che 'mascherano' la reale identità del disponente, porterebbe a un'ingiustificata criminalizzazione dell'intero sistema di scambio

[25] F. Pomes, *op. cit*., p. 170.

[26] «Dal punto di vista ontologico le valute virtuali non sono altro che dati informatici difficilmente riconducibili al concetto penalistico di cosa o di bene, senza violare il principio di tassatività e il divieto di analogia», M. Croce, *op. cit*., p. 138, nota 55.

[27] E. Simoncini, *op. cit*., p. 897.

peer-to-peer[28]*:* invero, è proprio la tecnologia *blockchain* che garantisce la piena trasparenza dei blocchi e, quindi, della tracciabilità delle transazioni ivi registrate, costringendo i *cyber* criminali a ricorrere a sistemi di occultamento della catena, come i servizi di *mixing* cui si è accennato[29].

Dottrina maggioritaria[30] accoglie la piena sussumibilità della condotta *de quo* nelle maglie codicistiche di cui all'art. *648-bis* c.p., sfruttando l'elastica clausola di chiusura finale che non richiede alcuna specifica modalità tecnica, né alcun univoco risultato finale della condotta punibile, bastandone l'idoneità ad *"ostacolare"* l'identificazione della provenienza delittuosa dei *"valori ed altre utilità"*[31]. Sebbene in linea con gli intenti legislativi di ricomprendere all'interno di quest'ampia formula l'insieme eterogeneo di condotte derivanti dall'incessante evoluzione delle TIC, tale argomentazione finisce, a parer di chi scrive, per condurre a una pressoché totale elisione del principio di tassatività, dovendosi preferire, in chiave più garantista, un'interpretazione restrittiva, esigendosi sempre la realizzazione di operazioni con "*concreta"* capacità di occultare la provenienza della *res illicita*: di contro, ne conseguirebbe un'evidente lesione del principio di offensività, creando una fattispecie di pericolo astratto[32].

Quanto al delitto di cui all'art. *648-ter* c.p., che punisce l'impiego di denaro, beni o altre utilità di provenienza illecita in attività economiche o finanziarie[33], occorre verificare se nelle suddette tipologie di investimento possano rientrare anche le condotte di pagamento, trasferimento o scambio di valori mediante criptovalute. In tal caso, in accordo con la prevalente dottrina[34], si propende per una soluzione positiva, facendo leva sull'elastica clausola di *"attività economiche e finanziarie"* che, letta in combinato disposto con il concetto di "altre utilità", ove per

[28] Una *rete peer-to-peer* è una particolare architettura di rete distribuita in cui i partecipanti alla stessa condividono tra loro una parte delle proprie risorse *hardware* (potenza di elaborazione, capacità di archiviazione, capacità di collegamento di rete ecc.). Queste risorse condivise sono accessibili direttamente da altri *peer* senza passare attraverso entità intermediarie. In tal modo i partecipanti di tale rete sono contemporaneamente fornitori e usufruitori di risorse. Cfr. P. De Filippi, A. Wrigh, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018.

[29] Per approfondire le metodologie e i protocolli di anonimizzazione si veda in questo Volume A. Paselli, *DarkNet, DarkMarkets e CryptoForensics.*

[30] E. Simoncini, *op. cit*., p. 608., nello stesso senso, L. Picotti*, op. cit*., p. 615 e A. Rosato, op. cit. , p. 81.

[31] L. Picotti, *op. cit*., p. 608.

[32] Cfr. G.J. Sicignano, *op. cit*., pag.10 e ss.

[33] S. Messina, G. Spinnato, *Manuale breve di diritto penale*, Giuffrè, 2020, p. 868.

[34] L. Picotti, *op. cit*., p. 609, A. Rosato, *op. cit.,* p. 81

quanto detto in tema di riciclaggio trovano collocazione le criptovalute, sarebbe idonea a ricomprendere qualsiasi attività di trasferimento o scambio via cripto.

Un'ultima riflessione attiene alla fattispecie di autoriciclaggio ex art. *648-ter.1* c.p., in cui il soggetto attivo coincide (o concorre) con il soggetto agente del reato presupposto. Analogamente a quanto detto in tema di riciclaggio, non vi sarebbero particolari problemi di compatibilità con le condotte di *"(auto)riciclaggio strumentale",* essendo posta in essere dallo stesso autore del reato presupposto la smaterializzazione dei proventi illeciti in *cryptocurrencies*, idonea a dissimulare la provenienza da reato del profitto: in tali casi, infatti, l'attività finanziaria tipizzata nel dato normativo viene a identificarsi con quella del cambiavalute[35]. Più problematica apparare, di contro, la configurazione nella fattispecie *de quo* delle condotte di *"(auto)riciclaggio integrale",* ove il reato presupposto e la successiva attività di riciclaggio si esplicano direttamente in rete: si potrebbe ritenere che, venendo meno qualsiasi attività volta a convertire la valuta virtuale o ad impiegarla in attività speculative, essa non potrebbe ammettersi in quanto non vi sarebbe una *"contaminazione del circuito economico lecito"* [36]. Secondo alcuni[37], invece, anche soltanto la semplice movimentazione degli illeciti virtuali tra i nodi della rete, sarebbe comunque concretamente idonea a dissimularne la provenienza delittuosa, nonostante manchi la destinazione degli impieghi, ciò in ragione del fatto che il bene giuridico tutelato dalla norma non sarebbe la tutela dell'ordine economico, quanto in realtà la *"tracciabilità dei flussi finanziari".* Di certa compatibilità si ritiene, infine, con il concetto di attività speculativa, in ragione dell'ampia volatilità dei prezzi delle criptovalute[38] che le rendono, di fatto, uno strumento versatile di acquisto e di scambio per fini speculativi[39].

[35] Cfr. A. Rosato, *op. cit*., p. 82, nota 289.

[36] *Ibidem.*

[37] L. Sturzo, *Bitcoin e riciclaggio 2.0*, in *Diritto penale contemporaneo*, n. 5/2018, p. 26.

[38] Si pensi al recente e immediato crollo di oltre l'11% del valore del *bitcoin* a seguito della sospensione degli acquisti con tale criptovaluta delle automobili Tesla, avvenuto con un semplice *tweet* del suo fondatore Elon Musk. *Cfr*. M. Valsania, *Elon Musk sconfessa Bitcoin: niente più acquisti di Tesla con la valuta digitale,* in Il Sole 24 Ore del 13 maggio 2021.

[39] *Contra* G.J. Sicignano, *op. cit*., p. 20.

4. Prevenire il *cyberlaundering*: la V Direttiva antiriciclaggio e la responsabilità di *exchangers* e *wallet providers*

L'insita difficoltà di apprestare una risposta sanzionatoria efficace a reprimere il complesso fenomeno del riciclaggio via cripto, reso tale dalle proteiformi e sempre più innovative tecniche di dissimulazione virtuale dei proventi illeciti, impone al legislatore nazionale, ma soprattutto europeo e globale[40], la scelta di giocare d'anticipo, predisponendo apposite normative in materia di antiriciclaggio capaci di incidere significativamente su un fenomeno dalle forti radici internazionali. E proprio in questa direzione si è mosso il legislatore italiano con l'emanazione del D.lgs. 27 maggio 2017, n. 90, mediante il quale, anticipando l'impianto normativo contenuto nella V Direttiva antiriciclaggio[41], ha ridefinito la vecchia disciplina contenuta nel D.lgs. 231/2007 per adeguarla ai nuovi risichi derivanti dalla dimensione virtuale dell'economia[42].

L'intero comparto normativo di prevenzione è infatti fondato sul principio del *risk based approach* e sulla collaborazione attiva fra autorità pubblica e intermediari privati. I soggetti destinatari degli obblighi previsti dal decreto sono cinque: a) intermediari finanziari; b) altri operatori finanziari; c) professionisti; d) prestatori di servizi di gioco; e) altri operatori non finanziari. Su tali soggetti incombe, dunque, l'onere di adeguata verifica della clientela, in guisa da consentire l'individuazione degli indici rivelatori del fenomeno al fine da contrastarlo in via preventiva, nonché gli obblighi di conservazione dell'intera documentazione afferente ciascun cliente e di segnalazione di attività sospette all'Unità di Informazione Finanziaria (UIF)[43].

Il suddetto decreto definiva le valute virtuali come «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di

[40] Ad esempio negli USA la normativa antiriciclaggio *(cd. travel rule)* richiede alle piattaforme di scambio di criptovalute di verificare l'identità dei propri clienti e i beneficiari di transizioni pari o superiori a 3 mila dollari. Cfr. CipherTrace, *Cryptocurrency Anti-Money Laundering Report*, luglio 2019, consultabile all'indirizzo https://ciphertrace.com/wp-content/uploads/2019/08/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q2-1.pdf.

[41] Direttiva n. 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018.

[42] M. Croce, *op. cit.*, p. 132.

[43] Una possibile applicazione dell'Intelligenza Artificiale (IA) nella lotta al riciclaggio può derivare dall'impiego dei *Multi-Agent Systems* (MAS). Si veda il contributo di G. Lasagni, *Policing via Multi-Agent Systems: un nuovo volto per la digital forensics (e non solo)?*

beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente»[44]. Tale definizione è stata poi adottata in sede europea con la V Direttiva antiriciclaggio, venendo a sua volta recepita dal legislatore interno attraverso il D.Lgs. 4 ottobre 2019, n. 125, col quale, all'art. 1, comma 1, lett. h), sono stati inseriti gli incisi *"né garantita"* e *"o per finalità di investimento"*.

Da tale interpolazione normativa si desume come la produzione legislativa interna in materia si sia articolata lungo due direttrici: dapprima, attraverso l'adozione del D.Lgs. 27 maggio 2017, n. 90, e poi, mediante il D.Lgs. 4 ottobre 2019, n. 125.

Quanto al primo, esso non solo ha avuto il pregio di anticipare una definizione di valute virtuali, ma ha inciso, altresì, sui soggetti destinatari degli obblighi antiriciclaggio, estendendone la disciplina anche ai cd. *currency exchangers,* ossia i prestatori dei servizi di cambiavalute, inquadrandoli all'interno della categoria di *"altri operatori non finanziari"*. Su questi ultimi, pertanto, incombono gli obblighi sopra menzionati, con l'aggiunta dell'iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli agenti e dei mediatori creditizi[45]. Sebbene in tal caso il legislatore abbia anticipato i tempi mostrandosi in sede comunitaria come un precursore in materia, lo stesso è apparso tuttavia "timido"[46], non contemplando all'interno della categoria anche la figura dei fornitori dei servizi di portafogli virtuali, soggetti che svolgono il compito di custodire le criptovalute attraverso la salvaguardia delle chiavi crittografiche private. Su questo punto è intervenuto il citato Decreto legislativo del 2019 che, accogliendo l'impostazione fornita dalla V Direttiva, ha ricompreso all'interno della suddetta categoria anche i prestatori dei servizi di portafoglio digitale, includendoli tra i soggetti obbligati alla normativa antiriciclaggio. Questi ultimi sono definiti all'art.1 lettera *ff-bis)* come «ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali»[47].

[44] Art. 1, comma 2, lett. qq) del D. Lgs. 231/2007 così come modificato dall'art.1, comma 1, del D.lgs. 27 maggio 2017, n. 90.

[45] M. Croce, *op. cit.,* p. 131.

[46] M. Naddeo, *Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale*, in Dir. Pen. Proc., 2019, p. 99 ss.

[47] Seconda attenta dottrina tale nozione includerebbe soltanto i *custodian wallet providers* ove la custodia della chiave privata per accedere alle criptovalute contenute nel *wallet* è delegata

Circa le responsabilità degli *exchangers* e *wallet provider,* la loro qualificazione come soggetti sottoposti agli obblighi in materia di antiriciclaggio li rende certamente destinatari anche delle sanzioni penali contemplate all'art. 55 del riformato d.lgs. 231/2007[48]. Inoltre, affinché tali soggetti possano essere chiamati a rispondere del delitto di riciclaggio, occorre che vi sia integrato l'elemento soggettivo richiesto dalla norma incriminatrice. A parere di chi scrive, sfuggendo da una criminalizzazione *tout court* dell'utilizzo di criptovalute, occorre individuare nei suddetti soggetti l'elemento psicologico del dolo tipico, quantomeno nelle forma eventuale, per cui potersi addossare la responsabilità nel aver accettato – concretamente – il rischio di agevolare con la propria condotta l'autore del reato presupposto[49]. Diversamente, tale elemento soggettivo può essere ravvisato in capo ai *mixers*, i quali, svolgendo attività dissimulatoria delle transazioni in valute virtuali con lo scopo di occultarne la tracciabilità, accettano il rischio di agevolare con la loro condotta la realizzazione di pratiche di *cyberlaundering.*

5. L'indagine forense sulle criptovalute: lo stato dell'arte della *Blockchain Forensics*

Si è osservato sin qui come la tecnologia *blockchain* rappresenti il nucleo funzionale della quasi totalità delle criptovalute oggi in circolazione. In sintesi, la *blockchain* è definibile come una sorta di registro condiviso decentralizzato che utilizza blocchi cronologici, crittografati e concatenati per archiviare dati verificabili e sincronizzati (ad es. le transazioni) su una rete *Peer-to-Peer* (P2P)[50].

In sostanza, ogni membro di questa rete, chiamato "nodo", può avviare la creazione di un nuovo blocco di dati, contenente vari tipi di informazioni, il quale viene trasmesso a tutti gli altri nodi della rete in

allo stesso *provider;* di contro, pare escludersi per gli *hardware* e *software wallet,* ove la custodia della chiave privata dello stesso risulta nella disponibilità esclusiva dell'utente, non rivenendosi, pertanto, un servizio di custodia per conto di terzi.

[48] R.M. Vadala', *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale,* in Sistema Penale, maggio 2020. Si veda anche, in questo Volume, A. Paselli, *DarkNet, DarkMarkets e criptovalute: attività investigativa di contrasto.*

[49] M. Croce, *op. cit.,* p. 147.

[50] Y. Maleh, M. Shojafar, M. Alazab, I. Romdhani (a cura), *Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications,* CRC Press, 2020.

forma crittografata; questi ultimi, determinano collettivamente la validità del blocco secondo un metodo di convalida crittografico predefinito, comunemente denominato *meccanismo di consenso,* atto a garantire un corretto sequenziamento delle transazioni sulla *blockchain*. Nel caso delle criptovalute, tale sequenziamento è reso necessario per affrontare la questione della *"doppia spesa"*, vale a dire la possibilità che uno stesso strumento o attività di pagamento possa essere trasferito più di una volta, soprattutto ove i trasferimenti non vengono registrati e controllati da un'autorità centrale. Trattandosi, come detto, di un sistema decentralizzato, tale consenso può strutturarsi in diversi modi: un esempio è la cd. *"proof of work"*, ossia la risoluzione di complessi "puzzle crittografici"[51] cui competono i vari nodi della rete per poter aggiungere il nuovo blocco alla catena, venendo così ricompensati con una certa quantità di criptovaluta[52]. Una volta convalidato, il nuovo blocco viene aggiunto alla *blockchain*, traducendosi essenzialmente in un aggiornamento del 'libro mastro' delle transazioni e dunque distribuito attraverso la rete a tutti i nodi presenti.

La firma digitale apposta sui blocchi delle transazioni avviene utilizzando una chiave privata; ogni utente su una rete *blockchain* possiede, infatti, un *set* di due chiavi: una chiave privata, che viene utilizzata per creare una firma digitale per una transazione, e una chiave pubblica, che è nota a tutti sulla rete e che possiede, sostanzialmente, due funzionalità: 1) funge da indirizzo sulla rete *blockchain*; e 2) viene utilizzata per verificare una firma digitale, e dunque convalidare l'identità del mittente[53].

Esemplificata concettualmente l'infrastruttura e il funzionamento della *blockchain*, appare evidente come, soprattutto in casi ove le criptovalute siano usate per finalità illecite, lo studio e l'analisi della stessa risulti di fondamentale importanza per ricostruire e tracciare

[51] H. NATARAJAN, S. KRAUSE , H. GRADSTEIN, *Distributed Ledger Technology (DLT) and blockchain,* 2017, FinTech note, no. 1, in https://documents1.worldbank.org/curated/en/1779 11513714062215/pdf/122140-WPPUBL IC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.

[52] Tale attività viene comunemente chiamata *"mining"*. In termini sintetici, questi "*puzzle crittografici*" sono costituiti da tutte le informazioni precedentemente registrate sulla *blockchain* e da una nuova serie di transazioni da aggiungere al "blocco" successivo. Poiché *l'input* di ogni puzzle diventa sempre più grande nel tempo, con conseguente calcolo computazionale più complesso, il meccanismo della "prova del lavoro" richiede una grande quantità di risorse di calcolo, che consumano una quantità significativa di elettricità, ben comprendendosi il perché le criptovalute siano definite "energivore".

[53] H. NATARAJAN, S. KRAUSE , H. GRADSTEIN, *op. cit*., pp. 8-9.

eventuali attività sospette. E proprio in tal senso, con il termine *Blockchain Forensics* suole riferirsi al complesso delle attività di *forensics* applicate alla tecnologia *blockchain*, con l'obiettivo di individuare e acquisire potenziali evidenze digitali ivi allocate. Si pensi, ad esempio, agli *artifacts* relativi alle operazioni che coinvolgono le criptovalute[54]: in tal caso, l'attività di *forensics* può esplicarsi nell'analisi delle transazioni e degli indirizzi, nell'esame delle chiavi pubbliche e private, o ancora dei *wallet* e del traffico di rete.

Come osserva Costabile, rispetto agli obiettivi investigativi, il sistema Bitcoin offre il vantaggio duplice che il registro delle transazioni è pubblico ed immutabile e che è possibile svolgere attività di *intelligence* sulle transazioni pubblicate[55].

In letteratura è emerso che la *blockchain* è considerata ancora come una nuova area di studio per la *forensics*, come dimostrano recenti *literature review* sul tema che rifereriscono di soltanto undici documenti di ricerca correlati alla *Blockchain Forensics*[56]. Ciononostante, come ogni attività di *forensic* la prima fase si esplica nell'individuazione degli elementi di potenziale interesse investigativo da cui poter ricavare indizi probatori utili. In questo senso, nel caso delle criptovalute, indubbia rilevanza rivestono i *wallet* ove le stesse sono archiviate: ad esempio, *Bitcoin Core (Bit-Qt)*, uno dei *software wallet* più famosi poiché legato al creatore di *bitcoin,* scarica in locale, sul dispositivo ove è installato, l'intera *blockchain* su cui risiedono tutte le transazioni. Effettuata una copia forense del dispositivo *target*, poiché ad esempio legato ad un soggetto indagato di *cyberlaundering*, è possibile esaminare la cartella "*Bit-Qt"* relativa al predetto *software wallet* che si compone di tre sottocartelle: (1)*".blocks"*, contenente i blocchi *bitcoin* effettivi, in formato di rete, che vengono scaricati sul disco con estensione "*.raw"*; (2) *".database"*, contenente i *file* di sistema del *database*; (3)*"chainstate"*, contenente i metadati su tutti i

[54] Quando oggetto di studio sono le *cryptocurrencies tout-court* si tende a parlare, quasi in accezione sinonimica, di *Crypto forensics*, declinandosi poi, a seconda della criptovaluta oggetto di studio, in *Bitcoin Forensics, Ether Forensics* ecc.

[55] Per approfondimenti G. Costabile, *op. cit*. p. 125 e ss.

[56] M.Z. Mas'ud *et al*, *A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology*, *2021 3rd International Cyber Resilience Conference (CRC)*, 2021, pp. 1-6. Nello specifico, sugli undici *paper*, dieci articoli discutono dell'identificazione delle prove nell'ambiente delle criptovalute, otto articoli discutono sul processo di raccolta e conservazione mentre quattro articoli discutono sul processo di esame e analisi. Nessun documento discute sul processo di presentazione.

blocchi conosciuti e quelli relativi all'origine delle transazioni; altresì, sempre nella cartella *"Bit-Qt"*, sono presenti ulteriori *file* aggiuntivi: "*.lock,",* contenente il *file* di blocco del *database*; *"peers.dat,"* sostanzialmente un archivio per le informazioni sui *peer* per facilitare la riconnessione; *"wallet.dat"*, contenente elementi relativi all'archiviazione delle chiavi, alle transazioni e ai metadati inerenti le operazioni *bitcoin*[57].

L'analisi dei suddetti *artifacts* consente poi di indirizzare l'indagine sulla *blockchain*, le cui transazioni sono pubbliche e immutabili, soprattutto ove si sia riusciti a risalire alla chiave privata del *wallet target*, potendosi utilizzare quest'ultima come parametro per tracciare tutte le transazioni ad essa collegate.

Tra le varie tecniche a tal fine preposte si citano l'attività di *labeling* e quella di *clustering*. La prima consiste nell'etichettatura degli indirizzi *bitcoin* tramite elementi reperibili nel *web* sì da ricondurre all'identità dei possessori: in sostanza, vengono utilizzati congiuntamente un *crawler*, particolare *software* che consente di analizzare il contenuto di una pagina *web* e di quelle ad essa collegate, e un *web scarping* che permette di prelevare singoli dati da un insieme di pagine *web* per raccoglierli all'interno di *database*; in tal modo è possibile ricercare nel *web* determinate stringhe alfanumeriche verificando se le stesse possano corrispondere a potenziali indirizzi *bitcoin*, acquisendone dalla pagina *web* ove sono state individuate, in caso di *matching* positivo, ogni informazione utile per risalire all'identità del possessore. L'attività di *clustering*, invece, consente di estendere l'etichetta a tutti gli indirizzi considerati dello stesso proprietario, così da determinare se quell'indirizzo possa far parte di un *wallet* più ampio[58].

Infine, diversi sono i *tools* appositamente sviluppati per la *Blockchain Forensics*, spaziando da quelli *open source* come *Block Explorer*[59] che consente di navigare nella *blockchain,* visualizzare la cronologia delle transazioni di un determinato indirizzo e lo stato delle transazioni in un blocco, ovvero *BitIodine*[60] che analizza la *blockchain*

[57] M. DORAN, *A Forensic Look at Bitcoin Cryptocurrency*, SANS Institute, 2015, in https://www.sans .org/white-papers/36437/.

[58] S. BISTARELLI, *Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition*, in Network Digital 360, in https://www.agendadigitale.eu/sicurezza/bitcoin-forensics-le-tecniche-labeling-clustering-e-mixnet-recognition/, aprile 2018.

[59] https://blockexplorer.com.

[60] M. SPANGUOLO, F. MAGGI, S. ZANERO. *BitIodine: Extracting Intelligence from the Bitcoin Network,* in Christin N., Safavi, R. Naini. (eds) *Financial Cryptography and Data Security*, FC 2014, Lecture notes in Computer Science, vol. 84347, Berlin, Springer, marzo 2014.

e fornisce un *front-end* su cui approfondire una varietà di informazioni come il saldo del conto di un dato indirizzo, il numero totale di transazioni e informazioni più avanzate come il raggruppamento e l'etichettatura degli indirizzi utilizzando le risorse pubbliche raccolte in *Internet*, fino a quelli di natura commerciale, come *Elliptic*[61], che, in aggiunta alle *utilities* anzidette, offrono anche un *database* proprietario contenente milioni di indirizzi di transazioni via cripto collegati ad attori del mondo reale.

Sul piano tecnico operativo[62], individuato l'indirizzo Bitcoin dell'indagato, procedere al sequestro implica un certa complessità anche operativa perché non è possibile sequestrare il Bitocoin da remoto ma occorre individuare: il *wallet bitcoin* sul disco rigido dell'indagato (e ciò presuppone siano note credenziali di accesso e *password* di decrittazione) la chiava privata e il seme. Per perfezionare il sequestro, a fronte anche del rischio che gli stessi indagati in possesso della chiave privata possano spostare i fondi su un altro conto, è necessario realizzare un contestuale trasferimento dei fondi verso un nuovo portafoglio *bitcoin* controllato dalle forze dell'ordine che potrà essere materializzato sotto forma di *paper* o *hardware wallet* e sequestrato al pari di ogni altra *res* pertinente al reato. Si registra come non sia possibile ad oggi fare confulire nel Fondo Unico di Giustizia le somme di bitcoin che risultino prezzo, prodotto o profitto della condotta criminosa.

6. Conclusioni

Quale che sia il futuro che si prospetta all'orizzonte delle criptovalute, ciò che certamente rileva è la dirompente capacità delle stesse di aver dato avvio a un mutamento irreversibile del substrato economico e finanziario dell'odierna società, segnando con la dematerializzazione del contante il ritorno al cittadino della sovranità monetaria; viene così attuato quell'ideale di uguaglianza economica e sociale nel quale ciascuno riveste un ruolo fondamentale nell'intero ecosistema finanziario virtualizzato, la cui fiducia viene riposta nel consenso generato da un *network* decentralizzato di persone (i cd. "nodi") che la tecnologia *blockchain* ha saputo implementare, mettendo in crisi e in discussione

[61] https://www.elliptic.com.
[62] Sul punto, C. FEDERICI, *op. cit.,* p. 362.

gli attuali *asset* istituzionali su cui si regge e si struttura il complesso apparato della politica economica nazionale e globale.

Sebbene possa concordarsi, comprensibilmente, sulle potenzialità criminogene delle criptovalute, non bisogna tuttavia cadere nell'errore di ritenerle uno strumento economico dedito unicamente a tal fine: affermare che quest'ultime servano esclusivamente per attività speculative e di riciclaggio[63] in ragione della loro volatilità, opacità e assenza di regolamentazione, sottintende una mancata conoscenza della tecnologia alla base del funzionamento delle stesse: in quanto totalmente pubblica ed accessibile a chiunque, proprio la *blockchain* garantirebbe la possibilità di verificare tutte le transazioni effettuate dagli utenti di quella determinata criptomoneta, senza che le stesse possano andar perse o addirittura alterate e manipolate.

Soltanto l'1% delle transazioni via cripto si sostanza, infatti, in attività illegali[64], derivandone che la vera sfida concerne quelle specifiche attività dirette ad occultare il *paper trail*, e dunque la tracciabilità delle transazioni sul registro, come gli appositi servizi di *mixing* o l'utilizzo di strumenti di navigazione anonima come *Tor*; solo in tal caso, la "concreta" attività tesa al riciclaggio dell'illecito provento sarebbe suscettibile di integrare la fattispecie penale, evitandosi, di contro, un'ingiustificata criminalizzazione dell'intero sistema di scambio *peer-to-peer*.

Ebbene, nell'esigenza di perseguire la punibilità delle condotte di *cyberlaundering* che si sostanziano mediante simili artifici, dando vita a zone franche virtuali ove possa proliferare il *cybercrime*, un ruolo cruciale riveste la *Blockchain Forensics,* capace di rispondere alle sfide derivanti dell'incessante contaminazione delle innovazioni tecnologiche e digitali nelle quotidiane attività sociali e finanziarie, attraverso la predisposizione di tecniche d'indagine forense in costante evoluzione e *suites* di strumenti sempre più performanti.

[63] Si fa riferimento, tra i tanti interventi in questo senso, alle recenti parole della Presidente della BCE Christine Lagarde sui *bitcoin*, nello specifico F. Goria, *Lagarde va all'attacco di Bitcoin*, in La Stampa, del 13 gennaio 2021, consultabile all'indirizzo *https://www.lastampa.it/eco nomia/2021/01/13/news/lagarde-va-all-attacco-di-bitcoin-1.39769252.*

[64] Nel 2017 le transazioni illecite via cripto rappresentavano soltanto lo 0,7 % del totale, nel 2018 lo 0,5 %, nel 2019 il 2% e nel 2020 l'1%. Dati estrapolati dal report di Chainalisys *The 2021 Crypto Crime Report* del febbraio.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643011
pp. 207-226 (gennaio 2022)

DarkNet, DarkMarkets e criptovalute: attività investigativa di contrasto

ANDREA PASELLI[1]

1. Introduzione

I mercati illeciti online hanno ormai una lunga storia, infatti la prima transazione illecita online di cui si ha notizia risulta essere avvenuta nel 1972, si trattava di una piccola quantità di cannabis scambiata tra alcuni studenti del Massachusetts Institute of Technology ed altri studenti dell'Università di Stanford utilizzando i rispettivi account ARPANET[2].

Da allora passando per forum e messaggi attraverso le storiche reti BBS (Bulletin Board System) la tecnologia ha fatto enormi progressi.

L'avvento di Internet, di nuovi protocolli di comunicazione sempre più veloci ed efficienti unitamente allo sviluppo di nuove reti e metodologie di navigazione anonima quali ad esempio la rete TOR (The Onion Ring), unitamente alla creazione e l'utilizzo di mezzi di pagamento anonimi come le criptovalute hanno radicalmente trasformato la vendita anche al dettaglio di beni e prodotti di natura illecita. La vasta gamma di opportunità di comunicazione e commercio resa possibile dalla rete geografica Internet ha alimentato l'imprenditorialità e contribuito a costruire comunità completamente nuove con forme di interazione che erano impossibili da immaginare solo due decenni fa, queste nuove opportunità non sono sfuggite alle principali organizzazioni criminali ed ai malintenzionati più abili nell'utilizzo di queste nuove tecnologie. Tra queste opportunità vi è quella di nascondere l'origine delle comunicazioni, mediante l'instradamento del proprio traffico di rete su numerosi nodi offuscando

[1] Dottore di ricerca in Diritto e nuove tecnologie - Università di Bologna; Vice Ispettore della Polizia di Stato. Per più di 20 anni in forza alla Polizia Postale dove ha svolto complesse e articolate indagini informatiche; dal 2016 al 2020 Esperto Nazionale Distaccato in Payment Fraud presso Europol EC3.

[2] J. BARTLETT, *The dark net: Inside the digital underworld.* Random House, 2014.

così la posizione geografica da cui proviene il traffico, e la possibilità di mantenere il quasi assoluto anonimato nei pagamenti, utilizzando una delle numerose criptovalute disponibili.

L'ambiente sul world wide web in cui avviene tale comunicazione anonima è comunemente indicato come "DarkNet". La rete Darknet, pertanto, può essere definita come un "gruppo di reti e tecnologie utilizzate per la *condivisione di contenuti digitali*". Si tratta di un ambiente nascosto al generico utente della rete, nel senso che non è accessibile attraverso normali motori di ricerca come Google o Yahoo ed altri, il cui accesso è veicolato dall'utilizzo di specifici software di navigazione, quali ad esempio il citato TOR *browser*, talvolta per accedervi è inoltre necessario ricevere un invito, consistente nella ricezione di uno specifico collegamento, *link*. Poiché l'anonimato è una caratteristica di grande attrattiva per i criminali, non sorprende affatto come negli ultimi anni numerosi mercati illeciti siano fioriti sulla Darknet.

Il termine Darknet è stato usato per la prima volta nel 2002, nel documento di ricerca di Microsoft "The *Darknet and the Future of Content Distribution*"[3].

Indubbiamente oggi questo è un tema di grande attualità all'interno dei media mainstream, soprattutto a causa di numerose azioni di contrasto poste in atto con successo dalle Forze dell'Ordine che hanno portato al sequestro e alla chiusura di famigerati servizi ospitati sulla Darknet, come ad esempio lo smantellamento nell'ottobre del 2013 del primo e principale mercato illegale on-line chiamato *Silk Road*, noto per offrire accesso a droghe e armi, avere più di 100.000 clienti e un fatturato di 1 miliardo di dollari[4].

In conseguenza della sua natura dinamica, non è affatto semplice comprendere le dimensioni della Darknet, tuttavia alcune recenti ricerche rivelano che le dimensioni stimate del Deep Web siano addirittura 4.000-5.000 volte superiori a quelle del Surface Web[5].

Attualmente si stima l'esistenza di circa 30.000 *hidden services* e circa 55.000 indirizzi attivi ". onion", tuttavia, solo circa 8.500 di questi

[3] M. PEINADO e W. BRYAN, *The Darknet and the Future of Content Distribution*, Workshop ACM sulla gestione dei diritti digitali. Washington, DC: Microsoft Corporation. Vol. 48. 2002.

[4] Il procuratore degli Stati Uniti di Manhattan annuncia il sequestro di ulteriori $ 28 milioni di Bitcoin appartenenti a Ross William Ulbricht, Proprietario e gestore di Silk Road https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website.

[5] K. FINKLEA, *Dark Web. Servizio di ricerca del Congresso*, 2015).

risultano effettivamente attivi. Questi numeri possono anche variare in modo significativo rispetto ai diversi metodi utilizzati per il conteggio e l'analisi dei servizi nascosti. Ad esempio, secondo il documento di ricerca "*Cryptopolitik* and the *Darknet*"[6], gli autori sono riusciti a identificare 5.205 servizi nascosti attivi e ha concluso che la stragrande maggioranza dei siti web presenti servizi nascosti di TOR sono illegali e legati alla criminalità, commercializzando servizi e beni assolutamente illeciti, quali droghe e stupefacenti di ogni tipo, armi, carte di credito e account di servizi finanziari contraffatti e pornografia infantile. Data la loro natura è ragionevole pertanto aspettarsi che la vita media di tali servizi sia molto più breve rispetto ai normali servizi ospitati su Surface Web, essendo costantemente presi di mira da Europol, e dalla maggior parte degli uffici investigativi delle Forze dell'Ordine (*LEAs, Law Enforcement Agencies*) come il Servizio Polizia Postale e delle Comunicazioni, reparto investigativo della Polizia di Stato italiana specializzato in indagini ad alta tecnologia, quotidianamente impegnati a ricercare e de-anonimizzare tali servizi con l'obiettivo finale di renderli inaccessibili.

Anche nei casi in cui detti servizi non vengano "chiusi" dalle Forze dell'Ordine, il rischio di essere esposti come operatore è sempre sostanziale, comportando un procedimento penale che potrebbe portare alla condanna ad una lunga detenzione.

In conseguenza di questi rischi, i gestori e gli operatori dei *DarkMarket* tendono ad essere molto attenti e tali mercati illegali tendono a scomparire al primo sospetto di essere stati compromessi nella loro sicurezza. Un'altra ragione per cui i servizi nascosti, in particolare i *DarkMarket*, tendono ad avere una vita breve è la sostanziale possibilità di essere truffati. Vi sono situazioni in cui i gestori di tali mercati illegali decidono autonomamente di chiudere il loro mercato presente nella Darknet nel momento in cui ritengono che siano state accumulate sufficienti attività finanziarie, normalmente criptovalute di varia natura, sui loro conti di deposito a garanzia. In questi casi, i clienti sono vittime di una truffa, perdendo i loro soldi senza ottenere il servizio o il prodotto acquistato, e senza ovviamente alcun mezzo di tutela legale. Si tratta dei cosiddetti "*SCAM DarkMarket*", cioè tentativi di truffa online pianificata con metodi di ingegneria sociale.

[6] D. Moore e T. Rid, *Cryptopolitik and the Darknet*. Survival 58.1, 2016.

2. Dark Web Marketplaces

Un *Dark Web Marketplace* (DWM) è una piattaforma di commercio anonima e non geolocalizzata che, come precedentemente descritto, si appoggia su un *hidden service* presente nella Darknet; queste piattaforme di e-commerce propongono una vasta gamma di beni e servizi per la stragrande maggioranza di natura illecita con una predominanza di sostanze stupefacenti di ogni genere.

Ogni mercato ha proprie regole ed i *Dark Web Marketplaces* non fanno eccezione, detto che molti di essi risultano accessibili solo utilizzando software/servizi di anonimizzazione come il già menzionato TOR o I2P, l'accesso a queste comunità non è sempre facile. Non è raro, infatti, che l'utente interessato ad accedervi debba passare attraverso diversi passaggi di verifica, talvolta l'accesso è consentito solamente attraverso un invito, questo per garantire che *bot* ed estranei indesiderati non ottengano l'accesso. D'altra parte, i venditori più apprezzati vengono spesso premiati con recensioni e riscontri (*feedback*) positivi, del resto come in qualsiasi altro mercato anche nei DWMs la reputazione del venditore è importante, analogamente anche le recensioni negative sono dannose per gli affari essere indicati come truffatori o venditori inaffidabili può comportare un grave danno nella reputazione e conseguentemente negli affari.

Negli ultimi anni a seguito dei numerosi successi investigativi, è stato riscontrato un alto livello di volatilità dei DWMs, infatti, il ciclo di vita dei *Dark Web Market* si è notevolmente ridotto rispetto agli anni precedenti, e non si intravvede più una chiara posizione dominante di una piattaforma rispetto ad un'altra come accadeva in precedenza.

Infatti, dopo i "*take down"* di Hansa Market e Wall Street Market nel 2019 e quello più recente di DarkMarket nel febbraio 2021, nessun altro DWM pare aver attualmente occupato le posizioni rimaste vacanti.

Come risposta, recentemente si è osservato uno sviluppo dell'adattabilità della comunità Dark Web nella ricerca delle migliori soluzioni di sicurezza, oltre ad un notevole incremento dell'utilizzo di *wallet privacy enhanced* come "Wasabi" e "Samurai"[7].

[7] IOCTA 2020 – Internet Organized Crime Threat Assessment.

Come precedentemente descritto, i DWMs operano online, ma all'esterno della normale rete *web*, in una area criptata e non indicizzata dai normali motori di ricerca. Silk Road Marketplace, lanciato nel 2011, può essere considerato come il primo DWM moderno, che proponeva una nuova modalità di commercio di droghe e stupefacenti di ogni tipo, armi, e molti altri beni illegali in maniera completamente anonima, replicando la semplicità d'uso dei moderni siti di *e-commerce*.

A parere dello scrivente i due principali fattori di successo in Silk Road Market erano legati alla impossibilità di essere tracciati e la possibilità di effettuare acquisti utilizzando criptovalute che garantivano a venditori e acquirenti un ulteriore garanzia di anonimità.

Successivamente al "*take down*" di Silk Road, avvenuto nel 2013 ad opera dell'F.B.I. (Federal Bureau of Investigation), nuovi DWMs non tardarono ad apparire per occupare lo spazio di mercato lasciato da Silk Road e continuare ad offrire gli stessi prodotti e servizi illeciti, adeguandosi tuttavia ad un superiore livello di sicurezza e *privacy*, quale ad esempio la possibilità di accesso anche mediante la rete I2P e l'implementazione di servizi di garanzia di tipo *escrow* offerti dalla piattaforma di *trading* nei confronti di acquirenti e venditori.

In tempi più recenti, nuove implementazioni tecnologiche, quali la possibilità di accedere a TOR anche mediante l'utilizzo di App su Smart Phone ha reso ancora più semplice ed immediato l'accesso ai moderni DWMs, dove Bitcoin ed Ethereum rimangono tutt'oggi le criptovalute più utilizzate con movimenti di denaro nell'ordine di centinaia di milioni di dollari ogni anno.

Nonostante il breve ciclo di vita medio dei vari DWMs, negli anni, questi ultimi hanno dimostrato una forte resilienza ai continui attacchi perpetrati da Hackers, spesso finanziati da DWMs concorrenti, (attacchi DDoS, tentativi di hackeraggio, ecc.) e all'incessante attività investigativa posta in essere dalle Forze dell'Ordine. Allorquando un DWM veniva chiuso, si è osservato che i maggiori venditori, soprattutto quelli più abili a crearsi una certa notorietà e reputazione nell'ambiente Darknet, rapidamente migravano verso altri DWMs esistenti oppure ne creavano dei nuovi. Detta resilienza ha trovato nel tempo un forte supporto anche grazie ai numerosi siti web e forums dove gli utenti scambiano esperienze ed opinioni, a titolo di esempio potremmo citare *Dread* un forum creato nel 2018 dopo la censura delle pagine sulla piattaforma *Reddit*.

Inoltre, altre piattaforme monitorano costantemente i DWMs attivi e quelli *offline*, verificando la genuinità dei feedback e delle referenze riportate nei vari DWMs. Talvolta gli amministratori di alcuni DWMs, dimostrando una etica del tutto personale, agiscono come moderatori, eliminando venditori o specifiche categorie di prodotti o servizi offerti ritenute particolarmente illecite e sgradevoli. Come accaduto su *DarkBay* dove furono eliminate offerte commerciali inerenti al traffico di esseri umani o l'ingaggio di sicari, oppure sul *Monopoly Marketplace* dove vaccini Anti COVID-19 contraffatti sono stati recentemente eliminati dalla lista dei beni offerti dai moderatori.

Come detto, negli ultimi tempi si è osservata la diminuzione dei mercati di maggiori dimensioni, come DarkMarket chiuso dalla polizia tedesca in collaborazione con Europol, NCA (National Crime Agency – UK) ed FBI nel gennaio 2021, questo *trend* ha portato ad un aumento dei DWMs di dimensioni più ridotte, in alcuni casi rivolti a utenti o esigenze specifiche, il tutto agevolato dalla possibilità di realizzare e gestire nuovi DWMs basati su *tools* e *script* acquistati, cioè senza la necessità di disporre di particolari conoscenze informatiche, tuttavia la maggior parte di questi piccoli DWMs sono scomparsi rapidamente a causa di hackeraggi o truffe perpetrate dai gestori in danno agli utenti (c.d. Scam). Pochi altri, invece, sopravvissuti alle schermaglie iniziali, sono attualmente in crescita e, man mano che ottengono riscontri positivi dagli utenti stanno crescendo nel numero di utenti e venditori, diventando sempre più consolidati.

Come precedentemente argomentato, gli utenti della Darknet monitorano con attenzione le valutazioni fornite dagli altri utenti e tendono a mantenersi all'interno dei mercati ritenuti più stabili e ad acquistare dai fornitori con valutazioni elevate. A questo proposito occorre evidenziare, come la comunità della Darknet si sia impegnata nel trovare nuovi modi per creare fiducia nei propri utenti, sviluppando l'affidabilità delle proprie procedure. Il nuovo sito web *DarkNet Trust* che verifica la reputazione dei fornitori effettuando una ricerca tramite nomi utente e impronte digitali PGP ed è in grado di cercare oltre diecimila profili dai marketplace, né è un fulgido esempio.

Dopo la rimozione di *DeepDotWeb*, un popolare servizio di informazioni che agevolava la navigazione degli utenti nell'ecosistema Darknet, nel maggio del 2019 da parte di Europol, di F.B.I. e della britannica N.C.A. (National Crime Agency), la centralizzazione delle informazioni sui mercati Darknet è addirittura aumentata.

Per ovviare a tale mancanza si sono via via implementati nuovi *hub* di informazioni, recentemente siti web come "dark.fail" e "darknetlive.com" hanno assunto il ruolo svolto in precedenza dal portale "DeepDotWeb".
Il già menzionato *Dread*, un popolare forum, continua a funzionare e a fornire informazioni agli utenti della Darknet da tre anni. Gli amministratori di Dread hanno inoltre implementato e reso disponibile a partire da marzo 2020 un motore di ricerca specifico per la Darknet, denominato "*Recon"*, un servizio che consente agli utenti di vedere che tipo di sostanze stupefacenti sono in vendita nella Darknet in un dato momento, quali venditori sono disponibili e quali valutazioni hanno.

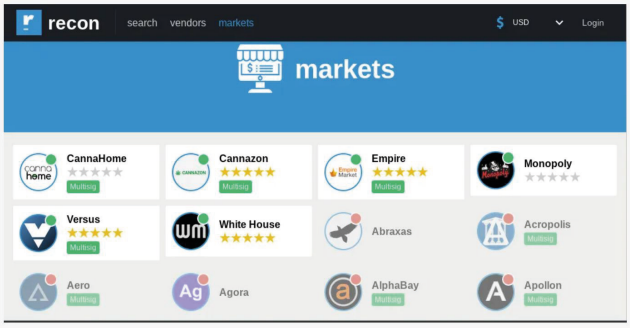


Figura 1. Recon, pratico ed intuitivo motore di ricerca dedicato al Dark Web.

Un altro esempio di motore di ricerca dedicato alla Darknet è *Kilos*, disponibile da novembre 2019, e realizzato sulle ceneri di *Grams*, un importante motore di ricerca Darknet che ha cessato le proprie funzionalità nel 2017. Il nuovo motore di ricerca *Kilos* ha provveduto ad indicizzare più piattaforme e aggiungere nuove funzionalità di ricerca rispetto al suo predecessore, mirate a garantire maggiore sicurezza e anonimato per i suoi utenti.

Anche se i Dark Web Markets continuano ad apparire e scomparire, negli ultimi mesi sono emersi un numero crescente di mercati operativamente sempre più sicuri, tra i quali nuovi DWMs "senza portafoglio" e "senza utenti". Inoltre, è apparsa la tendenza, di sviluppare anche nuovi DWMs con cicli di vita intenzionalmente brevi, con lo scopo di rendere ancora più difficoltose le indagini delle Forze dell'Ordine, che possono così contare su un minore arco temporale per sviluppare le loro attività investigative. Si conferma così la tendenza da parte dei gestori

dei DWM di voler rimanere al di sotto del radar delle forze dell'ordine chiudendo rapidamente i market sotto i riflettori degli investigatori e riducendone significativamente il ciclo di vita.

Tutte queste nuove caratteristiche hanno reso i moderni Dark Web Markets sempre più appetibili e remunerativi agli occhi delle organizzazioni criminali, che, limitando grandemente i rischi tipici di analoghi traffici online, riescono a raggiungere un numero elevato di utenti. In questo contesto altamente volatile e variabile, in conseguenza di tutte le ragioni esposte, è difficile fornire una indicazione esatta di quanti DWMs siano attualmente online, qualche recente ricerca indipendente ha stimato l'esistenza di circa 20 Dark Web Markets, tra i quali Hydra e White House marketplaces.

3. Cryptocurrencies e blockchain

3.1. *Introduzione*

Stabilire una definizione di criptovalute non è un compito facile, esistono numerose definizioni, tuttavia per quanto riguarda l'Italia, una definizione di criptovaluta ci è attualmente offerta dalla normativa antiriciclaggio (V direttiva), che descrive la criptovaluta come una «rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente». Le criptovalute come i Bitcoin sono protette tramite tecniche crittografia utilizzando un ingegnoso sistema di chiavi digitali pubbliche e private[8]. La prima parola che viene associata alla tematica criptovalute è, senza dubbio alcuno, Bitcoin, possiamo pertanto definire il 31 ottobre 2008 come una data fondamentale nella storia delle criptovalute: il sedicente Satoshi Nakamoto scrive il celebre *White Paper* dal titolo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" [9].

[8] J. FAULKNER, Getting started with Cryptography in .NET, München BookRix, 2016.

[9] Il White Paper verrà diffuso da Nakamoto a novembre dello stesso anno tramite diverse mail list crittografiche.

La sua idea è chiara: proporre una versione puramente *peer-to-peer* di denaro elettronico che permetta di effettuare pagamenti *online* senza l'intervento di una istituzione finanziaria. In questo paper risulta particolarmente evidente l'influenza di Wei Dai, ingegnere informatico che dieci anni prima di Nakamoto aveva ideato "b-money"; lo stesso Satoshi non ne fa mistero e difatti il primo riferimento bibliografico del *White Paper* Bitcoin è proprio al *Paper* di b-money, pubblicato nel 1998. L'idea alla base del Bitcoin è quella di una valuta elettronica gestita su una catena di blocchi in cui "scrivere" transazioni, cioè il passaggio di un certo numero di Bitcoin da un proprietario ad un altro.

Il problema di eliminare un'autorità fiduciaria centrale è principalmente quello del c.d. *double-spending* e dunque nasce la necessità di un protocollo che assicuri al beneficiario che il proprietario precedente non abbia già speso la stessa moneta.
Il primo blocco di questa catena, noto come "*Genesis Block*", è stato creato il 3 gennaio 2009 alle ore 18:18. Il suo valore *hash* è noto a tutti i partecipanti della rete come un punto di partenza, una *secure root* per tutti i successivi.

3.2. La *Blockchain*

Quanto precedentemente descritto permette la formazione di una lunga catena del consenso in cui sono riportate in maniera irreversibile tutte le transazioni. I blocchi sono validati ed aggiunti sequenzialmente, secondo la scelta indicata dal sedicente Nakamoto nel suo Paper: il sistema prevede che venga inserito mediamente un blocco ogni dieci minuti. Questo limite pone sicuramente delle difficoltà nell'utilizzo della valuta come metodo di pagamento per l'assenza di immediatezza e sarà un tema ampiamente discusso in seguito.

La Blockchain è quindi un insieme di tecnologie, in cui il registro è strutturato come una catena di blocchi immutabili contenenti le transazioni e il consenso, distribuito su tutti i nodi della rete. Tutti i nodi possono partecipare al processo di validazione delle transazioni da includere nel registro. Sebbene la sua dimensione sia destinata a crescere nel tempo, è immutabile in quanto, di norma, il suo contenuto una volta scritto non è più né modificabile né eliminabile, a meno di non invalidare l'intera struttura. Tali tecnologie sono incluse nella più ampia famiglia dei "*Distributed Ledger*", ossia sistemi che si basano su un registro distribuito, che può essere letto e modificato da più nodi di una rete.

Non è richiesto che i nodi coinvolti conoscano l'identità reciproca o si fidino l'uno dell'altro. Difatti, per garantire la coerenza tra le varie copie, l'aggiunta di un nuovo blocco è globalmente regolata da un protocollo condiviso. Una volta autorizzata l'aggiunta del nuovo blocco, ogni nodo aggiorna la propria copia privata: la natura stessa della struttura dati garantisce l'assenza di una sua manipolazione futura.

Le caratteristiche che accomunano i sistemi sviluppati con le tecnologie Blockchain e "*Distributed Ledger*" sono digitalizzazione dei dati, decentralizzazione, disintermediazione, tracciabilità dei trasferimenti, trasparenza/verificabilità, immutabilità del registro e programmabilità dei trasferimenti[10].

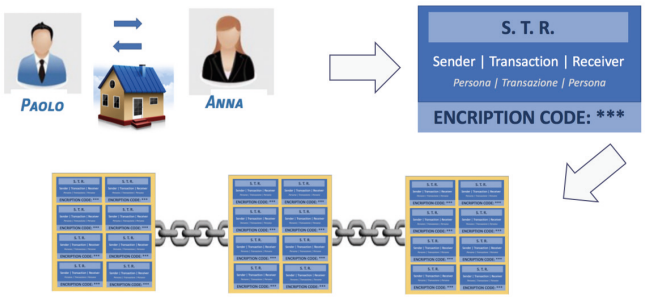


Figura 2. Partendo dalla singola Transazione, la stessa viene raggruppata in un insieme di altre transazioni che formano il "Blocco", l'unione di più "Blocchi" formano la Blockchain.

Per poter spiegare il funzionamento dei "*Distributed Ledger*" di tipo *blockchain*, può essere utile ricordare come operano i *Ledger* tradizionali, ovvero i "Libri Mastro". Imprese, banche e Pubbliche Amministrazioni hanno da sempre utilizzato dei registri (*Ledger*) per gestire la contabilità delle transazioni o delle proprietà immobiliari. Ogni volta che avveniva una transazione, si procedeva a una modifica dei registri attraverso un'autorità centrale deputata appunto alla gestione del Registro Centrale. La base di questo funzionamento è tutta racchiusa nella fiducia che tutti devono avere nel gestore del Registro Centrale (*Central Ledger*). La grande rivoluzione che la tecnologia Blockchain ha permesso è quella di garantire la stessa funzionalità nella gestione dei *Ledger*, ma senza dover fare riferimento a una struttura centralizzata, senza cioè che sia necessario che una autorità centrale verifichi, controlli e

[10] *Blockchain Technology and Smart Contracts: Discussion on Draft Principles*, ELI, 2021.

autorizzi la legittimità di una transazione, di uno scambio, di un passaggio. Se prima il Libro Mastro era univoco, uno solo e stava in capo all'autorità centrale, adesso il Libro Mastro è di tutti, ovvero tutti gli utenti ne hanno una copia e tutti possono controllarlo, visionarlo e, a fronte di regole che vanno a comporre la Governance della blockchain, possono modificarlo. Pertanto, grazie alla *blockchain*, ogni nuova transazione da registrare viene unita ad altre nuove transazioni e va a formare un "blocco", che viene aggiunto come anello di una lunga "catena" di transazioni cronologiche. Ogni volta che si genera un blocco si allunga la catena. Questa catena va a comporre il grande Libro Mastro *blockchain* che è posseduto da tutti gli utenti. La *blockchain* è stata riconosciuta per la prima volta all'interno dell'ordinamento giuridico italiano con la legge nr. 12 dell'11 febbraio 2019, nella quale è stato altresì riconosciuto il valore legale di ogni informazione registrata su di essa.

3.3. Le *Criptovalute*

Il termine "criptovaluta" o "criptomoneta"[11] è un neologismo derivato del termine inglese "*cryptocurrency*" e si riferisce ad una rappresentazione digitale di valore basata sulla crittografia. Le criptovalute utilizzano tecnologie di tipo peer-to-peer (p2p) su reti i cui nodi risultano costituiti da computer di utenti, situati in tutto il globo. Su questi computer vengono eseguiti appositi programmi che svolgono funzioni di portamonete. Come descritto nel paragrafo precedente, non esiste attualmente alcuna autorità centrale che le controlla. Grazie alla descritta tecnologia blockchain a registro diffuso, le transazioni ed il rilascio avvengono collettivamente in rete. Il controllo decentralizzato di ciascuna criptovaluta funziona attraverso una tecnologia di contabilità generalizzata (DLT), che funge da database di transazioni finanziarie pubbliche.

Dopo l'introduzione del già citato Bitcoin nel 2009, numerose sono state le criptovalute create, subito battezzate come "altcoin" (*alternative coin*) ovvero monete alternative al Bitcoin, che si differenziano per alcuni aspetti ed utilizzano un differente sistema blockchain.

[11]Criptovaluta, Criptomoneta, in Treccani.it – Vocabolario Treccani on line, Neologismi, Istituto dell'Enciclopedia Italiana, (2018).

Si stima esistano oggi circa 7.000 criptovalute[12], tra le quali le principali sono le seguenti:

- Bitcoin (BTC o XBT)
- Bitcoin Cash (BCH)
- Ethereum (ETH)
- Tether (USDT)
- Cardano (ADA)
- Litecoin (LTC)
- Monero (XMR)
- Ripple (XRP)

Analogamente a quanto descritto nel paragrafo precedente a proposito dei Dark Web Marketplaces, negli ultimi anni sono nate moltissime nuove criptovalute, alcune sviluppatesi con successo, altre miseramente scomparse nel giro di pochi giorni. Al momento tra le circa 7.000 criptovalute esistenti, sono state definite oltre trenta diverse specifiche e protocolli perlopiù simili o derivati dal Bitcoin, tutte le c.d. "Altcoin" [13] (Alternative Coin, cioè criptovalute alternative ai Bitcoin) offrono differenti caratteristiche e funzionalità rispetto a quest'ultima.

Litecoin (LTC), considerata da tutti come la prima *altcoin*, lanciata il 7 ottobre 2011, dall'ex programmatore di Google, Charlie Lee. Caratteristica peculiare di Litecoin è quella di superare la lentezza del Bitcoin come metodo di pagamento; infatti, come detto, quest'ultimo genera blocchi ogni 10 minuti e per la possibile presenza di biforcazioni occorre attendere altri 5/6 blocchi per essere certi che la transazione sia stata approvata. Litecoin invece permette una maggiore velocità in quanto ogni blocco viene generato ogni 2,5 minuti circa, inoltre ogni blocco genera un numero più elevato di transazioni rendendolo più idoneo per gli acquisti più frequenti.

Ethereum (ETH), creato nel 2013 dal diciannovenne programmatore di origini russe Vitalik Buterin, già impegnato attivamente nel mondo Bitcoin, il cui scopo era quello di modificarne il protocollo per renderlo più flessibile e adatto a differenti applicazioni.

[12] CoinMarketCap, su coinmarketcap.com.

[13] P. Ciaian, M. Rajcaniova,K. d'Artis, *Virtual relationships: Short and long run evidence from BitCoin and altcoin markets*, ScienceDirect, 2018.
https://www.sciencedirect.com/science/article/pii/S1042443117302858.

Ripple (XRP), anche in questo caso l'idea che ha portato alla creazione di questa criptovaluta era quella di rendere più veloce l'operatività, permettendo un tempo massimo di cinque secondi per l'approvazione della transazione. Questo anche grazie al fatto che non viene eseguito "*mining*" di valuta per Ripple per coniarne nuova, in quanto tutta la quantità di criptovaluta prevista, pari a 100 miliardi, è già stata coniata, e viene immessa nel mercato nella misura di 1 miliardo di Ripple al mese, e dunque non è ancora totalmente in circolazione.

Monero (XMR) [14], è una criptovaluta creata nell'aprile 2014 che si focalizza sulla privacy, la decentralizzazione, la scalabilità e sulla fungibilità. Il suo primo nome è stato BitMonero per poi divenire semplicemente Monero che in esperanto significa moneta.

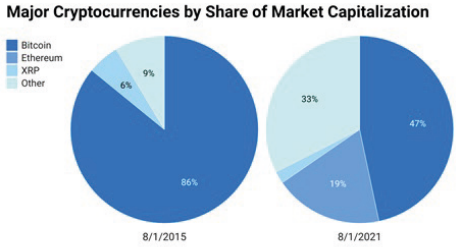


Figura 3. Principali Criptovalute per capitalizzazione.Fonte: CoinMarketCap.

4. Cryptoforensics

Tutti i vantaggi offerti dalle moderne criptovalute – consentire transazioni più facili e veloci con commissioni ridotte o nulle, l'anonimità offerta dalla crittografia – le hanno rese molto popolari anche alle organizzazioni criminali di ogni tipo e livello.

Questi moderni mezzi di pagamento, non regolamentati, e che garantiscono un alto livello di anonimato, spesso consentono di aggirare più facilmente i limiti normativi ed evitare di essere rilevati dalle autorità. Un recente rapporto della società Chainalysis ha rilevato che le transazioni illecite effettuate con criptovalute nel 2020 hanno

[14] S. Aggarwal, N. Kumar, *Monero. The Blockchain Technology for Secure and Smart Applications across Industry Verticals*, ScienceDirect, 2021.
https://www.sciencedirect.com/topics/computer-science/monero.

superato il valore di $ 10 miliardi. Le attività criminali che hanno ricevuto il maggior numero di finanziamenti in criptovalute tra il 2017 e il 2020 includono il finanziamento di organizzazioni terroristiche, la vendita di sostanze stupefacenti e armi sulla Darknet, truffe, ransomware, pedopornografia online. Inoltre, le criptovalute vengono sempre più utilizzate anche nel riciclaggio di denaro e nell'evasione fiscale[15].

L'utilizzo sempre più massivo ha reso le criptovalute elemento di facilitazione in traffici illeciti e, conseguentemente, una minaccia emergente per le Forze dell'Ordine di tutto il mondo e per le Agenzie di Sicurezza ed Intelligence. Per illustrare meglio la situazione, Europol, l'Agenzia Europea di Polizia, nel suo recente IOCTA 2020 – Internet Organized Crime Threat Assessment, ha dedicato particolare attenzione ai nuovi portafogli crittografici *e-wallet*, come "*Wasabi*" e "*Samurai*", indicandoli come una nuova minaccia ed un nuovo notevole ostacolo alle indagini delle forze dell'ordine. Anche il rapporto di fine 2020 sull'utilizzo delle criptovalute della Cyber-Digital Task Force del Dipartimento di Giustizia degli Stati Uniti evidenzia il crescente utilizzo delle criptovalute nelle transazioni e commerci illeciti, con particolare riferimento alla Darknet.

Le nuove sfide investigative per le Forze dell'Ordine non possono quindi prescindere da una attività di *Cryptocurrency Forensics* quale fattore chiave per rilevare e de-anonimizzare le transazioni illecite sulla blockchain, mediante l'analisi crittografica specializzata e l'intelligenza blockchain. Questa innovativa attività forense rappresenta oggi l'unico modo in cui le forze dell'ordine e le Agenzie di Sicurezza possono affrontare e mitigare queste nuove sfide investigative, mediante:

- identificazione di transazioni illecite o sospette e relativi indirizzi crittografici;
- attività di tracciamento sulla blockchain, seguendo le tracce delle criptovalute utilizzate in transazioni illecite;
- individuare le reali identità di coloro che stanno dietro queste transazioni.

[15] In argomento si rimanda al contributo di P. SAMMARIO, R. BRIGHI, *Cyberlaundering e Blockchain Forensics: aspetti giuridici e tecnici del riciclaggio di criptovalute*.

Disporre di un adeguato *know how* e della necessaria tecnologia avanzata tuttavia non è sempre sufficiente, essendo questo un ambito investigativo in continua evoluzione dove criminali e terroristi riescono a nascondere più facilmente le loro tracce con l'ausilio di specifici servizi e tecnologie, tra cui:

- Mixers – piattaforme online che, come il termine suggerisce, permettono di mescolare numerose transazioni illecite in criptovalute, potenzialmente identificabili con altri al fine di rafforzare l'anonimato delle stesse;
- Shapeshifters – per mescolare e convertire fondi di criptovalute da una moneta crittografica a un'altra;
- Portafogli di Criptovalute con una incrementata protezione della privacy, quali ad esempio i già menzionati *Wasabi* e *Samurai*, che incorporano funzionalità di privacy o sicurezza come browser anonimizzati e/o servizi di miscelazione.

L'attività di Cryptoforensics, in ausilio di una attività investigativa, come detto, richiede la compresenza di vari fattori unitamente ad una adeguata tecnologia. All'esperienza operativa degli investigatori coinvolti vanno abbinate le corrette *best practice*, ovvero l'utilizzo delle procedure che hanno permesso di ottenere nel tempo i migliori risultati ed una adeguata tecnologia, in particolare per quanto riguarda la corretta piattaforma di analisi.

Queste piattaforme di decrittazione, come ad esempio quella di Chainalysis, combinano l'analisi delle *blockchain* delle varie criptovalute pubblicamente disponibili con dataset proprietari di indirizzi conosciuti di varie entità, risultando essenziali per tracciare il percorso seguito dalle criptovalute per giungere infine al beneficiario.

L'analisi non può che iniziare con l'individuazione della transazione illecita in criptovaluta, solitamente nota. Queste transazioni, quando generate per trasferire fondi, a differenza di quanto avviene quando si effettuano degli acquisti con beni espressi in valute correnti come dollari o euro, hanno normalmente importi ben definiti, ovvero senza troppi decimali, ad esempio 0.001 BTC, mentre quando vengono effettuati acquisti di beni o servizi illeciti espressi in altre valute correnti hanno normalmente importi con numerosi decimali, ed esempio 0.003961 BTC.

Evidentemente una singola transazione con numerosi decimali può rappresentare un importo con una specifica unicità, permettendo così, almeno inizialmente, una maggiore facilità di individuazione e tracciabilità, in mezzo a tante altre. Partendo quindi dal portafoglio o *e-wallet* di provenienza si seguono le tracce fino all'*e-wallet* di destinazione e quindi, eventualmente, verso altri *e-wallet* ed infine, normalmente, ad uno o più *Cryptocurrency Exchangers* (scambiatori di criptovalute) dove tali fondi possono rimanere dormienti o essere incassati al netto delle commissioni in "*FIAT money*", ovvero in valuta corrente (dollari, euro, o altra valuta) dall'ultimo beneficiario. Tuttavia, normalmente questi importi vengono immediatamente aggregati con altri importi e quindi trasferiti su altri *e-wallet* o uno dei citati servizi di *Mixer* dove le specifiche criptovalute attenzionate, vengono mischiate con altre criptovalute provenienti da altre transazioni, magari lecite, e quindi al netto di una commissione, trasferite su altri *e-wallet* riconducibili allo stesso proprietario. In altre circostanze, per offuscare il flusso di criptovalute e rendere sempre più difficoltosa la tracciabilità delle transazioni e spendite illecite attenzionate, vengono utilizzati servizi di *Shapeshifters*[16], che permettono di mixare e convertire fondi da una criptovaluta ad un'altra a scelta tra oltre 750 criptovalute disponibili.

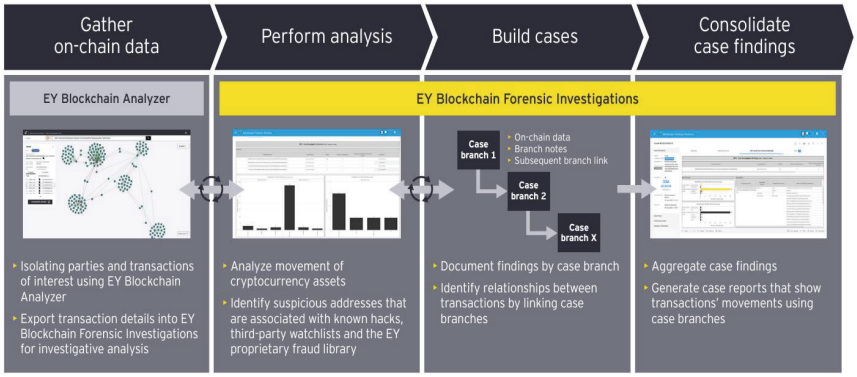


Figura 4. Questo schema riassume le principali fasi di raccolta e analisi dati della blockchain, necessarie per sviluppare e finalizzare una attività investigativa cripto forense. Fonte EY (Ernst & Young Global Limited).

[16] ShapeShift Publishes Report on Cosmos, Polkadot and NEAR *Decentralized Protocols. Analysis is the first of a series that assesses emerging smart contract blockchains*, 2021. https://shapeshift.com/newsroom/shapeshift-publishes-report-on-cosmos-polkadot-and-near-decentralized-protocols.

Al termine della complessa attività di tracciamento effettuata con i necessari ed indispensabili software e tool di analisi, come quelli offerti dalle società: Chainalysis e EY, o di altre società che svolgono analoghi servizi, risulterà essenziale la cooperazione degli "Exchangers", ovvero di quelle società finanziarie che si occupano di acquistare e vendere criptovalute, e che frequentemente custodiscono i portafogli digitali (*e-wallet*) beneficiari delle transazioni illecite analizzate.

Per convertire le varie criptovalute in una valuta corrente questi *e-wallet* devono necessariamente essere collegati ad uno o più conti correnti tradizionali e/o una o più carte di debito, in entrambi i casi necessariamente associati ad una società o ad una persona fisica. A questo proposito, infatti, la già citata Direttiva Europea 2018/843 (nota come quinta Direttiva antiriciclaggio), entrata in vigore il 10 gennaio 2020, ha esteso gli obblighi antiriciclaggio ai prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra le valute virtuali e valute aventi corso legale (quali appunto gli Exchangers) e i prestatori di servizi di portafoglio digitale (Custodial Wallet).

La stessa direttiva, tra le altre indicazioni, introduce l'obbligo da parte di queste società finanziarie di certificare la reale identità dell'intestatario del *e-wallet gestito* e di fornire tali informazioni qualora richieste dall'Autorità Giudiziaria. La Direttiva Europea in parola è stata recepita dal Legislatore italiano con il D.lgs. n. 125/2019, che ha modificato e integrato il Decreto legislativo 231/2007 estendendo gli obblighi antiriciclaggio alle due sopra citate categorie ma lasciando ad un decreto ministeriale il compito di istituire e di definire i requisiti di accesso a uno specifico albo. Introducendo anche specifici articoli, che disciplinano la cooperazione tra la FIU (*Financial Intelligence Unit*)[17] e le Autorità di Vigilanza di settore, italiana e quelle degli altri Stati Membri, rafforzando ulteriormente lo scambio di informazioni. Nelle more dell'emanazione del citato decreto, è intervenuta la Guardia di Finanza per precisare che, anche in assenza dell'iscrizione all'istituendo albo, Exchangers e Custodial Wallet operanti sul suolo nazionale dovranno comunque rispettare gli obblighi antiriciclaggio.

[17] Europol. Financial Intelligence Units – FIU.NET.
https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net.

Diventa pertanto indispensabile aver stabilito opportuni accordi di collaborazione con i vari Exchangers operanti al fine di concordare efficienti e sicure modalità di scambio delle informazioni richieste che, fornendo la reale identità del beneficiario finale delle transazioni illecite, permetteranno nella maggior parte dei casi di finalizzare l'attività investigativa.

5. Conclusioni

Nonostante l'enorme sforzo profuso dagli organi inquirenti, ed in particolare dalle Forze dell'Ordine di tutta Europa, che ha permesso negli anni di addivenire a numerosi successi investigativi esplicitatisi nella sistematica chiusura e rimozione dei maggiori Dark Markets attivi nella DarkNet, il continuo svilupparsi di nuove tecnologie e tecniche di anonimizzazione da parte dei gestori degli stessi, spesso supportati da facoltose organizzazioni criminali, rende sempre più difficile bloccare ed investigare l'acquisto e la vendita di beni illeciti online. Dalle carte di credito agli account dei social media, ai numeri di previdenza sociale, ogni informazione può essere trovata negli angoli più oscuri della Dark Web, dove tutto può essere trasformato in denaro.

Non ultimo il fenomeno criminale noto come CaaS (Crime As A Service), ove sviluppatori di malware vendono i loro prodotti, noleggiano i propri servizi, o forniscono tutto il supporto tecnico e informatico per realizzare un nuovo Dark Web Market; la barriera per l'ingresso per i criminali informatici rimane bassa. Allo stesso tempo un enorme sforzo ha avuto luogo nel settore delle criptovalute, dove nonostante le difficoltà crescenti nel cercare di tracciare i flussi di criptovalute sempre più numerose e sofisticate, la recente Direttiva Europea 2018/843 - meglio nota come quinta Direttiva antiriciclaggio, ha attuato una necessaria armonizzazione delle normative vigenti nei vari Stati Membri.

In particolare, estendendo gli obblighi antiriciclaggio ai prestatori di servizi quali Exchangers e Custodial Wallet, ha finalmente dato nuove prospettive alle complesse attività investigative e di Cryptoforensics che quotidianamente vengono svolte nella DarkNet. Conseguentemente l'industria delle criptovalute e gli scambi in particolare hanno continuato a rafforzare le loro *misure "know your customer"* (KYC), sia attraverso il loro crescente sforzo per identificare i clienti sia per un nuovo tessuto normativo.

Nel presente contributo abbiamo analizzato molti fattori che rendono le indagini nella DarkNet ed in particolare nel tracciamento delle criptovalute impegnative ed estremamente complesse, e possiamo ragionevolmente aspettarci che queste difficoltà continueranno ad aumentare nelle indagini future, in considerazione della continua evoluzione tecnologica degli strumenti e delle tecniche di anonimizzazione e offuscamento, tra cui: servizi di miscelazione di criptovalute centralizzati e decentralizzati, nuove criptovalute create "*privacy by design*", *trading over the counter*, servizi nidificati, nei quali lo scambio è incorporato all'interno di un portafoglio o di un altro servizio.

Oltre alle nuove criptovalute ed ai nuovi servizi incentrati sulla privacy, il protocollo Bitcoin stesso dovrebbe presto implementare nuove funzionalità che lo renderanno meno trasparente sia per gli osservatori occasionali che per gli investigatori[18]. Come osservato da Europol nell'ultima edizione del suo Internet Organised Crime Threat Assessment (IOCTA) 2020[19], è molto probabile che i criminali informatici si rivolgeranno sempre più a mercati che supportano transazioni decentralizzate, pertanto si assisterà ad un progressivo abbandono del tradizionale modello centralizzato con conti di deposito ed "escrow accounts" a garanzia delle transazioni dirette tra acquirenti e venditori, diminuendo l'influenza degli amministratori di mercato e scoraggiando in tal modo le truffe di "*exit scams*" tutt'altro che rare.

Tuttavia, l'impegno delle Forze dell'Ordine, con il coordinamento e la fattiva collaborazione di Europol, e grazie ad una sempre più stretta collaborazione con le principali aziende informatiche, società finanziarie ed istituti di credito di tutto il mondo, ha permesso negli anni di ottenere importanti successi investigativi. Iniziando con *Silk Road* chiuso definitivamente dall'F.B.I. nel 2014, proseguendo con l'Operazione Bayonet gestita da F.B.I., Polizia olandese e Polizia Federale tedesca, che nel luglio del 2017, dopo alcuni mesi di gestione, ha permesso la chiusura e l'arresto degli amministratori di *AlphaBay* e "Hansa Market", all'epoca i maggiori DarkNet Markets operativi. Nel 2019 la chiusura di "Berlusconi Market" a conclusione dell'Operazione Darknet.Drug da parte delle Guardia di Finanza.

[18] Armor. *Dark Market Report: The New Economy*, 2020.

[19] Europol. Internet Organised Crime Threat Assessment (IOCTA 2020). https://www.europol.europa.eu/printpdf/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

Per giungere infine nel febbraio 2021 ad opera della Polizia Federale tedesca, UK NCA, Polizia Australiana, ed altre con la consueta collaborazione di Europol, alla chiusura ed all'arresto degli amministratori di *DarkMarket*[20], fino a quel momento nuovo market leader della DarkNet con quasi 500.000 utenti, più di 2400 venditori, ed oltre 320.000 transazioni che hanno portato ad un giro di affari di oltre 4650 Bitcoin e 12.800 Monero, per un controvalore complessivo stimato di oltre 140 milioni di euro. Ma nuovi DarkMarket sono in agguato.

[20] Europol. *Darkmarket: World's largest illegal Dark Web Marketplace taken down*. (2021), https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643012
pp. 227-243 (gennaio 2022)

Dal *Phishing* allo *SMiShing*. Strumenti di prevenzione e repressione delle frodi informatiche

Ulrico Bardari[1]

1. Introduzione

Il *Phishing* e lo *SMiShing* utilizzano rispettivamente e-mail e mes-saggi di testo del telefono cellulare (SMS) per indurre le vittime a un'azione immediata come il download di malware mobile, la visita a un sito Web dannoso o la chiamata a un numero di telefono fraudolento. Questi atti criminali sono solitamente creati per suscitare un'azione immediata da parte del bersaglio, richiedendogli di consegnare informazioni di identificazione personale e dettagli dell'*account*. I profitti realizzati con questi sistemi possono essere paragonati a quelli realizzati dallo spaccio di sostanze stupefacenti su larga scala, ma con rischi e costi estremamente inferiori.

Nonostante alcuni di questi fenomeni siano noti già da diversi anni[2,3] nei paesi occidentali, restano scarse ed inefficaci le misure preventive e repressive volte ad arginare il problema.

> Ciascuno di noi si crede uno ma non è vero: è tanti, signore, tanti, secondo tutte le possibilità d'essere che sono in noi: uno con questo, uno con quello diversissimi! E con l'illusione, intanto, d'esser sempre uno per tutti, e sempre quest'uno che ci crediamo, in ogni nostro atto. Non è vero![4].

[1] Dottore di ricerca in Diritto e Nuove tecnologie, Università degli Studi di Bologna; Vice Ispettore della Polizia di Stato.

[2] C. Donuta (a cura di), *Handbook, The Language of Cybercrime, European Judicial Training Network*, EU, Lisbona, 2019.

[3] E. Yeboah-Boateng, P. Mateko Amanor, *Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices*, Journal of Emerging Trends in Computing and Information Sciences, 2014.

[4] L. Pirandello, *Sei personaggi in cerca di autore,* ETS, Milano, 2007.

2. Il *phishing* e le tipologie di attacco

I criminali informatici hanno a disposizione una varietà di strumenti e tecniche, inclusi *malware*, *ransomware* e attacchi *denial-of-service* indeterminata. Le strategie utilizzate dagli hacker nel *phishing* richiedono un *know-how* tecnico minimo e possono essere messe in atto da qualsiasi parte del mondo tramite una semplice e-mail.

In termini generali, il *phishing* è un metodo utilizzato dai criminali informatici per raccogliere informazioni personali e riservate. In queste truffe, i phisher inviano un'e-mail o indirizzano gli utenti a siti Web fraudolenti, chiedendo alle vittime di fornire informazioni sensibili. Queste e-mail e questi siti Web sono progettati per sembrare legittimi e ingannare le persone nel fornire numeri di carta di credito, numero di conto, password, nomi utente o altri dati particolari.

2.1. *Il phishing*

Phishing è un termine generico che si riferisce a qualsiasi attacco informatico in cui un hacker si traveste da a fonte attendibile per acqui-sire informazioni sensibili. In genere, sotto i tradizionali attacchi di *phishing*, gli *hacker* inviano e-mail fraudolente e dannose a quante più persone possibile. Non è insolito per il *phishing* attaccare per colpire migliaia di individui contemporaneamente nella speranza di ottenere anche solo poche vittime.

Gli attacchi di *phishing* adottano un approccio basato sulla quantità rispetto alla qualità. Nonostante la casualità degli attacchi, i phisher possono ottenere informazioni molto accurate sulle loro vittime tramite l'invio di e-mail di massa, facili da replicare.

L'obiettivo di queste e-mail è compromettere i dati o una rete più ampia sfruttando la più grande vulnerabilità della sicurezza nello spazio cibernetico, ovvero gli utenti stessi. In effetti, invece di passare attraverso un attacco diretto alle difese dei sistemi di archiviazione, gli hacker preferiscono usare attacchi di *phishing* per indurre qualcuno a dargli accesso a una rete o ai propri dati.

Per ingannare le vittime, gli aggressori personalizzano le e-mail di *phishing* per farle sembrare legittime, a volte utilizzando loghi o account di posta elettronica fittizi per migliorare l'efficacia dell'attacco. Di solito, i phisher fingono di essere una fonte attendibile, come un ospedale, una banca o un datore di lavoro. Il messaggio di *phishing*

potrebbe includere un linguaggio allarmante o suggestivo per ingannare le vittime inducendolo a, clickare su un link, aprire un documento, installare un software (*malware o keylogger*), inserire il *proprio username* e password in un sito web apparentemente originale.

A seguito di una delle azioni sopra descritte, l'hacker può infettare il computer della vittima e rubare informazioni sensibili, spesso senza dover utilizzare una sola riga di codice. Con gli attacchi di *phishing*, anche i più potenti firewall non possono impedire a un individuo di fare click su una e-mail contenente un *malware*. E, una volta infettato un singolo computer, il *malware* può diffondersi in un'intera rete.

2.2. *L'evoluzione del phishing: lo spear-phishing*

Sebbene gli attacchi di *phishing* siano efficaci, sono progettati per essere ampi e colpire il maggior numero di persone possibili; di conseguenza sono generalmente scritti in modo vago e sono facili da individuare. Attacchi di *spear phishing* sono molto più convincenti, mirati e sofisticati.

Con lo *spear phishing*[5], i criminali informatici restringono l'ambito del loro attacco a un gruppo più piccolo, a volte solo una manciata di individui. In questo modo, gli hacker possono fare ricerche e impostare il *phishing* e-mail in modo più convincente sulla base al profilo di una vittima o all'attività online. Gli *hacker* possono trovare la maggior parte delle informazioni necessarie per effettuare un attacco di *spear phishing* direttamente su *Internet*, in particolare sui siti web aziendali e sui *social network*. Non è raro che i *phisher* utilizzino come bersaglio le informazioni personali (ad es. nome o indirizzo) o le informazioni personali dei loro amici, familiari e colleghi come leva in un'e-mail.

Poiché gli attacchi di *spear phishing* sono molto personalizzati, è più probabile che abbiano successo rispetto ad attacchi di *phishing* tradizionali. Inoltre, questi attacchi hanno spesso obiettivi specifici. Per esempio, un *phisher* può prendere di mira determinate persone in base a chi lavora, il tipo di informazioni a cui hanno accesso o sulla loro situazione finanziaria. Gli attacchi di *spear phishing* possono concentrarsi su una particolare azienda, organizzazione, gruppo o agenzia governativa in base al potenziale ritorno d'investimento.

[5] M. Shacklett, *Spear Phising*, Techtarget, agosto 2021.

2.3. *Il whailing*

Il whailing (caccia alle balene) è un altro tipo di schema di rappresentazione di mittenti e domini, ad esempio, e-mail che vengono inviate a una singola persona o ad un piccolo gruppo di obiettivi, che differisce dalle tecniche di distribuzione di massa utilizzate nello standard del *phishing attack*[6]. Si parla di "*attacchi di balene*", perché i cyber-criminali prendono di mira in modo specifico dirigenti aziendali di alto profilo.

In queste truffe, le e-mail e le pagine Web fraudolente sono progettate per simulare la segnalazione di attività critiche da parte di qualcuno con legittima autorità, esterno o interno all'organizzazione. Solitamente si rivolgono ai dirigenti, in prima persona, con dettagli credibili quali nome completo, azienda e ruolo.

Negli attacchi di *whailing*, i criminali di solito cercano informazioni riservate dell'azienda. Ad esempio la password per accedere ad account sensibili o ad informazioni su processi e prodotti specifici. Messaggi di *whailing* spesso impiegano tattiche intimidatorie, minacciando spese legali, licenziamento e bancarotta per indurre la vittima ad intraprendere un'azione specifica (ad esempio, fare click su un collegamento, scaricare software dannoso o completare un'azione fraudolenta). L'e-mail o il sito Web sul *whailing* può presentarsi sotto forma di un falso mandato di comparizione, un falso messaggio della polizia o una sorta di denuncia legale.

2.3. *Il pharming*

Il *pharming* è noto anche come "*phishing* senza esca" perché l'esca è rappresentata dalla stessa e-mail. Il *pharming* è una forma avanzata di ingegneria sociale in cui l'attaccante crea un sito Web fasullo, per esempio un portale di accesso "Microsoft", e quindi inganna il server DNS[7] per reindirizzare a questo sito Web. Una volta arrivati sulla pagina, alla vittima viene richiesto di inserire le proprie credenziali o informazioni finanziarie, che vengono poi inviate direttamente all'attaccante.

[6] L. Gobbi, *Attacchi whaling la caccia informatica alle balene che minaccia ceo cfo e tutti i c-level/*, Cybersecurity360, febbraio 2021.

[7] Domain Name System: sistema di nomi di dominio utilizzabili come "risoluzione" per indirizzi IP originali.

Il *pharming* non si rivolge specificamente a una persona: reindirizza semplicemente il traffico da un sito Web autentico a una pagina apparentemente identica e contraffatta, al fine di rubare le informazioni dei visitatori. Un esempio pratico è il massiccio furto di dati subita da *British Airways* nel 2018, che ha visto gli *hacker* rubare i dati di oltre 500.000 clienti tra il mese di aprile e di settembre. Questi clienti avevano effettuato l'accesso al sito Web di *British Airways* per effettuare una prenotazione e sono stati inconsapevolmente dirottati su un sito fraudolento in cui gli aggressori hanno raccolto le loro informazioni finanziarie. La colpa della violazione è stata attribuita ai sistemi di sicurezza di *British Airways* e, in conformità a quanto previsto dal Regolamento Generale per la Protezione dei Dati Personali (Regolamente EU 619/2016), la compagnia aerea è stata multata di 20 milioni di sterline dall'Information Commissioner's Office (ICO): la più grande multa che l'ICO ha emesso fino ad oggi[8].

3. Lo SMiShing

Lo *SMiShing*, noto anche come SMS *phishing*, potrebbe essere classificato come una sorta di attacco di ingegneria sociale. A differenza dell'e-mail *phishing*, lo *SMiShing* viene eseguito tramite messaggi di testo SMS. Un tipico esempio di *SMiShing* è quando l'autore delle minacce, analogamente al *phishing*, impersona un'entità legittima come il servizio IT o l'amministratore della sicurezza di note aziende, banche, agenzie governative, e-commerce, consegna pacchi, ecc., per indurre le vittime a divulgare il loro nome utente/password o altre informazioni sensibili.

Sebbene ci sia stato un aumento della consapevolezza riguardo alle truffe SMiShing[9], la minaccia rappresentata da questa modalità non può essere ignorata perché la maggior parte degli individui dipende ancora dagli SMS e da altre applicazioni mobili di messagistica per comunicare.

Con le autenticazioni a due fattori e la dismisssione delle chiavi RSA per generare password temporanee, gli SMS sono diventati il principale strumento di autenticazione fornito agli utenti.

[8] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers.

[9] G. Perego, *Smishing, la truffa dell'SMS: cos'è e come difendersi*, INSIC notizie, maggio 2021.

Ciò che rende lo *SMiShing* il tipo di attacco più insidioso è la tendenza a fidarsi dei messaggi SMS più dei messaggi di posta elettronica. Il funzionamento di un attacco di *SMiShing* è simile a quello del *phishing*, il malintenzionato si finge provenire da un ente attendibile e chiede i dati della vittima o la incoraggia a visitare un collegamento per ottenere un'offerta, un premio, uno sconto oppure risolvere un finto problema ma con un grado di fiducia maggiore perché proveniente da un SMS con intestazione conosciuta.

Questa azione consentirà all'autore della minaccia di ottenere, con maggiore probabilità rispetto al *phishing*, i dati sensibili della vittima o avviare un processo di download di *malware* in background.

Lo screenshot riportato in figura 3 rappresenta un elenco di messaggi provenienti dal medesimo ID (identificativo, ovvero il nome del mittente che compare a video) corrispondente a un noto istituto di credito, ma, in realtà il secondo SMS proviene da un *sender* incaricato dal Phisher ad inserire l'ID utilizzato dalla Banca.

La raccolta di SMS o *chat* sotto il medesimo ID è tipica dei software installati nei sistemi operativi più diffusi: *Android e iOS*. In tale contesto le vittime avranno maggiori difficoltà nel distinguere all'interno della stessa chat quali possano essere i messaggi autentici e quali quelli fittizi.

Figura 1. SMS reali e fittizi provenienti dallo stesso ID bancario ricevuti sullo smartphone dall'autore del capitolo.

Secondo uno studio svolto dalla Proofpoint[10], nei primi sei mesi del 2021 lo *SMiShing* è aumentato del 700% rispetto ai sei mesi precedenti. Ciò significa che gli sforzi fatti dagli istituti di credito e dalle aziende coinvolte con maggiore frequenza, sono stati inefficaci tecnicamente e inadatti a scoraggiare i malviventi.

3.1. *Il vishing*

Il *vishing* è una forma di *phishing* che utilizza sistemi telefonici e tecnologie simili. Gli utenti possono ricevere un'e-mail, messaggio telefonico o testo (di solito chiamato *smishing*) che li incoraggia a chiamare un numero di telefono per correggere qualche discrepanza.

In genere, gli aggressori utilizzano una tecnica chiamata *spoofing* dell'ID chiamante (come in Fig. 1 per lo *SMiShing*) per far apparire le chiamate come fossero provenienti da un numero di telefono legittimo. Se una vittima chiama un numero in una truffa di *vishing*, una registrazione o un criminale affiliato richiede loro di fornire informazioni dettagliate, inclusi numeri di carta di credito, date di nascita e indirizzi, oppure un codice d'accesso per l'autenticazione a due fattori.

Recentemente gruppi criminali, anche improvvisati, sono riusciti ad elaborare truffe con attacchi di *vishing* e *smishing* combinati. Per eseguire gli attacchi, gli *hacker* installano la voce interattiva software di risposta su computer remoti, oppure vengono coinvolte persone che parlino la stessa lingua o, addirittura, lo stesso dialetto delle vittime. Le chiamate e i messaggi sembravano provenire da un istituto finanziario rispettabile che istruisce le vittime a chiamare un numero di telefono a causa di un problema con l'account; in questo modo vengono rubati numeri di conto bancario, PIN e altri dati personali.

3.2. *Come viene realizzato tecnicamente lo SMiShing*

Nonostante vi sia certezza che le forme di criminalità informatiche descritte nel presente contributo vengano realizzate in gran parte da organizzazioni criminali, la loro implementazione può essere facilmente sviluppata anche da una persona singola.

[10] Cfr. *Report State of the Phish 2021*, https://www.proofpoint.com, Proofpoint, Inc. è una società di sicurezza aziendale americana con sede a Sunnyvale, California, che fornisce software come servizio e prodotti per la sicurezza.

Per iniziare, il criminale ha bisogno di avere a disposizione una grande quantità di utenze telefoniche mobili da contattare. Liste di utenze telefoniche divise per area geografica, piuttosto che per sesso del titolare o altri elementi qualitativi sono reperibili presso "venditori" che creano appositi gruppi Telegram o si rendono reperibili nel *dark web*. Ad esempio, per i criminali è importante scegliere contatti telefonici di una determinata area geografica perché, durante la telefonata al bersaglio per la richiesta delle credenziali, sarà più facile ottenerli proponendo un accento familiare. Oppure potrebbe essere più proficuo attaccare utenze telefoniche appartenenti a soggetti anziani perché più facilmente raggirabili.

Ottenuta la lista delle utenze l'agente deve rivolgersi ad un *sender* per inviare gli SMS con il contenuto prescelto e con un ID che possa essere verosimilmente lo stesso dell'istituto di credito o dell'azienda reale. Nel corpo del messaggio, oltre al testo ingannevole ci sarà un link che indirizzerà ad una pagina di accesso identica all'originale, ma gestita dall'autore del reato. In tale contesto si realizza la fase in cui vengono carpiti i primi dati sensibili, ovvero l'inserimento della username e password nella home page clonata che le memorizza su un database collegato alimentato dai *file di log*. Mediante i dati carpiti si potranno ricavare informazioni personali del cliente, compreso il numero di telefono e, qualora si tratti di un conto corrente bancario, anche il saldo e la lista movimenti.

A questo punto è possibile completare l'attacco per raggiungere il profitto attraverso il *vishing*, cioè entrando nel profilo di home banking della vittima e richiedendo il cambio del numero di telefono oppure la sostituzione del dispositivo come secondo fattore di autenticazione. Il sistema invierà un codice di verifica all'utenza del titolare reale, il quale riceverà una telefonata da parte di un presunto impiegato dell'azienda per ottenere il codice ricevuto via SMS. Se quest'ultimo passaggio verrà portato a termine, da quel momento, l'autore del reato diventa titolare del profilo, dell'*account* o dell'*App gestionale* della vittima assumendone il pieno controllo, compresa la possibilità di effettuare movimenti finanziari.

3.3. *Le azioni per prevenire lo SMiShing*

In base a quanto previsto dall'art. 10 del Decreto legislativo 11/2020[11] la banca deve dimostrare:

1. autenticazione corretta da parte del cliente;
2. corretta registrazione e contabilizzazione delle operazioni contestate (producendo documentazione dei *LOG* delle operazioni, con la prova di invio di codice OTP[12], autenticazione *Touch ID, Face ID*, chiave *Device* univoca…);
3. assenza di malfunzionamenti dei sistemi informatici o *dell'online banking*;
4. in alternativa: la presenza di frode, dolo o colpa grave da parte dell'utente cliente.

Nella documentazione relativa ai *file di log* emergerà la seguente successione di eventi:

1. l'utente si autentica da un indirizzo IP differente rispetto ad i soliti utilizzati;
2. la richiesta di cambio del numero di telefono e/o del dispositivo per il secondo fattore di autenticazione;
3. una serie di operazioni bancarie.

Questa serie di operazioni possono essere oggetto di maggiore attenzione dai sistemi di monitoraggio automatici degli istituti bancari. Le tre variabili descritte, ma anche solo le prime due, dovrebbero far destare sospetti e di conseguenza dovrebbero essere dilatati i tempi di avvio del nuovo sistema di autenticazione del secondo fattore oppure dovrebbero attivare degli *alert* diretti alla precedente numerazione e/o dispositivo.

Le frodi informatiche di tipo *Smishing, Spoofing, Vishing* sono talmente diffuse da rendere incomprensibile il motivo per cui i sistemisti incaricati dalla Banca, deputati alla prevenzioni delle frodi informatiche, non attivino forme di *alert* ogni qualvolta vengano registrati cambi di utenza a seguito di autenticazione attraverso IP o dispositivo "insolito".

[11] Decreto Legge 30 novembre 2020, n. 157. Ulteriori misure urgenti connesse all'emergenza epidemiologica da COVID-19 (GU Serie Generale n.297 del 30-11-2020).

[12] One Time Password: password utilizzabile una sola volta.

Ancor più inspiegabile è il motivo per cui gli stessi sistemisti non sospendano operazioni bancarie immediatamente successive all'attività sospetta appena descritta. Tali operazioni tecniche, di controllo e verifica dei tabulati in *real time*, sarebbero di banale applicazione per qualunque sistemista.

4. Le vittime degli attacchi

Sia le truffe di *phishing* che quelle di *smishing* possono colpire chiunque. Gli attacchi di *phishing* sono più espansivi e non hanno necessariamente una componente psicologica rispetto a chi viene attaccato. Gli attacchi di *smishing*, tuttavia, sono più ragionati e pianificati. Questi attacchi hanno spesso due obiettivi: individui o datori di lavoro.

I criminali informatici prendono di mira gli individui perché sono i più facili da colpire e i più suscettibili da attacchi di *phishing*. Questo a causa della inevitabile asimmetria informativa che caratterizza il rapporto di molti individui con la tecnologia. I *phisher* possono ottenere una serie di informazioni critiche da un individuo, comprese informazioni bancarie, credenziali eBay, Facebook, PayPal ecc. che consentono di rubare denaro o identità con facilità.

Per i datori di lavoro ogni dipendente rappresenta una potenziale esposizione ad attacchi di *phishing*: un truffatore esperto potrebbe facilmente ingannare i dipendenti a tutti i livelli dell'organizzazione mettendo a repentaglio informazioni finanziarie dell'azienda, segreti commerciali, documenti riservati. I datori di lavoro sono spesso il bersaglio di campagne di *spear-phishing* altamente mirate. Infatti i loro nomi e le informazioni di contatto sono facilmente recuperabili dai siti Web aziendali e, grazie a tali informazioni, i cyber-attaccanti possono creare e-mail convincenti per ingannare i dipendenti.

Gli obiettivi di questi attacchi variano in genere in base alle motivazioni di un *phisher* e al tipo di dati ricercati. Sebbene il guadagno finanziario sia spesso il fattore principale per gli attacchi di *phishing*, il furto aziendale può avere insiti altri obiettivi come la divulgazione di dati, la divulgazione di segreti commerciali o lo spionaggio industriale. I datori di lavoro di ogni settore sono a rischio, ma lo sono in modo particolare quelli di imprese finanziarie e siti di vendita al dettaglio *on-line*.

Per far fronte alla vulnerabilità degli utenti della rete, resta particolarmente rilevante la formazione ad un uso consapevole delle tecnolo-

gie. In particolare, occorre sensibilizzare le persone ad essere cauti nell'aprire mail che provengono da mittenti non riconosciuti, con contenuti vaghi o impersonali. Gli utenti devono porre particolare attenzione a non confermare le informazioni personali o finanziarie anche se si pensa di conoscere il mittente. In generale bisogna evitare di rispondere al mittente se si sospetta che un'e-mail sia dannosa. Nel caso si riconosca l'individuo o l'azienda che invia l'e-mail sospetta, sarà utile seguire il mittente *offline* per avere la garanzia della volontarietà del contatto ricevuto. Le e-mail o gli SMS spesso includono un linguaggio minaccioso, spaventoso e persuasivo devono essere analizzate più accuratamente. Gli utenti vanno istruiti anche sul rispetto di basilari accorgimenti tecnici di non fare *click* sui collegamenti in una schermata *pop-up* ed evitare di passare il mouse sopra e ricontrollare l'indirizzo di eventuali collegamenti prima di fare *click* su di essi.

L'attacco di tipo *phishing* o *smishing* si può prevenire esaminando regolarmente gli account online e utilizzare *password* diverse per ciascuno di essi, oltre a rivedere spesso gli estratti conto della propria banca e carta di credito assicurandosi che tutte le transazioni siano sempre autorizzate. I browser e gli antivirus devono essere mantenuti costantemente aggiornati ed è consigliabile l'uso di *firewall*. Altra buone prassi è verificare la sicurezza di un sito web. I siti Web legittimi avranno un URL che inizia con *https* con un'icona a forma di lucchetto chiuso vicino alla barra degli indirizzi. Infine è indispensabile segnalare immediatamente l'attacco al datore di lavoro e alle autorità competenti per consentire un intervento tempestivo che possa ridurre o evitare ulteriori conseguenze dannose.

5. Norme applicabili

La consulenza informatica forense e la correlata perizia, nel contesto trattato in questo capitolo, possono permettere di appurare le eventuali responsabilità di una delle parti coinvolte nel procedimento giudiziario, in particolare attraverso l'acquisizione di prove digitali. Il C.T.U.[13] informatico può quindi occuparsi di acquisire informazioni e dichiarazioni, seguendo specifici protocolli e usando adeguate strumentazioni.

[13] Consulente Tecnico d'Ufficio.

Al fine di individuare le fattispecie di reato è opportuno esaminare parallelamente le fasi costitutive del *phishing* e delle norme potenzialmente applicabili. Attualmente nell'ordinamento italiano non è presente una disciplina giuridica ad hoc che consideri unitariamente il fenomeno del *phishing* e delle forme d'attacco precedentemente descritte, esistendo, per contro, differenti norme giuridiche nelle quali poter ricondurre le condotte tipiche poste in essere per realizzare le singole fasi che lo contraddistinguono[14]. Infatti un attacco di tipo *phishing* non offende direttamente il patrimonio dell'utente, ma manifesta una propria ed autonoma dimensione offensiva, che si concretizza nel "furto di dati riservati" e la conseguente realizzazione di una serie di operazioni concernenti l'utilizzo illegittimo dei dati fraudolentemente raccolti. Ciò rileva certamente la necessità di proteggere la sfera riservata dell'individuo che, a seguito della evoluzione tecnologica diviene maggiormente vulnerabile[15].

Inoltre, non si rileva come alcune delle manifestazioni criminose proprie del fenomeno in esame assumano una valenza plurioffensiva, astrattamente riferibile a più fasi come nel caso della combinazione *SMiShing/Vishing*.

Per quanto riguarda le prime fasi, relative alla creazione e all'invio del messaggio di posta elettronica o SMS, contenente il link che reindirizza al sito web artefatto, solo all'apparenza proveniente dal mittente reale, potrebbe ritenersi integrata la fattispecie di sostituzione di persona ex art. 494 c.p.. Tale disposizione è applicabile, in quanto con l'e-mail o SMS inviato il phisher utilizza i dati identificativi di un mittente reale, sostituendosi illegittimamente ad altri attribuendosi un falso nome, stato o qualità a cui la legge riconosce effetti giuridici, inducendo così in errore un elevato numero di utenti, al fine di carpire i dati sensibili e le credenziali di ciascuno di essi, procurando un vantaggio a sé o recando un danno a terzi[16].

L'effettiva configurabilità di tale delitto deve essere comunque verificata in concreto in ragione delle peculiarità del web, in quanto potrebbero verificarsi delle asimmetrie rispetto agli elementi tipici del

[14] M. Crisafi, E. Trunfio, *Il phishing,* in Cendon P. (cura di), *Trattato dei nuovi danni*, Padova, CEDAM, 2011.

[15] F. Cajani, G. Costabile, G. Mazzaraco, *Phishing e furto d'identità digitale: indagini informatiche e sicurezza bancaria*, Milano, 2008.

[16] R. Flor, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in Riv. it. dir. e proc. pen., 2007, pp. 899-946.

reato, come, ad esempio, inesistenza nella realtà del mittente. Invece, la figura criminis prevista dall'art. 494 c.p. può delinearsi molto più chiaramente con il *Vishing*, ovvero quando, attraverso la telefonata con *ID spoofing*, una persona fisica esplicita un nome o di uno specifico stato o qualità in una società o di un ente. Infatti, nei casi in cui i dati riservati o le credenziali identificative degli utenti, fraudolentemente carpiti, siano utilizzati su siti web è possibile configurare il reato di accesso abusivo ad un sistema informatico o telematico ex art. 615-ter c.p.. L'impiego on-line di tali dati non induce in errore il sistema informatico, che esegue esclusivamente i comandi impartiti dall'utilizzatore del sistema, individuato come soggetto legittimato in ragione dell'uso delle credenziali autenticative.

Quando la condotta volta a carpire i dati riservati e le credenziali viene realizzata per mezzo della divulgazione di un *malware* nel sistema target potrà applicarsi il reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico ai sensi dell'art. 615-quinquies, dal momento che il software malevolo è finalizzato a reindirizzare l'utente ignaro a siti web, apparentemente identici a quelli reali, appositamente predisposti dal phisher per sottrargli le informazioni utili, ravvisandosi così l'ipotesi dell'"alterazione del funzionamento" del sistema utilizzato dalla vittima. Il *link* ingannatorio, generalmente contenuto nella e-mail ricevuta dall'utente, rimanda ad un sito identico nel formato e nel contenuto al sito reale elaborato dal *phisher*. Il sito web fittizio, così come rappresentato, induce la vittima ad inserire le proprie credenziali d'accesso nell'apposito *form* e ad effettuare un atto di disposizione (come descritto in precedenza, anche di natura patrimoniale), consentendo al *phisher* di ottenere i dati riservati e conseguire un ingiusto profitto. Si configura in questo modo la struttura tipica del reato di truffa ex art. 640 c.p.

La disposizione patrimoniale, quale conseguenza dalla condotta ingannatoria del phisher, indica chiaramente la natura del reato a cooperazione artificiosa della vittima, poiché l'induzione in errore non può che riferirsi all'utente ingannato[17].

Nel 2013[18] il legislatore, proponendosi di far fronte alle condotte di sottrazione di dati sensibili sulla rete internet, volte a conseguire un in-

[17] R. Flor, *op.cit.*

[18] Art. 9, co. 1, lettera a), della legge di conversione 15 ottobre 2013, n. 119, del d.l. 14 agosto 2013, n. 93.

debito profitto, aggiunse un'aggravante all'art. 640-ter c.p., rubricato «Frode informatica», nel terzo comma, a mente della quale «La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti».

Sembrerebbe potersi ammettere il concorso tra la sostituzione di persona di cui all'art. 494 c.p. e di truffa ex art. 640 c.p., poiché si tratta di due norme poste a salvaguardia di differenti beni giuridici. Inoltre, la condotta dell'agente che, «al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno», indebitamente si procuri i codici di accesso ad un sistema informatico o telematico difeso da misure di sicurezza integra il reato di cui all'art. 615-quater c.p., vale a dire del reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.

La fase successiva alla fraudolenta acquisizione dei dati riservati riguarda l'utilizzo delle stesse informazioni per accedere abusivamente a servizi *on-line* o ad aree private della vittima. L'accesso illegittimo, senza diritto, all'account dell'utente, eludendo le misure di sicurezza o l'autenticazione, configura l'ipotesi del reato di accesso abusivo ad un sistema informatico o telematico ai sensi dell'art. 615-ter c.p.. In ragione dell'eterogeneità dei beni giuridici tutelati si considera ammissibile il concorso tra il reato di truffa ex art. 640 c.p. e il reato di accesso abusivo ad un sistema informatico o telematico ex art. 615-ter c.p.

Qualora il phisher, dopo aver ottenuto le credenziali d'accesso dell'utente, dovesse utilizzare le stesse nei relativi account, alterando il funzionamento del sistema o intervenendo senza diritto su dati, informazioni o programmi presenti, determinando così l'ingiusto profitto con altrui danno, dovrebbe ritenersi integrato il delitto di frode informatica ai sensi dell'art. 640-ter c.p.[19]. In tal caso la condotta dell'agente sarebbe rivolta al sistema informatico e non alla vittima, in quanto finalizzata a manipolare il sistema stesso.

[19] Cfr. C. Pino, *Phishing-Cassazione Penale: risponde di frode informatica l'intestatario della carta prepagata utilizzata per attività di phishing*, in www.filodiritto.it, 29 novembre 2018, che richiama Cass. pen. sez. II, 24 ottobre 2018, n. 48553.

5.1. Il *financial manager*

Ultimamente si sono sviluppate nuove forme di attacco, c.d. "miste", che includono nell'azione criminosa oltre al *phisher* anche ulteriori soggetti, come il c.d. *financial manager* o prestaconto. Più precisamente, il phisher invia ad una moltitudine di soggetti una o più e-mail al fin di individuare chi sia disposto ad essere incaricato di far transitare sui propri conti e dietro pagamento di una commissione, il denaro frutto del *phishing* che sarà trasferito all'estero su altri conti correnti. Pertanto, nei casi in cui non si ravvisa il concorso del terzo nel reato può ritenersi configurabile il delitto di riciclaggio ex art. 648-bis c.p., qualora la condotta del suddetto soggetto terzo appositamente individuato dal *phisher*, consista nell'offrire a quest'ultimo un conto corrente sul quale poter spostare il denaro, ostacolando cosi l'individuazione della provenienza illecita.

Per ritenere sussistente il reato in questione il *financial manager* deve aver agito, a fronte di corrispettivo, nonostante la consapevolezza della provenienza illecita delle somme depositate sul conto da lui messo a disposizione. Il prestaconto, infatti, riceve il denaro, quale conseguenza dell'azione del *phisher* e, al fine impedire la ricostruzione della reale provenienza delle somme, lo trasferisce su un conto appositamente istituito, a seguito dell'attacco di *phishing*, facendo ricorso a società di *money transfer*, così da interrompere ogni traccia dei flussi monetari. Diversamente, può configurarsi il reato di ricettazione di cui all'art. 648 c.p. nei casi in cui il *financial manager*, avendo coscienza dell'origine criminosa del denaro, percependo le somme senza poi trasferirle sul conto.

Alla luce di quanto detto emerge chiaramente l'esigenza di tenere conto della concreta situazione di riferimento, poiché la condotta del *phisher* può astrattamente configurare i diversi tipi di reati preceden-temente esposti.

La giurisprudenza recente[20] si è orientata sull'attribuzione del concorso nel delitto di truffa piuttosto che di riciclaggio. Più sensibile alle modalità tecniche in cui si concretizzano gli attacchi di *Phishing*, ha compreso che spesso questi consistono in una vera e propria "alterazione" del funzionamento del sistema informatico, ad esempio tramite l'inoculazione sul PC o su uno smartphone di *trojan o malware*, nonché

[20] Cass., Sez. II, 1 marzo 2017, n. 10060.

tramite un «intervento non autorizzato su dati o informazioni» dell'utente, nell'ipotesi di trasferimenti *home banking* di fondi[21].

6. Attività di contrasto e conclusioni

Internet ha sempre facilitato il raggiungimento di clienti in tutto il mondo senza alcuna restrizione sul mercato e con un uso crescente ed efficace dell'*e-commerce*. Durante i *lockdown* imposti per contenere l'epidemia di Covid-19, grazie ai progressi tecnologici degli ultimi anni, le persone hanno potuto trasferire online parte delle proprie vite. Così, seppur spinti a rispettare politiche di tipo *stay at home*, è stato possibile mantenere una parvenza di normalità: a prescindere dalle diverse opinioni, favorevoli o contrarie, non si può negare il ruolo fondamentale che l'ICT ha avuto nel portare scuola, lavoro e tempo libero nelle case di tutti. Di conseguenza, il numero di clienti che si affidano ad Internet per eseguire gli acquisti è aumentato in maniera considerevole. In rete le transazioni economiche contano quotidianamente transazioni per centinaia di milioni di dollari. Questo flusso di denaro ha spinto i truffatori ad avviare operazioni fraudolente con buone possibilità di successo, grazie all'esposizione e alla vulnerabilità degli utenti di Internet rispetto ai diversi tipi di minacce proposte.

Il *social engineering* e i trucchi tecnici vengono comunemente combinati insieme per avviare un attacco di *phishing*. Prevedere e fermare gli attacchi di *phishing* rappresenta la sfida principale ed un passaggio obbligato per garantire la protezione delle transazioni online.

Sono stati proposti diversi approcci per mitigare le tipologie di attacco descritte in questo capitolo. Potrebbero essere adottate diverse misure *anti-phishing* tra cui soluzioni legali, educative e tecnologiche. Ancora oggi, nella maggior parte dei casi, l'identificazione dei siti Web di *phishing* viene eseguita manualmente. In questo caso l'utente, o il team preposto alla sicurezza, analizza la pagina Web e in base alle informazioni estratte prende una decisione sulla legittimità del sito stesso. Tuttavia, l'intelligenza artificiale e l'apprendimento automatico possono notare schemi problematici nei dati non strutturati e fornire ai team di sicurezza i dati di cui hanno bisogno per rispondere rapidamente.

[21] Cass., Sez. II, 24 febbraio 2011, D.L.P.M.C., in Mass. Uff., n. 249675.

L'apprendimento automatico è particolarmente adatto per rilevare le vulnerabilità che potrebbero eludere il team di sicurezza[22]. I metodi di filtraggio attualmente esistenti sono tutt'altro che ade-guati come, ad esempio, le *black-list* e le *white-list*.

Recentemente si è molto diffusa l'analisi euristica, cioè un metodo di rilevazione dei virus basato sull'esame del codice per la ricerca di proprietà sospette. Uno dei metodi euristici, noto come analisi euristica statica, comporta la "decompilazione" di un programma sospetto e l'esame del suo codice sorgente. Il codice viene quindi confrontato con virus noti e presenti in un database euristico. Se una determinata percentuale del codice sorgente corrisponde a qualcosa che è presente nel database euristico, il codice viene contrassegnato come possibile minaccia.

Un altro metodo è noto come analisi euristica dinamica. Quando gli scienziati vogliono analizzare qualcosa di sospetto senza mettere a rischio le persone, contengono la sostanza in un ambiente controllato, ad esempio un laboratorio protetto, ed eseguono i loro test. Il processo dell'analisi euristica è simile a questo, ma si svolge in un mondo virtuale[23]. Si isola il programma o il codice sospetto all'interno di una macchina virtuale specializzata, o *sandbox*, e si dà al programma antivirus la possibilità di testare il codice e simulare che cosa accadrebbe se si eseguisse il file sospetto. Si esamina ogni comando quando si attiva e si cercano eventuali comportamenti sospetti, come l'auto-replicazione, la sovrascrittura di file e altre azioni che sono comuni ai virus.Tuttavia, l'accuratezza degli approcci basati sull'euristica può diminuire notevolmente se alcune caratteristiche ambientali cambiano. Quindi, in tale contesto, gli utenti dovrebbero sempre dubitare del sistema di protezione e ignorare gli avvertimenti sollevati dai sistemi di rilevamento.

Il *phishing*, lo *smishing* e le altre forme d'attacco rappresentano un problema le cui caratteristiche significative sono in continua evoluzione. Pertanto, un modello di rilevamento del *phishing* di successo dovrebbe essere in grado di adattare le proprie conoscenze e la propria struttura in modo continuo e autonomo, in modo strutturante e interattivo potendo, solo così, fornire una difesa adeguata contro la mutevolezza che caratterizza questi tipi di minaccia.

[22] Z. ZHANG, et al. *Artificial intelligence in cyber security: research advances, challenges, and opportunities*. In *Artificial Intelligence Review: An International Science and Engineering Journal*, Springer Netherlands, p. 1, 2021.

[23] https://www.kaspersky.it/resource-center/definitions/heuristic-analysis.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643013
pp. 245-260 (gennaio 2022)

Indagini digitali forensi sui Social Network. Nuovi orizzonti investigativi

ANTONIO PUGLIESE[1]

1. Premessa

In una società perennemente interconnessa gli strumenti comunicativi in rete rappresentano proiezioni ineludibili della quotidianità umana. Non una valutazione sociologica, bensì oramai ampiamente giuridica. Numerosi atti legislativi suggeriscono questo approdo. Si pensi agli interventi eurounitari in punto di trattamento dati personali[2], cybersecurity[3], ovvero alla normazione in merito all'acquisizione di tabulati telefonici[4], o anche solo all'aggiornamento del codice penale e di procedura[5].

Le scienze informatiche vanno assumendo una accresciuta centralità nell'accertamento di penale responsabilità, centralità acuita dal progressivo avanzare della tecnica. Nell'era di più ampia diffusione di reati informatici, ove anche delitti "tradizionali" si mostrano perpetrabili in rete[6],

[1] Dottore di ricerca in Scienze Giuridiche, Assegnista di ricerca in procedura penale, Università di Bologna.

[2] Reg. UE/679/2016, sia alla Dir. UE/680/2016, nonché agli atti interni correlati, ossia il D.lgs 101/2018 e il 51/2018. Il *Considerando* n. 3 della Dir. UE/680/2016 rammenta come «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della raccolta e della condivisione di dati personali è aumentata in modo significativo. La tecnologia […] consente il trattamento di dati personali nello svolgimento di attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati […]».

[3] Reg. UE/2019/881, nell'ambito della più ampia e complessa Cybersecurity strategy dell'Unione. Sul punto, R. BRIGHI e P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in Federalismi, n. 21/2021, p. 18 ss. Si pensi, in un contesto più ampio, anche alla Convenzione sulla criminalità informatica di Budapest, del 2001.

[4] GU n. 234, 30/09/2021, D.L., n. 132, in seguito a Grande sezione della Corte di giustizia dell'Unione europea, sentenza 2/03/2021, C-746/18.

[5] Si pensi alla legge n. 547/1993 e poi l. 48/2008.

[6] Relegare l'approfondimento ai soli reati informatici (si vedano quelli introdotti e/o modificati dalle leggi 547/1993 e 48/2008: frode informatica; accesso abusivo a un sistema informatico; detenzione e diffusione abusiva di codici di accesso a sistemi; diffusione di hardware e

ove più alta è l'esposizione del singolo nel web o nelle *app* di messaggistica istantanea, maggiori sono gli scenari e gli orizzonti applicativi della *digital forensics*[7]. La rete è luogo di condivisione e restituisce una mole imprecisata di informazioni, alcune utili ai fini preventivi, investigativi e d'accertamento.

Su questo fronte, numerosi sono gli ambiti ove possono essere spese le conoscenze informatiche e i dati reperiti per tale via. Questi, peraltro, sono assistiti da una presunzione di infallibilità dal tratto suadente per gli attori del processo[8]. È opportuno precisare come, nel far generico riferimento all'uso di detti dati, si intenda effettuare il più ampio richiamo sia soggettivo sia oggettivo. Si intende cioè riferirsi sia alla più ampia gamma di atti e momenti della procedura in cui il tema può inserirsi (indagini, incidente cautelare, mezzi di ricerca della prova, giudizio), sia ad ogni attore processuale.

È necessario rinnovare il dibattito su di un bilanciamento fra i valori in gioco, specie in ambito investigativo, fra aspettative tutte legittime: necessità d'accertamento da un lato, diritti e prerogative della difesa dall'altro.

Il presente capitolo tenterà di rispondere proprio ai quesiti in punto di acquisizione e utilizzazione processuale dei dati digitali prodotti dall'utilizzo di alcune applicazioni, specie *social network* e di messaggistica istantanea (quali *Telegram* o *Whatsapp*). Infine, si volgerà lo sguardo alle prospettive future in ordine all'implementazione dell'utilizzo dei metodi investigati tesi ad assicurare questo tipo di dati, con l'intento di tracciare un'ideale linea dei necessari bilanciamenti fra i diritti e le legittime aspettative in gioco.

2. *Digital forensics* e processo penale: delicati equilibri

Come noto, la *digital forensics* si occupa del trattamento di dati digitali al precipuo scopo di ricavarne elementi di prova utili all'attività inve-

software diretti a danneggiare sistemi; etc.) varrebbe a menomare la ricerca di ambiti di non minore importanza.

[7] Il termine *digital forensics* è qui utilizzato come sinonimo di informatica forense, V. R. Brighi, *Sfide recenti e nuovi paradigmi per l'informatica forense.*

[8] Si veda per questo F. Caprioli, *Tecnologia e prova penale: nuovi diritti e nuove garanzie,* in L. Luparia-L. Marafioti-G. Paolozzi (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019, p. 45 ss.

stigativa o prove spendibili davanti al giudice del merito. La formazione di questa "prova informatica" segue alcune fasi fondamentali: identificazione, raccolta, acquisizione, analisi, valutazione, presentazione[9]. Il materiale probante di cui si parla può essere tuttavia alterato o distrutto da gestioni e analisi improprie, di qui la centralità del tema delle modalità di acquisizione. La l. 48 del 18 marzo 2008, di ratifica della Convenzione di Budapest del 2001, esprime numerose volte la necessità che nelle operazioni di apprensione dei dati debbono essere adottate «le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[10].

La stessa legge è intervenuta sulle attività d'indagine di polizia giudiziaria. Specie in epoche coeve alla riforma, si è posto l'interrogativo circa la qualificazione di siffatte attività d'indagine. Il dubbio ha riguardato se fosse o meno il caso di ricondurle sotto l'ombrello normativo degli accertamenti tecnici irripetibili, attorniati da speciali cautele visto la propensione immediatamente probatoria del *materiale*. Sotto questo versante, è stato fatto notare come il tipo d'attività che pretende un'indagine informatica meglio si concilierebbe con l'accertamento tecnico in ragione dei rischi che questi dati digitali siano manipolati; ciò imporrebbe «un'urgenza […] di verificare caso per caso l'eventuale utilità di una cristallizzazione del risultato probatorio attraverso lo strumento dell'accertamento tecnico irripetibile»[11]. L'*evidenza digitale* esulerebbe dalle conoscenze dell'uomo medio e richiederebbe l'apporto di specifiche conoscenze e competenze, *ex* artt. 359 e 360 c.p.p.[12]

L'approccio non s'è visto sinora sposato dalla giurisprudenza, che ha invece avuto modo di precisare come «[n]on rientr[i] nel novero degli atti irripetibili l'attività di estrazione di copia di "file" da un computer […] non […] determina alcuna alterazione dello stato delle cose […]

[9] R. Brighi e M. Ferrazzano, *Digital forensics: best practices and perspective,* in M. Caianiello e A. Camon (a cura di), *Digital forensic evidence towards common european standards in antifraud administrative and criminal investigations*, p. 35 ss., Wolters Kluwer 2021. V., su tutto, standard ISO 27037.

[10] In via esemplificativa, art. 8 l. 48/2008, che interveniva sull'art. 244 co. 2 c.p.p. in tema di ispezioni. Uguali intendimenti sono rinvenibili per le perquisizioni e i sequestri. Si modificava poi l'art. 491 *bis* c.p., *Documenti informatici*, atto a sanzionare le falsità in documenti informatici dal valore probatorio.

[11] L. Luparia, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in Luparia-Ziccardi*, Investigazione penale e tecnologia informatica,* Giuffrè, 2007, p. 152 ss; si veda anche M. Daniele, *La prova digitale nel processo penale,* in Riv. dir. proc., 2011, p. 292.

[12] Ogni ulteriore riferimento normativo senza indicazione di fonte va riferito al c.p.p.

nella prospettiva dibattimentale, essendo […] assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale»[13]. Depone in questo senso anche la scelta assunta dal legislatore del 2008, che interviene in tema di attività d'indagine di polizia, rappresentando *per tabulas* che in questa sede vadano ricercati i diritti della difesa: non nella propensione probatoria del dato, bensì nei presupposti e nelle procedure utilizzate per la sua apprensione[14]. Potrebbe contro argomentarsi invocando una precisa specializzazione in tal senso. Argomento astrattamente valido, non tanto da superare la previsione legislativa esistente nell'art. 348, co. 4: la polizia giudiziaria, quando compie atti od operazioni che richiedono specifiche competenze tecniche, può avvalersi di persone idonee. La letteratura ha potuto interessarsi più volte della differenza intercorrente tra "persone idonee" e "consulenti"[15], laddove con i primi si individuano degli esperti nella tecnica (es: estrazione di file), con i secondi persone dotate di specifiche conoscenze scientifiche. Non è opinabile che esistano e vadano implementandosi corpi operativi con precipue specializzazioni in tal senso, si pensi al ruolo della polizia postale sul versante della repressione di condotte criminose attuate in rete[16].

La conclusione deve essere tuttavia meglio ponderata. Al netto dell'orientamento rinvenibile nel diritto vivente[17], questo non si spinge così in là dal rinnegare in principio il bisogno di affidarsi alle maggiori guarentigie offerte dagli accertamenti tecnici irripetibili. Se di per sé

[13] Cass. Pen., Sez. I, 05/03/2009, n.14511, con nota E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto passando per la copia*, in Cass. pen., fasc. 4, 2010, pag. 1522 ss.; ovvero Cass. Pen., Sez. II, sent. 4-16/06/2015, n. 24998.

[14] L'avanzare della tecnologia non cesserà di riproporre la questione dell'inquadramento di queste indagini. La raccolta di elementi indiziari comporta una certa disamina dei dati attenzionati (quelli prodotti dall'utilizzo di *social network* o app di messagistica istantanea su dispositivi connessi in rete). Deve pervenirsi a un dato informatico spendibile dal punto di vista giuridico e ciò comporta attività di tipo deduttivo.

[15] R. KOSTORIS, *I consulenti tecnici nel processo penale*, Giuffrè, 1993, p. 139 ss.; ovvero F. Giunchedi, *Accertamenti* tecnici, in Dig. d. pen., vol. VII, Utet, 1993, p. 2: «L'indicazione di "persone idonee" in un caso, e "consulenti" dall'altro, disvela differenze non trascurabili [...] Il consulente molto spesso opera sui dati raccolti dalla polizia giudiziaria e dai suoi esperti». V. anche Amato-D'Andria, *Organizzazione e funzioni della polizia giudiziaria nel nuovo codice di procedura penale*, Milano, 1990; D'Ambrosio-Vigna, *La pratica di polizia giudiziaria*, p. 50 ss., Padova, 1998.

[16] Si veda il *Report 2020 della Polizia Postale: in aumento le minacce e le truffe sul web. +436% segnalazioni di fakenews*. Si vedano sul punto i preziosi spunti, anche comparati, in R. BRIGHI e M. FERRAZZANO, *Digital forensics: best practices and perspective,* cit., p. 24 ss., Wolters Kluwer 2021.; ovvero, stessa fonte, L. BARTOLI e G. LASAGNI, *The handling of digital evidence in Italy,* p. 87 ss.

[17] Si dica "permissivo" e di cui si darà conto nel prosieguo.

l'attività di estrazione files da dispositivi può non porre questioni di competenza, ciò non significa che queste non possano emergere. Alle volte l'esperimento dell'accertamento non può essere replicato. La categoria degli accertamenti tecnici (quindi anche irripetibili) è dinamica e segue l'evolversi del progresso tecnologico. Non sfugge da questa sorte neppure l'accertamento informatico[18]. La polizia è chiamata ad assicurare l'adempimento d'ogni operazione di repertazione così da preservare la replicabilità della stessa. Questo è l'approccio da applicare anche agli accertamenti urgenti di polizia di cui all'art. 354, co. 2, riferito proprio ai dati informatici[19].

Si comprende, quindi, la peculiare attenzione rivolta alle *best practices*[20] del settore. Sul punto si è mostrata a quel tempo innovativa la l. 48/2008. Gli artt. 8 e seguenti l. cit. manifestano tutti un intendimento: debbono essere adottate misure tecniche necessarie ad assicurare i dati e ad impedirne alterazioni[21].

Il legislatore si astiene dall'individuare le singole operazioni ritenute conformi alle migliori tecniche avvalorate dalla comunità scientifica. Si pone in un'ottica di risultato: le operazioni debbono rassicurare circa la provenienza e l'integrità dell'evidenza digitale, non sono posti specifici adempimenti procedurali[22]. Vale una regola finalistica: devono essere fatti salvi i caratteri originali dell'evidenza digitale.

[18] Si guardi per la ricostruzione dell'istituto a Cass. Pen., Sez. Un., 18/12/2006, n. 41281.

[19] S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in Giur. merito, fasc.4, 2013, pag. 0955B ss, ove è detto «[l]e operazioni urgenti che possono compiere gli ufficiali di P.G. di fronte ad un elemento di prova digitale devono cercare di essere […] operazioni materiali e tecniche di conservazione del dato nella sua integrità […]. Ove ciò non fosse tecnicamente possibile ci si troverebbe di fronte ad una attività tipicamente irripetibile».

[20] L'insieme di procedure avvalorate dalla comunità scientifica e utili al fine di individuare, rilevare, acquisire, conservare una evidenza digitale. Pur dando atto di come il legislatore non abbia indicato dettagliatamente le singole modalità d'esecuzione, si è comunque focalizzata l'attenzione su due basilari aspetti: la correttezza della procedura di copia dei dati e la loro integrità e non alterabilità in sede di acquisizione. V. G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. Lupária (a cura di), *Sistema penale e criminalità informatica,* Giuffrè, Milano, 2009; ovvero R. BRIGHI, C. MAIOLI*, Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologia*, Informatica e Diritto, 2016, XXIV, pp. 217 - 23.

[21] V. art. 354, co. 3, c.p.p., come modificato dalla l. 48/2008.

[22] «In proposito è necessario […] precisare […] che non è compito del giudicante determinare una sorta di protocollo […], ma solo verificare se nella fattispecie l'acquisizione probatoria sia fidefaciente, o se abbia subito alterazioni», Corte App. Bologna, II Sez. Pen. sentenza 30/01/2008 (dep. 27/03/2008). *Leitmotiv* già proprio della sentenza di primo grado, Trib. Bologna, sentenza n. 1823 del 21/07/2005.

Ciò conduce ad alcuni quesiti: quale sanzione per il mancato rispetto delle *best practices*? Quali sono le regole di utilizzabilità (*lato sensu*) della *digital evidence*? Come vengono contemperati i diritti e le legittime aspettative della difesa?

Si tornerà sui quesiti, tuttavia è il caso di esplicitare il dilemma dinanzi al quale è posto l'interprete. Come fatto notare[23], non è codificata una sanzione per il mancato rispetto delle migliori procedure di acquisizione[24]. Tuttavia, preme considerare come gli strumenti sanzionatori propri del codice di rito non necessitano obbligatoriamente di una espressa previsione sul punto. Prerogative irrinunciabili, quali quelle attinenti al rispetto del contradditorio nella formazione della prova e alla necessità di preservare lo spazio della difesa non impediscono di ricondurre certe violazioni a sanzioni processuali quali la nullità o l'inutilizzabilità. A dispetto dell'apparente linearità delle osservazioni che precedono, vedremo un diritto vivente alle volte distante dagli assiomi e dai dogmi cui dovrebbe votarsi. Osservarne lo stato contribuirà a tracciare l'ideale orizzonte nella materia trattata.

3. I molteplici usi delle evidenze digitali

L'attività di indagine informatica posta in essere dalla *digital forensics* ambisce ad esplorare la più vasta gamma di strumenti, hardware, dispositivi mobili[25] e traffico telematico sui diversi sistemi connessi in rete. Il versante attiguo è quello delle eventuali sanzioni processuali irrogabili nei

[23] Fra gli altri, D. La Muscatella, *La ricerca della prova digitale e la violazione delle best practices: un'attività investigativa complessa tra recenti riforme e principi consolidati,* in Ciberspazio e Diritto, n. 2, 2011, p. 222, ma anche M. Tonellotto, *Evidenza informatica, computer forensics e best practices,* in Rivista di Criminologia, Vittimologia e Sicurezza – Vol. VIII – N. 2 – Maggio-Agosto 2014.

[24] Sanzione invece espressamente comminata per il caso della perizia ex art. 224 *bis* c.p.p. L'espletamento di questa impone un preciso vaglio di ammissibilità del mezzo e sono molteplici gli adempimenti imposti dalla legge processuale, posti sotto la scure della nullità (cfr. art. 224 *bis*, co. 2, c.p.p.).

[25] Ambito delicato in ragione della intrinseca complessità e peculiarità della *mobile forensics*, ossia quel ramo della *digital forensics* impegnata nel reperimento di evidenze digitali dai dispositivi mobili (es: *smartphone*). Aspetti quali la varietà dei sistemi operativi; condivisione di dati in cloud; maggiori rischi di alterazione dei dati; svariati meccanismi di autenticazione pongono continue sfide nel campo dell'apprendimento dei dati da siffatti dispositivi. V., fra gli altri, A. Zareen e S. Baig, *Mobile Phone Forensics: Challenges, Analysis and Tools Classification,* in Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on. IEEE. 2010; A. Hoog, *Android forensics: investigation, analysis and mobile security for Google Android*. Elsevier, 2011.

casi in cui non siano adoperate tecniche idonee a garantire ognuno degli attori processuali della bontà delle operazioni poste in essere[26].

I noti casi *Vierika*[27] o l'omicidio di Garlasco[28] hanno a loro tempo posto alla prova la giurisprudenza, tesa a puntellare questo tipo di materiale probante secondo il reticolato di garanzie offerte dal codice di rito. Dopo questi, altre volte il diritto vivente ha avuto modo di interessarsi del tema, specializzandosi in ragione del singolo accertamento attenzionato. Per esigenze di scrittura non sarà possibile intraprendere la più ampia analisi della molteplicità degli orientamenti espressi in ragione di singole evidenze digitali. Ci si limiterà qui ad esplorare i soli profili prossimi al reperimento di informazioni utili su *social network* o su *app* di messaggistica istantanea. Con questi orizzonti verranno di seguito analizzati singoli lembi giurisprudenziali, proiettando, ove necessario, l'analisi verso i futuribili impieghi della *digital evidence.*

3.1. *Delle devianze condivise in rete: nuovo oggetto di indagine?*

Il riferimento a recenti fatti di cronaca può valere alla questione dibattuta. Si pensi ad alcune cc.dd. fronde no-vax balzate di recente agli onori delle cronache, alcune attenzionate in ragione di elementi di allarme emersi e raccolti proprio a seguito di indagini nate e sviluppatesi quasi esclusivamente su canali *Telegram*[29]. La tipologia di indagine

[26] Si veda, fra gli altri, F. M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.,* fasc.3, 2013, pag. 1259B, in nota 1 si rammenta come «[u]n'attività di indagine informatica, quella posta in essere dalla *digital forensics*, che ambisce ad esplorare la più vasta gamma di strumenti, hardware, dispositivi mobili […] pone con urgenza il tema delle metodologie più idonee al reperimento di questi dati. Il versante immediatamente attiguo è quello delle eventuali sanzioni processuali irrogabili […]».

[27] Trib. Bologna, 22/12/05, n. 1823. V. L. Lupária, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova digitale. I profili processuali*, in dir. Internet, 2006, p. 153 ss.

[28] V. Trib. Vigevano, sent. 17 dicembre 2009 e la sentenza conclusiva della Corte di Cassazione, V Sez. Penale, n. 257/2016 (dep. 21.06.2016). Il caso di Garlasco, specie la sentenza di primo grado resa a cavallo della modifica normativa occorsa con l. 48/2008, si interroga della sussistenza di un alibi informatico, per così dire. In quel caso costituito dall'utilizzo del pc personale dell'imputato. In quella vicenda si giunse ad affermare come le attività sul pc effettuate dagli inquirenti che lo avevano in custodia finirono col danneggiare la gran parte (circa i ¾) dei materiali ivi contenuti.

[29] Si vedano, *Blitz della polizia contro no vax: preparavano uso di armi nei cortei, tra indagati 5 "guerriere*", di A. PALMA, FanPage, al link: https://www.fanpage.it/attualita/ perquisizioni-contro-i-no-vax-in-tutta-italia-in-chat-parlavano-di-violenze-nei-cortei/; *Le minacce in chat dei No Vax: "Facciamo saltare i camion tv"* di Ilaria Carra, Luca De Vito, su Repubblica, al link https://www.repubblica.it/cronaca/2021/09/10/news/le_minacce_in_chat_dei_no _vax_ facciamo_saltare_i_camion_tv_-317153680/.

adottata costituisce l'epifenomeno più noto di una modalità investigativa invalsa da tempo[30]. Gli inquirenti hanno negli anni intensificato le indagini di questo tipo al fine della repressione di fenomeni terroristici transnazionali[31], pornografia, o episodi di cessione di sostanze stupefacenti[32], per citarne alcuni.

Evidenze digitali cui si ha di regola accesso attraverso il sequestro[33] degli smartphone degli indagati, con conseguente estrapolazione (su supporti cartacei) delle conversazioni occorse su *Whatsapp* o *Telegram*, ovvero accedendo ai profili *social* in uso agli interessati[34].

È evidente: una volta acquisiti, questi materiali possono essere spesi nelle più disparate sedi processuali. Il multiforme impiego, tuttavia, non deve far desistere da una attenta analisi circa la legittimità di una loro spendita processuale.

Il tema passa sovente in sordina, velocemente ricondotto all'alveo della prova documentale (art. 234 c.p.p.). Eppure, specie in ragione della fisiologica avversione verso il contraddittorio di questo mezzo di prova, converrebbe una approfondita analisi. La giurisprudenza di legittimità ha espresso orientamenti ondivaghi, spesso tesi a fare salva la prova. Assumono tratti dirimenti affermazioni quali

> L'estrazione di dati archiviati in un supporto informatico non costituisce accertamento tecnico irripetibile anche dopo l'entrata in vigore della L. 18 marzo 2008, n. 48, che ha introdotto unicamente l'obbligo per la polizia giudiziaria di

[30] Si veda, fra gli altri, F. CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e inviolabilità dei diritti della persona*, in *Riv. It. Dir. Proc. Pen*., n. 2/2021, p. 499 ss.

[31] Si guardi la recente Cassazione penale sez. V, 18/12/2020, (ud. 18/12/2020, dep. 04/03/2021), n.8891. Si veda poi M. DANIELE, *Contrasto al terrorismo e captatori informatici*, in *Riv. Dir. Proc*., 2017 p. 393 ss.

[32] Si veda Cass. Pen., Sez. IV, 07/02/2019, n.16030.

[33] Di certo interesse la recente circolare della Procura Generale di Trento, al link Nota-a-PG-Cass-e-PG-CA-per-sequestro-chat.pdf (penaledp.it), con commento di L. Filippi, *Sequestro dispositivi elettronici: nota della Procura Generale di Trento*, in Penale Diritto e Procedura, 22/11/2021, al link sequestro-dispositivi-elettronici-nota-della-procura-generale-di-trento.pdf, ove è trattata la necessità di affidarsi al principio di proporzionalità nell'apprensione fisica dei dispositivi mobili utile all'estrazione di file digitali. Circa il principio di proporzionalità, si veda, fra gli altri, M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, Riv. Trim. Dir. pen. cont 3–4/2014, p. 143; ovvero F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, Dir. pen. cont., 8/01/2018, https://www.penalecontemporaneo.it/upload/9279-nicolicchia2018a.pdf..

[34] Si veda, G. LASAGNI, *Tackling phone searches in Italy and in the US. Proposals for a technological re-thinking of procedural rights and freedoms*, in NJECL, 2018, 9, p. 386 ss.

> rispettare determinati protocolli di comportamento, senza prevedere alcuna sanzione processuale in caso di mancata loro adozione […].
> Si è recentemente ritenuto che i fotogrammi scaricati dal sito internet "Google Earth", costituiscano prove documentali pienamente utilizzabili ai sensi dell'art. 234 c.p.p., comma 1 o art. 189 c.p.p. […].
> Qualunque documento legittimamente acquisito è soggetto alla libera valutazione da parte del giudice ed ha valore probatorio, pur se privo di certificazione ufficiale di conformità e pur se l'imputato ne abbia disconosciuto il contenuto[35].

> I messaggi e le chat whatsapp prodotte nel contesto di un processo penale, anche attraverso semplice screenshot, costituiscono documenti ai sensi dell'art. 234 c.p.p., in quanto la captazione di messaggi e chat rappresenta una forma di documentazione di una conversazione ex post, e non in corso, e quindi sfugge alla disciplina delle intercettazioni o delle semplici registrazioni e ha valore di prova documentale[36].

> I dati informatici (Sms, messaggi WhatsApp, messaggi di posta elettronica scaricati o conservati nella memoria) rinvenuti in un telefono cellulare sottoposto a sequestro hanno natura di documenti ai sensi dell'art. 234 c.p.p., con la conseguenza che la relativa acquisizione non soggiace né alle regole stabilite per la corrispondenza, né tantomeno alla disciplina delle intercettazioni telefoniche[…][37].

Il complesso delle affermazioni riportate non può essere acriticamente condiviso. L'acquisizione poco disciplinata di materiale di questo tipo non può essere consentita "fino a prova contraria"[38]. Alcuni dubbi e perplessità si mostrano in particolare (e solo) quando i documenti si vedano disconosciuti dagli imputati, approdo tuttavia irrispettoso del rito prescelto. Come lascia intendere il legislatore del 2008,

[35] Cass. Pen., Sez. V, 16/01/2018, n. 8736.
[36] Cass. pen. Sez. V, 10/03/2021, n. 17552.
[37] Cass. pen. Sez. V, 21/11/2017, n. 1822.
[38] V. Cass. Pen., Sez. VI, 06/02/2020, n.12975, che afferma «[i]n tema di prove, la copia estratta da un documento informatico ha la medesima valenza probatoria del dato originariamente acquisito, salvo che se ne deduca e dimostri la manipolazione». Nel corpo della sentenza: «i messaggi di posta elettronica […], costituiscono meri documenti informatici intesi in senso "statico", dunque acquisibili ai sensi dell'art. 234 c.p.p., dovendo escludere che si possa parlare di documentazione relativa a flussi informatici: termine quest'ultimo che, attenendo ad una trasmissione in atto, indica in una concezione "dinamica" lo scambio di comunicazioni che avviene in maniera telematica o informatica tra apparecchi posti a distanza, che, in quanto tale, soggiace alla diversa e più rigorosa disciplina processuale delle intercettazioni di comunicazioni o conversazioni […]». V. anche Cass. Pen., Sez. III, 05/07/2012, n. 37419. Fra gli altri, Marafioti, *Digital evidence e processo penale,* in Cass. Pen. n. 12/2011, 2011, 4509B; Plantamura, *La tutela penale delle comunicazioni informatiche e telematiche,* in Dir. inform., fasc. 6/2006, 2006, 847.

occorre che siano gli organi impegnati nelle indagini a dare prova di averle attuate nel rispetto delle garanzie della difesa, non il contrario.

Si aggiunga che gli orientamenti giurisprudenziali citati evitano di proporre una soluzione definitiva al quesito inerente all'eventuale sanzione processuale conseguente a una irresponsabile apprensione di dati. Il tema della mancanza di una previsione tassativa si mostra miope. È pur vero che di fianco alle auspicate tecniche atte a preservare integrità e autenticità del dato non v'è una espressa comminatoria sanzionatoria, vero pure che ciò non basta a fare salvo ogni deficit acquisitivo riconducendolo alla irregolarità processuale. La teoria poggia sul filone interpretativo che colloca nelle irregolarità processuali quelle afferenti al mancato rispetto delle *leges artis* quando non recepite da norme di rango primario; ciò che può accadere nel caso dell'ascolto di minori senza il rispetto degli standard psico-forensi in uso (V. Carta di Noto[39]).

Meritano un cenno le sanzioni dell'inutilizzabilità e le nullità. La prima, disciplinata all'art. 191 opera allorquando «[l]e prove [siano] acquisite in violazione dei divieti stabiliti dalla legge»[40]. L'espressione è sì ampia, ma non del tutto chiarificatrice in ordine al tipo di divieto la cui violazione farebbe derivare la sanzione. In letteratura si ritiene che «per riconoscere un divieto, sono determinanti la *ratio* della norma e il rapporto fra violazione ed interesse protetto [ovvero] che i divieti probatori derivano […] da una lesione di diritti fondamentali […] che pone l'atto al di fuori del sistema e reclama una sanzione radicale»[41]. Nel caso di specie v'è margine per sostenere il ricorrere della sanzione processuale[42].

[39] Cass. Pen., Sez. III , 13/01/2021 , n. 24121.

[40] I riferimenti in materia sarebbero molteplici. Si guardi, fra gli altri, E. Amodio, *Fascicolo processuale e utilizzabilità degli atti*, in Aa.Vv., *Lezioni sul nuovo processo penale*, Giuffrè, 1990; F. M. Grifantini, *Art. 191*, in *Commentario breve al codice di procedura penale*, diretto da G. Conso e G. Illuminati, 2a ed., Cedam, 2015, p. 694; A. Scella, voce *Inutilizzabilità della prova (diritto processuale penale)*, in *Enc. dir., Annali* II, tomo I, Giuffrè, 2008, p. 486 ss.

[41] A. Camon, *Le prove*, in (a cura di) A. Camon; M. Daniele; D. Negri; C. Cesari; M. L. Di Bitonto e P. P. Paulesu, *Fondamenti di Procedura Penale*, Cedam 2019, p. 302 ss.; si vedano poi F.M. Grifantini, voce *Inutilizzabilità*, in *Dig. pen.*, vol. VII, Utet, 1993, p. 348; Cass., Sez. un., 27 marzo 1996, Sala, in *Cass. pen.*, 1996, p. 3268 s.; G. Pierro, voce *Inutilizzabilità degli atti (proc. pen.)*, in *Dizionario di diritto pubblico*, diretto da S. Cassese, vol. IV, Giuffrè, 2006, p. 3252 s.

[42] Neppure può essere scarsamente considerato il tema delle cc.dd. prove incostituzionali, vale a dire quelle acquisite in violazione di situazioni giuridiche soggettive garantite dalla Costituzione. Non potendosi in questa sede riprendere il dibattito attorno al tema, valgano alcuni spunti. In effetti si è già avuto modo di far notare come nella categoria dell'inutilizzabilità si debbono ricomprendere le prove formate o acquisite in violazione dei diritti soggettivi tutelati in modo specifico dalla Costituzione. Nel contesto qui sotto esame, si pensi agli artt. 14 e 24

Nel 2008 si è imposto agli operanti di garantire la genuinità del dato digitale raccolto. Seppur non esplicitate le singole operazioni, queste nei fatti trovano riferimento nelle diverse norme di rango primario, quale è il codice di procedura penale. Il difetto, nel richiamo, è figlio dell'impossibilità di dettare regole univoche per ognuno dei molteplici e indefiniti accertamenti informatici che possono porsi in essere. Valga una deduzione banale. Nel 2008 non erano neppure diffusi (certo non come adesso) gli *smartphone*. Si accedeva ai *social network* dai pc domestici, non si aveva la possibilità di condividere attimo per attimo la propria vita *online*. Oggi sì. Ebbene, il legislatore non ha dettato regole precise per l'apprensione di evidenze digitali dagli *smartphone* in termini diversi rispetto a quelle dettate per l'acquisizione dei dati da un pc. In entrambi i casi deve essere fatto salvo il risultato: l'evidenza deve risultare corrispondente all'originale e le procedure debbono essere ripetibili. Neppure pare corretto auspicare una specializzazione così acuta del codice da individuare e predeterminare ognuno dei possibili accertamenti informatici. L'evoluzione della tecnica si incaricherebbe di dichiararne l'inadeguatezza.

Non appare in linea con le direttrici ordinamentali tentare di ovviare al problema affidandosi al libero convincimento del giudice. Egli è sì libero, ma nell'ambito di un compendio probatorio costituito da prove tutte utilizzabili e non il contrario. Sono i canoni di utilizzabilità a delimitare i confini del libero apprezzamento[43].

Nell'ambito attenzionato, quello inerente alla captazione di chat di messaggistica istantanea, pare venire in rilievo anche il tema delle intercettazioni. In via di esemplificazione, se gli inquirenti "fotografano" conversazioni occorse su *Whatsapp* apprendono del contenuto di esse e, quindi, potrebbe ritenersi utile affidarsi alla serie di norme in tema di intercettazioni, tra cui l'art. 266 *bis.* Se l'aggancio riuscisse varrebbe a

Cost. Nel primo caso trattasi di libertà assoluta, di cui è consentita una limitazione solo nei casi e nei modi previsti dalla legge. La difesa, poi, è dichiarata inviolabile. Il punto di ricaduta è quindi l'inviolabilità di alcune situazioni giuridiche dovrebbe imporre, anche nella materia *de qua*, un'analisi più approfondita e tesa alla salvaguardia di valori irrinunciabili per il rito. Si veda Cass. Pen., Sez. Un., 13/07/1998, n. 21; Corte cost. n.34 del 1973. V. anche A. Camon, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove "incostituzionali"*, in Cass. pen. 1999, p. 1188.

[43] Non senza tacere che la lesione al diritto di difesa, al diritto di potere intervenire in concreto nel procedimento che si produrrebbe all'imputato potrebbe sorreggere conclusioni argomentative tese a sostenere il ricorrere di una nullità generale assoluta vertente sulla prova assunta coi difetti di cui s'è trattato.

superare ogni ritrosia circa il ricorrere di eventuali sanzioni processuali. I presupposti di questa attività tipica di ricerca della prova andrebbero ricercati negli artt. 266 e ss. e il mancato rispetto renderebbe inservibile il materiale probante appreso.

In giurisprudenza, però, s'è andato diffondendo un filone interpretativo oggi prevalente teso a disconoscere in capo ai messaggi appresi dagli inquirenti la fattispecie delle intercettazioni[44]. Il dato dirimente sul punto verrebbe a collocarsi nel tempo della captazione. L'intercettazione pretende la cognizione di conversazioni contemporanee all'atto di captazione. Se così è, i messaggi di posta elettronica o *Whatsapp* o *Telegram* presenti sui dispositivi costituiscono meri documenti informatici perché "statici", dunque documenti ex art. 234[45].

L'art. 266 *bis* verrebbe quindi ad essere relegato alle ipotesi in cui si capti una conversazione (anche messagistica) che occorre contemporaneamente all'attività di captazione, ovvero siccome trattasi di conversazioni in essere su applicazioni quali *Skype* o *Teams* o simili.

Su di un diverso versante, viene poi pure ritenuto inoperante l'art. 254 in quanto questo prevede una corrispondenza da apprendere presso terzi[46].

[44] Si veda Cass. Pen., Sez. IV, 8/05/2003 n. 3435 o, più di recente, Cass. Pen., Sez. VI, 27.11.2018, n. 14395, questa in tema di captazione di comunicazioni in chat protette per mezzo del sistema *pin to pin* e sull'applicazione denominata *Blackbarry Messanger*.

[45] V. Cass. Pen., Sez. V, 21/11/2017, n.1822, «[n]on è applicabile la disciplina dettata dall'art. 254 c.p.p. con riferimento a messaggi WhatsApp e SMS rinvenuti in un telefono cellulare sottoposto a sequestro, in quanto questi testi non rientrano nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito».

[46] La questione meriterebbe ulteriori riflessioni. Non si ignori come le interpretazioni della Cassazione poggiano su di un dato normativo che non ha saputo adeguarsi ai tempi. Occorrerebbe un intervento legislativo che chiarisca ove ricondurre l'apprensione di dati contenuti sui dispositivi sotto sequestro, invece che fomentare il proliferare di attività di indagine atipiche e così incidenti su valori sovralegali, quale i diritti di libertà di cui in Costituzione. Come notato da G. Illuminati, *Libertà e segretezza della comunicazione*, in Cass. Pen., fasc.11/2019, pag. 3826 ss., «[p]rima dell'approvazione della riforma, […] [s]enza entrare nei dettagli, possiamo ricordare che nell'articolato si differenziavano le varie operazioni eseguibili: osservazione dei dispositivi e acquisizione dei dati da remoto, intercettazione tra presenti, intercettazione di comunicazioni cifrate, geolocalizzazione. Si indicavano presupposti, condizioni e procedure specifiche, con il limite invalicabile del rispetto della dignità umana e personale, nonché garanzie di immodificabilità e di conformità dei dati raccolti […]». Linea che si condivide: urge una presa di coscienza legislativa. L'art. 254, co. 3, tuttavia fornisce qualche utile spunto di riflessione. Si riferisce ad un principio di proporzionalità e pertinenza nel discoprimento di corrispondenza altrui: ciò che non è sequestrabile deve essere immediatamente restituito all'avente diritto ed è comunque inutilizzabile.

Sotto questo ultimo versante, la giurisprudenza si è di recente mostrata attenta in ragione di alcune riflessioni imposte dalla normativa sulla *privacy* (Dir. 680/2016/UE e D.lgs 51/2018).

Allo stato dell'attuale giurisprudenza, frastagliata e refrattaria ad alcune istanza che pure paiono legittime e visto l'attuale stato della legislazione, certo perfettibile, svuotare di contenuto quei riferimenti alle tecniche idonee a rassicurare della bontà delle operazioni di apprensione dei dati digitali vale a svuotare di spirito la l. 48/2008. Deve permanere la *ratio* avanguardista a tratti perseguita dalla novella. Un'attività che non sappia certificare la correttezza delle sue stesse procedure non deve poter trovare alcun uso processuale: non nella fase cautelare, non a dibattimento.

Al contrario, pure al netto delle difficoltà definitorie, potrà essere utilmente spesa. E così, nella fase cautelare di già si rinvengono diverse affermazioni tese a spendere le attività sui *social* ai fini ricostruttivi delle esigenze cautelari. Non è raro imbattersi in pronunce che ritengano di potere trarre utili elementi dalla vita degli imputati per come condivisa su *Facebook* o *Instagram*[47].Così pure nell'affermazione della penale responsabilità, l'attività sui *social* può guidare il giudice, anche ai fini commisurativi della pena (ex art. 133 c.p.). Non solo contro l'imputato, ovviamente, ma pure a suo vantaggio. L'alibi o un'attenuante possono del pari essere reperite nelle evidenze digitali di cui si discute. Le conoscenze acquisite in internet invece non sono riconducibili al *notorio,* quindi non sono spendibili in camera di consiglio all'atto di decidere[48].

Limitando i cenni a quegli utili a desumere lo spazio da assegnare al valore della riservatezza nel rito penale, basti osservare come anche in questo contesto sono garantiti diversi diritti agli interessati in ordine alla correttezza del trattamento dei loro dati (idoneità, necessarietà, proporzione in senso stretto. V. artt. 3; 5; e il Capo II del D.lgs 51/2018, nonché D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo,* in *Riv. ut. dir. proc. pen.,* 2020, 3 ss.). Anche nell'ambito del trattamento dei dati personali, operato per le finalità di repressione dei reati, non è ammessa un'indiscriminata eccedenza dei mezzi utilizzati in virtù del solo fine perseguito e proprio sull'estrazione di dati custoditi su dispositivi informatici sotto sequestro si è interessata la Cassazione. V. Cass. Pen., Sez VI, n. 34265/2020, nota di M. PITTIRUTI, *Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus,* in Sistema Penale, al link Sequestri informatici: un vademecum della Cassazione | Sistema Penale | SP. V. anche nota 33. Per una proposta metodologica si veda il contributo di M. FERRAZZANO, L. SUMMA, *La selezione di dati informatici in ambito giudiziario*: prassi e modalità operative.

[47] Si veda Cass. Pen., Sez. IV, 09/01/2018, n. 6539. Certo, il dato così appreso e utilizzato non fa venire meno la necessità si rispettino gli altri doveri motivazionali del giudice. Dovranno essere elementi concreti e attuali.

[48] Cass. Pen., sez. I, 20/05/2016, n.36315.

3.2 *Sul versante opposto: la produzione privata di conversazioni*

Parrebbero destinate ad allargarsi le maglie della giurisprudenza alle prese con l'ammissibilità di conversazioni su *app* di messaggistica o sui *social network* esibite da privati.

Non occorre sottovalutare questo dato. Non sempre si giunge a sequestro nei procedimenti penali e poi v'è l'ampio capitolo delle pretese civilistiche dentro il rito penale e, non meno importante, quello delle indagini difensive. Per diverse ragioni le parti possono avere interesse a produrre conversazioni *Whatsapp* o pagine estrapolate da *social network*.

In virtù degli artt. 237 e 239 parrebbero maggiori le possibilità di fare entrare nel rito anche il materiale probatorio cui ci si riferisce. Non sempre è così. La Cassazione ha di recente assunto atteggiamenti rigorosi[49], subordinando la trascrizione dei messaggi *Whatsapp* prodotti dall'imputato all'acquisizione del supporto contenente la conversazione, essendo necessario controllare l'affidabilità della prova medesima. L'orientamento era riferito ad una fattispecie in cui si tentava di produrre una chat asseritamente dimostrativa della scarsa credibilità della persona offesa. Per le volte in cui si dovesse cercare di produrre una chat occorsa con terze persone potrebbe invero farsi affidamento al forse più rudimentale ma non smentito strumento del riconoscimento ex art. 239.

L'utilizzo privato è tutt'altro che marginale. Si pensi a reati quali gli atti persecutori (c.d. *stalking*) oramai di diffusa consumazione a mezzo di messaggi o tramite post sui *social*[50]. Il pensiero può pur andare ad alcuni reati che si consumano in contesti famigliari, come gli omessi versamenti degli assegni di mantenimento (art. 570 *bis* c.p.). Il nodo spesso passa nella possibilità o meno, del "debitore", di versare quanto a lui imposto. In contesti siffatti, una pagina *social* ricca di costose esperienze può validamente guidare il giudice sia come indizio sia per commisurare l'eventuale pena[51].

[49] Si veda Cass. Pen., Sez. V, 19/06/2017, n. 49016, commento a cura di R. De Cocco, *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali,* su Processo penale e giustizia, fasc. n. 3/2018, reperibile al link http://www.processopenaleegiustizia.it/whatsapp-normative-avanguardie-giurisprudenziali.

[50] Cass. Pen., sez. V, 31/03/2021 , n. 19363 «il reato di stalking può essere commesso anche a mezzo di messaggi e comunicazioni diffusi tramite i social-media (nella specie, Facebook) […]». E ancora, Tribunale Milano, sez. uff. indagini prel. , 08/03/2019 , n. 336 «In tema di atti persecutori sussiste l'aggravante di aver commesso il fatto con il mezzo telematico vi siano contatti attraverso profili Facebook». Si pensi anche alla diffamazione a mezzo Facebook. Fra le tante, Cass. Pen., Sez. V , 04/03/2021 , n. 11426; 25/01/2021 , n. 13979.

[51] Si veda Trib. Bologna, inedita, 15/12/2020, n. 3954.

L'utilizzo di s*creen* di pagine *social* e di conversazioni su app di messaggistica è sempre più diffuso in ambito processuale, eppure va sottolineata l'impostazione della giurisprudenza citata in quanto subordina l'utilizzabilità della chat alla verifica sull'attendibilità della fonte. Preoccupazione certo legittima, risulta però dissonante che simile rigore sia applicato verso l'imputato, che gode della copertura offerta dall'art. 237[52] e non anche quando si discuta degli esiti di accertamenti investigativi informatici atipici. Ove, cioè, è pure lecito aspettarsi la disponibilità di maggiori mezzi e risorse da parte degli inquirenti, sicché più grave dovrebbe risultare il vizio per le volte in cui non si assicuri la genuinità della produzione d'accusa. O ancora nei confronti delle altre parti coinvolte nel rito, che pure possono contare a dibattimento (come ogni parte del resto) sul ricorso al sistema del riconoscimento. Vale la pena segnalare come non sempre sia così, emergendo casi in cui alcuni *screen* estrapolati dai *social* siano stati utilizzati sia per fondare l'accertamento di penale responsabilità sia per commisurare, ai sensi dell'art. 133 c.p., la pena[53].

4. Conclusioni

In conclusione, la disamina delle questioni sul tappeto dà modo di comprendere di come la materia sia in costante evoluzione. Gli sforzi del legislatore del 2008 sovente non conducono al rigore applicativo che si sarebbe atteso. Sotto questo versante è pur vero, tuttavia, che un ulteriore intervento chiarificatore varrebbe a superare definitivamente alcuni dubbi oggi persistenti in giurisprudenza: quale peso dovrebbero assumere le *best practices*?

Si sostiene che esse, per quanto aperte, valgano a fare salvo un risultato: dovrebbero assumere dignità solo quegli accertamenti idonei a rassicurare circa la bontà delle operazioni. Indagini sui *social* o su app di messaggistica coltivate con pressapochismo debbono essere definitivamente relegate in soffitta, senza potersi affidare al salvagente offerto dal libero convincimento (e non arbitrio) del giudice.

Con questa consapevolezza, gli accertamenti informatici, di sempre maggiore diffusione, varranno come supporto alle attività investigative. Senza, assolveranno pur sempre a questo scopo, con minore rispetto

[52] In base al quale è comunque consentita l'acquisizione dei documenti provenienti dall'imputato.
[53] V., *supra*, nota 48.

della serie di diritti e legittime aspettative che gravitano attorno al rito. Gli ultimi indirizzi di legittimità citati[54] possono valere come utile guida per più consapevoli riflessioni future circa l'utilizzabilità degli esiti di indagini digitali sui *social network* e su app di messaggistica istantanea.

[54] V. nota 49.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643014
pp. 261-280 (gennaio 2022)

Tecniche di *digital forensics* nelle pratiche di concorrenza sleale su piattaforme di *advertising online*: il caso di *Google AdWords*

VINCENZO COLAROCCO[1], MICHELE FERRAZZANO[2]

1. Elementi del marketing online: banner, SEO, digital advertising

È difficile fornire una definizione univoca di cosa è il *marketing online*, ma è certo che aziende e professionisti non possano trascurarlo, perché Internet è entrato a pieno nelle nostre vite. I consumatori – o più in generale gli utenti finali, considerando anche il mercato *business to business* – si aspettano che qualsiasi azienda abbia un canale digitale attivo. Una buona strategia di comunicazione digitale si poggia prevalentemente su siti web, canali social ed *email marketing*: l'utente viene intercettato sulla base di scelte precedenti proponendo il nome dell'azienda, con l'obiettivo di acquisire il cliente anche nel lungo termine.

Il *web marketing* è identificabile come un insieme di strumenti applicati ad una strategia per raggiungere e massimizzare gli obiettivi di business di un'azienda, primo fra tutti la vendita dei propri beni e servizi. Il web marketing si propone di individuare i canali sui quali investire tempo e risorse, definire le campagne di comunicazione, convertire utenti interessati (o anche non) in clienti, fidelizzarli.

Nell'ambito del *marketing online* esistono, dunque, diverse modalità di promozione. Per *Digital Adv* si intende qualsiasi messaggio pubblicitario comunicato attraverso le piattaforme del mondo digitale, che include motori di ricerca, *social network* e tutti i siti della rete Internet.

[1] Cultore della materia di Informatica Giuridica e Informatica forense, Università di Bologna; Avvocato in Roma.
[2] Professore a contratto di *Computer forensics*, Università Statale di Milano, e di Informatica, Università degli Studi di Modena e Reggio Emilia*; Digital Forensics Expert.*

I due strumenti principalmente utilizzati per la pubblicità *online* sono i *banner online* e l'ottimizzazione del sito web rispetto alle ricerche degli utenti.

Un *banner* è un'immagine o altro tipo di formato multimediale, ovvero semplicemente un testo, utilizzato per proporre una pubblicità online allo scopo di promuovere un marchio e per ottenere visitatori a seguito di click su di esso. L'obiettivo basilare dei *banner* è infatti raccogliere click dagli utenti per portarli sul sito pubblicizzato all'interno di una pagina appositamente realizzata (detta "*landing page*") allo scopo di convertire i visitatori in clienti (c.d. *lead*).

L'ottimizzazione del sito web si occupa di migliorare la posizione delle pagine web nei risultati organici (non sponsorizzati) dei motori di ricerca, attività nota più spesso sotto il nome di SEO (*Search Engine Optimization*). Si tratta di un insieme di strategie e pratiche volte ad aumentare la visibilità di un sito con lo scopo di migliorarne la posizione nella classifica di risultati dei motori di ricerca: queste pratiche sono molteplici e riguardano diversi aspetti di un sito web, dall'ottimizzazione della struttura del sito e del codice HTML alla riscrittura dei contenuti testuali, dalla gestione dei *link* in entrata alle *performance* del server utilizzato. Spesso la SEO è direttamente associata a Google in quanto è il motore di ricerca più utilizzato al mondo, pertanto, le tecniche di ottimizzazioni si basano sull'analisi del suo algoritmo di indicizzazione.

Dunque, da un punto di vista infrastrutturale, ogni sistema di digital advertising si basa sul rapporto di – almeno – tre soggetti: una parte che vuole sponsorizzarsi; una parte che pubblica l'annuncio; una parte che raccoglie le richieste di sponsorizzazioni dei primi e organizza la pubblicazione sui canali dei secondi. Questo schema può prevedere più livelli di intermediari, ovvero chi raccoglie le richieste di sponsorizzazione e chi pubblica potrebbe coincidere, come nel caso della pubblicità sui motori di ricerca come Google.

2. La pubblicità sui motori di ricerca

La differenza tra pubblicità (attraverso annunci pubblicitari o *banner*) e SEO è fondamentale in una strategia di *marketing online*: mentre le pubblicità testuali o con *banner* prevedono delle forme di pagamento (generalmente per numero di visualizzazioni o per numero di click, talvolta in base alle conversioni), la SEO è "gratuita" nella misura in

cui la posizione apicale di classifica raggiunta non deve essere remunerata al motore di ricerca. Al contrario, la pubblicità prevede sempre forme di pagamento, per quanto la valorizzazione può variare nel tempo, in base alle parole chiave oggetto di sponsorizzazione, al settore merceologico, al sito e alla posizione in esso sul quale compare la pubblicità, alla quantità di concorrenti che competono con la medesima, o analoga, strategia di web markeging. Quando finisce il budget, si smette di pubblicare pubblicità.

L'ottimizzazione del posizionamento in SEO richiede a sua volta un costo, ma legato alle risorse umane e di eventuali strumenti software di supporto che lavorano per migliorare la considerazione del sito – o, meglio, delle sue pagine – da parte del motore di ricerca, ma una volta raggiunto un certo posizionamento sarebbe possibile interrompere la manutenzione per mantenere comunque, per un periodo più o meno lungo, il risultato raggiunto in termini di visibilità.

In linea di massima, comunque, a parità di utenti che raggiungono il sito di destinazione, il costo di acquisizione di utenti via banner è nettamente superiore all'equivalente costo legato alla SEO.

Fatta questa premessa per comprendere e chiarire gli ambiti del web marketing, si passa nel proseguo della presente trattazione a rilevare quali possano essere le attività illecite connesse al mondo del *webmarkeing* e, in particolare, a quanto concerne le attività di concorrenza sleale, spesso basate su un utilizzo illecito di marchi.

3. Le violazioni nell'uso di strumenti di *digital advertising*

Vale la pena ricordare che per ogni parola chiave (o *keyword*) inserita in un motore di ricerca vengono generalmente forniti due tipi di risultati: 1) gli annunci pubblicitari relativi a taluni siti che compaiono in quanto gli inserzionisti pagano il gestore affinché, in risposta a determinate parole chiave, vengano presentati i riferimenti ai loro siti; 2) i risultati organici, ossia una serie di risorse del web che il motore di ricerca rileva come pertinenti, forniti in base a criteri determinati dall'algoritmo di indicizzazione e frutto dell'ottimizzazione lato SEO.

Si noti a scopo esemplificativo il seguente stralcio di risultati mostrati dal motore di ricerca Google a fronte della *keyword* "informatica forense" (Fig. 1).

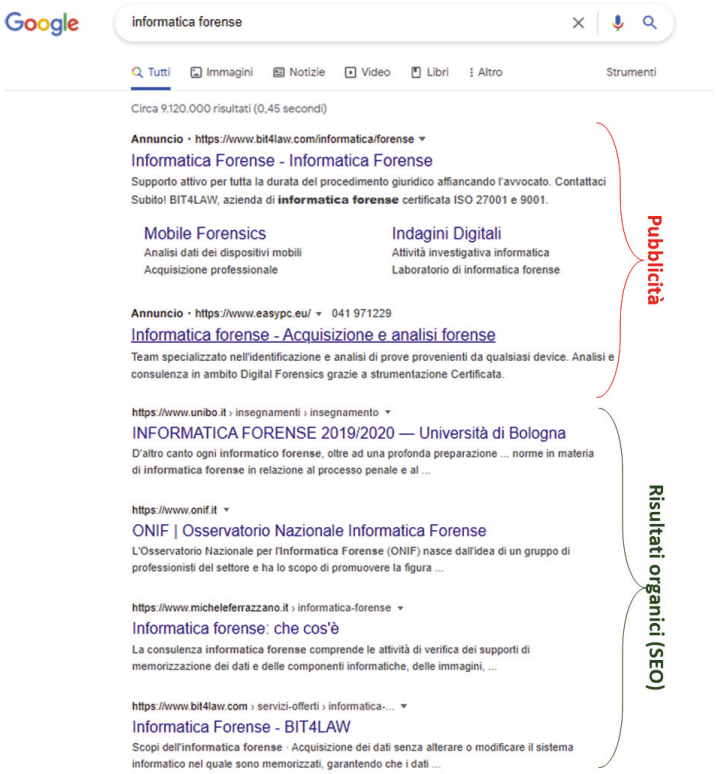


Figura 1. Esempio di risultato di ricerca: in alto gli annunci pubblicitari (caratterizzati dal testo "Annuncio"; in basso i risultati organici.

I risultati ottenuti dal punto di vista della SEO si basano principalmente sui termini contenuti nelle pagine, pertanto è raro – ma non impossibile – riscontrare attività di concorrenza sleale che prevedono un utilizzo di parole chiave riconducibili a marchi di concorrenti in quanto sarebbero immediatamente rilevabili dal soggetto che subisce la violazione. Al contrario, i risultati ottenuti tra gli annunci sponsorizzati possono essere veicolati sulla base di qualsiasi parola chiave che l'azienda ritiene utile, compresi termini totalmente estranei al settore di operatività o nomi di marchi altrui. Per questo motivo, la maggior parte di violazioni rilevanti dal punto di vista dell'utilizzo illecito di marchi in ambito di web marketing avviene proprio nell'ambito della pubblicità a pagamento basata su parole chiave definite dall'inserzionista.

Ne consegue che le aziende possono attivare dei monitoraggi delle parole chiave associate ai propri marchi al fine di rilevare violazioni. Laddove si riscontrassero delle violazioni, anche e soprattutto a causa dell'elevata volatilità di dette evidenze digitali, la prima attività da svolgere, come insegna la sequenza di fasi dell'informatica forense, è l'acquisizione forense degli annunci pubblicitari.[3]

Nel caso di Google, il servizio di acquisto di annunci pubblicitari è denominato "*AdWords*"[4]. AdWords consente a qualsiasi inserzionista di pianificare delle campagne pubblicitarie sulla base di alcuni parametri (tra cui periodo temporale, tipologia di browser e dispositivo, area geografica). Nell'ambito della campagna pubblicitaria è possibile selezionare una o più parole chiave al fine di far apparire, fra i risultati di una ricerca comprendente tali *keywords*, un *link* pubblicitario caratterizzato dalla parola "Annuncio" per distinguerlo dai risultati organici.

Tale *link* pubblicitario è accompagnato da un breve messaggio commerciale che, insieme al *link*, costituisce l'annuncio che appare nella già menzionata rubrica (Fig. 2).

Figura 2. Esempio di annuncio pubblicitario su Google.

L'inserzionista, ossia chi ha intenzione di pubblicizzare il proprio sito fra i risultati dell'operazione di ricerca attivata dall'utente, paghe-

[3] Giova precisare che comunque le medesime considerazioni valgono anche per i risultati della SEO: si consideri ad esempio il caso di un e-commerce che, pur non avendo accordi di vendita di prodotti di teterminati marchi, sviluppa pagine *ad hoc* al fine di catturare i clienti alla ricerca di quei *brand*, rispondendo con una pagina che informa l'utente che quel prodotto è terminato (in realtà, non è mai disponibile) e proponendo marchi concorrenti.

[4] La descrizione del servizio *AdWords* è rinvenibile al seguente indirizzo telematico: *https://ads.google.com/intl/it_it/home/a*. Servizi analoghi sono forniti anche da altri motori di ricerca, come ad esempio il servizio *Ads* di *Bing*, il motore di ricerca di Microsoft.

rà a Google tale servizio di posizionamento per ogni selezione (cioè ogni click) del proprio link pubblicitario (c.d. *pay per click*).

La stessa parola chiave può essere chiaramente selezionata da più inserzionisti (si pensi ad esempio per le pubblicità correlate a un termine generico, come ad esempio "automobile sportiva"). In tal caso, l'ordine di visualizzazione dei diversi *link* è determinato da algoritmi che sulla base di vari criteri (prezzo per click, visite precedenti, disponibilità di budget…) determina quale annuncio, e quindi sito, far apparire e in quale ordine, determinando di fatto un sistema di asta online per l'acquisto della *keyword* desiderata. La selezione di parole chiave e la relativa creazione di annunci avviene attraverso un processo automatizzato supportato da Google, mediante il quale gli inserzionisti selezionano le parole chiave, redigono il messaggio commerciale e inseriscono il *link* al loro sito Internet[5]. Tuttavia, è pratica non infrequente nel mercato del *digital advertising* l'acquisto di *keyword* corrispondente al marchio registrato di titolarità di un soggetto terzo, sì da determinare un alto rischio di confusione per i consumatori nell'individuazione del prodotto desiderato.

4. La digital forensics per il contrasto alle violazioni nel *digital advertising*

La prova a sostegno dei fatti dedotti in giudizio in un contenzioso di questa tipologia risiede nella pagina web del motore di ricerca in cui si è verificato l'evento. In particolare, la prova dell'illecito risiede nelle pagine web del motore di ricerca Google a fronte delle parole chiave inserite, tenendo conto eventualmente dell'indirizzo IP di provenienza (laddove la pubblicità sia destinata solo ad alcune aree geografiche) e del browser (laddove la pubblicità sia destinata, ad esempio, solo a dispositivi mobile piuttosto che computer). Infatti è tramite interrogazione del motore di ricerca che il sistema AdWords interroga la propria banca dati sulla base delle richieste di pubblicità e dei budget residui e propone gli annunci pertinenti, sulle base delle logiche del proprio algoritmo.

[5] Cfr. Corte di Giustizia UE, Sentenza della Corte (Prima Sezione) del 22.9.2011, causa *Interflora Inc*. e *Interflora British Unit* contro *Marks & Spencer plc* e *Flowers Direct Online Ltd*. (punti 9-13) e sentenza del 23.3.2010, *Google France SARL* e *Google Inc.* contro *Louis Vuitton Malletier SA* (punti 22-27).

La possibilità di acquisire dati di annunci pubblicati a fronte di specifiche parole chiave tramite acquisizione di pagina web non presenta alcun genere di criticità, atteso che tali riscontri sono pubblicamente disponibili. Tuttavia non permettono di raccogliere elementi utili a misurare la portata del fenomeno, ossia a quale possa essere – almeno indicativamente – il budget messo in campo dal concorrente.

Ulteriori elementi utili a questi scopi potrebbero essere acquisiti dal pannello di controllo dell'inserzionista, accessibile dietro inserimento di sue credenziali. All'interno del pannello, oltre a poter definire le proprie campagne, Google fonisce indicazione dei principali siti web competitor sulle parole chiave utilizzate: tali informazioni rappresentano un forte elemento indiziario nei confronti dei concorrenti in quanto fornisce anche una stima degli annunci mostrati in termini percentuali, potendo così misurare anche il budget utilizzato dalla controparte.

In Figura 3 si mostra un esempio di riscontro rispetto alle informazioni sulle aste da cui sono riportati nella prima colonna tutti gli altri siti che competono sulle medesime parole chiave: se la parola chiave è quindi il marchio, è possibile avere precise indicazioni su quali siti competono utilizzando illecitamente il marchio altrui e quante volte compare il relativo annuncio pubblicitario.

Informazioni aste

Dominio dell'URL di visualizzazione	↓ Quota impressioni	Percentuale di sovrapposizione	Tasso di posizionamento superiore	Tasso parte superiore della pagina	Tasso ass. parte superiore della pagina	Quota superamento target
Tu	56,67%	–	–	88,50%	61,21%	–
Sito A	30,81%	36,50%	6,56%	83,12%	4,48%	55,31%
Sito B	25,72%	31,46%	0,69%	45,07%	0,24%	56,55%
Sito C	19,62%	23,05%	94,90%	95,04%	88,44%	44,27%
Sito D	15,39%	19,66%	7,77%	47,19%	4,53%	55,80%
Sito E	14,39%	17,41%	3,49%	63,79%	2,40%	56,32%
Sito F	< 10%	6,18%	5,25%	50,22%	2,48%	56,49%
Sito G	< 10%	6,35%	0,64%	33,56%	0,27%	56,65%
Sito H	< 10%	7,29%	16,51%	56,14%	14,10%	55,99%
Sito I	< 10%	6,23%	0,65%	5,42%	0,29%	56,65%

1 - 10 di 10

Figura 3. Pannello di controllo AdWords relativo ai concorrenti che sono in asta sulle medesime parola chiave.

In questo altro esempio, invece, emerge che la parola chiave non è utilizzata da altri concorrenti, ottenendo come unico risultato (si noti dettaglio 1 di 1 in basso a destra) le performance del proprio sito.

Informazioni aste

Dominio dell'URL di visualizzazione	↓ Quota impressioni	Percentuale di sovrapposizione	Tasso di posizionamento superiore	Tasso parte superiore della pagina	Tasso ass. parte superiore della pagina	Quota superamento target
Tu	66,67%	–	–	100,00%	100,00%	–

1 - 1 di 1

Figura 4. Pannello di controllo AdWords relativo all'assenza di concorrenti in asta sulle medesime parola chiave.

Data la natura volatile del dato digitale rinvenuto in Internet, appare evidente che tutti questi dati devono, dunque, essere raccolti in maniera idonea dalle pagine web di competenza, attraverso delle procedure che assicurino integrità e autenticità delle prove digitali, lasciando possibilità di verifica ai terzi interessati.

In tema di produzione di pagine web come prove, nelle aule di Tribunale si assiste frequentemente alla mera produzione cartacea della stampa *screenshot* della pagina web, ritenendo detta allegazione idonea a provare in giudizio il fatto lesivo dei propri diritti. Tale metodologia è stata ritenuta non sufficiente ed inidonea sia nel panorama giurisprudenziale italiano[6], sia nelle regole definite nello standard ISO/IEC 27037. Sotto un profilo giuridico, si segnala come la Corte di Appello di Milano, con la recente sentenza n. 225 depositata il 22.1.2021 ha ritenuto idonea la garanzia fornita dalle tecniche di informatica forense che non si limitano ad archiviare gli *screenshot* delle pagine web ma che «sono in grado di replicare l'intero codice HTML delle pagine archiviate, conservando elementi caratterizzanti quali l'URL (...), la data, il tipo di codifica della pagina web». La stessa corte meneghina ha, peraltro, richiamato l'orientamento giurisprudenziale dello stesso tenore formatosi negli Stati Uniti[7].

[6] In merito si veda Cass. Civ., Sez. 6, 12.9.2012, 15307; Cass. Civ., Sez. 6, 20/03/2012, 4455; Trib. Bari, Sez. 2 23/01/2012, 250; Trib. Milano, 23/12/2011, 15519; Cass., Sez. lav., 08/11/2011, 23173; Trib. Roma, Sez. 9, 22/04/2008, n.8481; Trib. Roma, Sez. 3 25/03/2008, 6376; Trib. Bari, Sez. 4. 11/06/2007.

[7] Cfr.*United District Court for the Eastern District of Pennsylvania, case n. 05-3524, Healthcare Advocates vs. Harding Earley, Follmer & Frailey et. al*. del 20 luglio 2007; *Unit-*

La giurisprudenza anche più recente, pertanto, incoraggia l'utilizzo delle tecniche di informatica forense anche in ambito processualcivilistico, affinché vengano estratti adeguatamente i dati presenti nelle pagine web, cristallizzati in copie forensi che consentono di documentare integrità dei dati, non manipolazione e certezza temporale, rendendo la copia forense prodotta immodificabile e tendenzialmente vincolante per il giudicante.

Per l'acquisizione di pagina web esistono oggigiorno degli strumenti che facilitano l'apprensione delle stesse che però soffrono di alcune limitazioni tecniche (ad esempio, il vincolo di presentarsi al sito web con l'indirizzo IP del provider di macchine virtuali su cui poggia il servizio). In letteratura esistono comunque anche indicazioni su modalità operative di acquisizione di pagina web attraverso strumenti open source come, ad esempio, il sistema operativo Linux, il software di acquisizione di traffico di rete Wireshark e il browser Mozilla Firefox[8].

La procedura di acquisizione forense di pagine web può così essere descritta:

1. utilizzo di una macchina virtuale con installato un sistema operativo Linux di tipo forense;
2. avvio di una procedura di registrazione audio e video delle operazioni eseguite, utili allo scopo di riprodurle in maniera "semplice" e comprensibile anche in assenza di sistemi informatici per la verifica o per semplicità nei confronti del giurista;
3. avvio di una procedura di intercettazione del traffico di rete generato dalla macchina virtuale durante le attività di navigazione, utile per acquisire non solo i singoli file scaricati dal browser, ma anche le richieste e le risposte complete dai vari webserver contattati e per documentare in maniera inequivocabile gli indirizzi IP coinvolti;
4. consultazione di un sito dal quale poter documentare la data di inizio dell'acquisizione (ad esempio, l'*homepage* di un quotidiano online);

ed States District Court for the District of Kansas, case n. 14-2464-JWL, Marten Transport Ltd vs. Plattform Advertising Inc. del 29 aprile 2016

[8] Cfr. M. Ferrazzano, V. Colarocco, *La pagina web come prova digitale nel processo civile*, in C. Maioli (a cura di), Questioni di informatica forense, Aracne, 2015, pag. 239-262.

5. consultazione di tutte le pagine da acquisire utilizzando una procedure di consultazione manuale delle pagine di interesse o di strumenti per acquisizione di porzioni di sito in maniera automatica;
6. consultazione di un sito dal quale poter documentare la data di fine dell'acquisizione (ad esempio, l'homepage di un quotidiano online);
7. chiusura della procedura di intercettazione del traffico di rete;
8. chiusura della procedura di registrazione audio e video;
9. spegnimento della macchina virtuale;
10. generazione di un archivio compresso contenente i file della macchina virtuale, il file della registrazione audio-video, il file di traffico di rete, i singoli file delle pagine web;
11. calcolo dell'hash dell'archivio compresso prodotto al punto precedente;
12. applicazione di marca temporale all'hash calcolato al punto precedente.

Considerate le variabili utilizzate dai motori di ricerca per la promozione degli annunci, per meglio documentare l'estensione del fenomeno, ossia cercare di determinare le variabili prese in esame dall'algoritmo di Google che provvede alla pubblicazione degli annunci e la durata della campagna pubblicitaria, l'acquisizione forense andrebbe eseguita non solo *una tantum*, ma più volte (ad esempio con cadenza giornaliera o settimanale, in giorni e orari diversi), così da poter dedurre quali sono le logiche impostate dall'azienda nel pannello di AdWords.

La documentazione del comportamento del motore di ricerca a fronte delle parole chiave utilizzate – e in particolare all'uso del marchio, eventualmente combinato ad altre parole – è alla base della successiva azione stragiudiziale o giudiziale.

Nel momento in cui viene avviato un procedimento giudiziario, in caso di successivo accertamento tecnico da parte di un Consulente Tecnico d'Ufficio del Giudice, ad esempio nelle more di un accertamento tecnico preventivo ex art. 696 c.p.c., la verifica dovrà riguardare la configurazione del pannello di controllo dell'inserzionista all'interno della piattaforma pubblicitaria e in particolare l'elenco delle parole chiave impostate, l'elenco delle parole chiave negative, l'elenco delle parole chiave ricercate effettivamente dagli utenti che hanno generato l'annuncio. In altri termini, lo scopo dell'accertamento

tecnico è quello di raccogliere dati digitali che rappresentino riscontri puntuali a sostegno o smentita delle considerazioni del ricorrente. Questo ultimo punto è di estremo rilievo in quanto può accadere che l'inserzionista acquisti pubblicità con un termine generico (ad esempio "auto sportiva") per poi comparire con il proprio annuncio quando a quelle parole chiave viene associato il nome di un marchio di un concorrente (ad esempio "auto sportiva XXX", dove XXX è il nome del marchio).

Per questo motivo, è riduttivo limitarsi ad esaminare le sole parole chiave esplicitamente impostate in quanto, specialmente in alcuni contesti, è frequente che l'utente cerchi l'accoppiata di parole chiave <termine generico> assieme a <marchio noto>.

Inoltre, questo punto è rilevante in quanto permette di comprendere quanti utenti, dunque clientela, in termini assoluti e percentuali, viene acquisita dall'inserzionista, elemento utile per basare successive valutazioni in tema di lucro cessante e danno emergente.

5. La giurisprudenza in materia di uso del marchio nel digital advertising

5.1. *L'orientamento della Corte di Giustizia dell'Unione Europea*

La Corte di Giustizia[9] che sull'interpretazione dell'art. 5 della Direttiva 89/104 ("Prima direttiva 89/104/CEE del Consiglio del 21 dicembre 1988 sul ravvicinamento delle legislazioni degli Stati Membri in materia di marchi d'impresa") e l'art. 9 del Regolamento n. 40/94 (sulle modalità di esecuzione del regolamento (CE) n. 40/94 del Consiglio sul marchio comunitario) ha stabilito che il titolare di un marchio può vietare ad un inserzionista di fare pubblicità – a partire dall'utilizzo di una keywords identica al proprio marchio, selezionata dall'inserzionista senza il consenso dello stesso titolare – a prodotti o servizi identici a quelli per cui detto marchio è registrato «qualora l'annuncio del terzo adombri la sussistenza di un collegamento economico tra tale

[9] Con sentenza dell'8.3.2017, il Tribunale di Firenze ha condiviso l'orientamento della CGUE affermando che «vi era violazione del marchio dell'attore con una lesione alla sua funzione identificativa, oltre ad un illecito concorrenziale»; e ancora il Tribunale di Milano, con sentenza del 22.4.2016 n. 40348/13 richiamando i principi europei ha ravvisato «una violazione della funzione d'origine del marchio Remail da parte di un concorrente che la utilizzava come parola chiave nel sistema AdWords».

terzo e il titolare del marchio» oppure nel caso in cui esso «sia talmente vago sull'origine dei prodotti o dei servizi in questione che un utente di Internet normalmente informato e ragionevolmente attento non sia in grado di sapere, sulla base del link pubblicitario e del messaggio commerciale allegato, se l'inserzionista sia un terzo rispetto al titolare del marchio o, al contrario, sia economicamente collegato a quest'ultimo».

In particolare, è nota la sentenza della Corte di Giustizia UE, nel caso *Interflora* contro *Marks & Spencer* (C-323/09), relativo all'utilizzo da parte della convenuta, della keyword "Interflora" per posizionare un annuncio di consegna di fiori a domicilio, senza riportare il marchio Interflora nel testo dell'annuncio. La Corte ha chiarito che:

> il titolare di un marchio ha il diritto di vietare ad un concorrente di fare pubblicità – a partire da una parola chiave identica a detto marchio che tale concorrente, senza il consenso del titolare del marchio, ha scelto nell'ambito di un servizio di posizionamento su Internet – a prodotti o servizi identici a quelli per i quali tale marchio è stato registrato, quando il predetto uso è idoneo a violare una delle funzioni del marchio.

Secondo quanto indicato dalla Corte, un tale uso vìola la funzione di indicazione d'origine del marchio allorché la pubblicità che compare a partire dalla suddetta parola chiave non consente o consente solo difficilmente all'utente di Internet normalmente informato e ragionevolmente attento di sapere se i prodotti o i servizi menzionati nell'annuncio provengano dal titolare del marchio o da un'impresa economicamente collegata a quest'ultimo oppure, al contrario, da un terzo; nonché viola la funzione di investimento del marchio ove intralci l'utilizzo, da parte del titolare in questione, del proprio marchio per acquisire o mantenere una reputazione idonea ad attirare i consumatori e a renderli fedeli. La Corte adita statuisce poi che:

> il titolare di un marchio che gode di notorietà ha il diritto di vietare ad un concorrente di fare pubblicità a partire da una parola chiave corrispondente a tale marchio che il suddetto concorrente, senza il consenso del titolare del marchio, ha scelto nell'ambito di un servizio di posizionamento su Internet, qualora detto concorrente tragga così indebitamente vantaggio dal carattere distintivo o dalla notorietà del marchio (parassitismo) oppure qualora tale pubblicità arrechi pregiudizio a detto carattere distintivo (diluizione) o a detta notorietà (corrosione).

Pertanto, la Corte di Giustizia si è espressa sulla illiceità nell'acquisto a fini pubblicitari di *keywords* che arrecano pregiudizio al carattere distintivo del marchio, contribuendo a trasformare la natura di tale marchio rendendolo un termine generico.

Quanto nello specifico al *keyword advertising*, la base normativa di riferimento per determinare la sussistenza della violazione dei diritti di esclusiva del titolare del marchio da parte dell'inserzionista che – senza il consenso del titolare – ha utilizzato una parola chiave coincidente sono, come anticipato, l'art. 5, n. 1 e 2, della Direttiva n. 2008/95/CE e l'art. 9 del Regolamento CE n. 40/94, oltre agli artt. 20 e 21, del Codice di Proprietà Industriale[10]. Tali norme, autorizzano i titolari di marchi a vietare a terzi l'uso di segni identici o simili per prodotti identici o simili a quelli per i quali tali marchi sono stati registrati.

Sull'utilizzo *keyword advertising*, oltre a quanto sino ad ora analizzato, si è espressa plurime volte la Corte di Giustizia dell'Unione Europea, riaffermando i medesimi principi che possono considerarsi oramai cristallizzati: *i*) l'inserzionista che sceglie, come parola chiave in un servizio di posizionamento, una *keyword* identica al marchio di un concorrente che ha per oggetto e per effetto la visualizzazione di un link pubblicitario verso il sito sul quale l'inserzionista mette in vendita i propri prodotti, «fa uso del segno identico al marchio nel commercio se si colloca nel contesto di un'attività commerciale finalizzata a un vantaggio economico e non nell'ambito privato»[11];

[10] La norma sancisce che: «i diritti del titolare del marchio d'impresa registrato consistono nella facoltà di fare uso esclusivo del marchio» e nel diritto «di vietare ai terzi, salvo proprio consenso, di usare nell'attività economica: a) un segno identico al marchio per prodotti o servizi identici a quelli per cui esso è stato registrato; b) un segno identico o simile al marchio registrato, per prodotti o servizi identici o affini, se a causa dell'identità o somiglianza fra i segni e dell'identità o affinità fra i prodotti o servizi, possa determinarsi un rischio di confusione per il pubblico, che può consistere anche in un rischio di associazione fra i due segni; c) un segno identico o simile al marchio registrato per prodotti o servizi anche non affini, se il marchio registrato goda nello stato di rinomanza e se l'uso del segno senza giusto motivo consente di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o reca pregiudizio agli stessi». L'art. 21 c. 2 sancisce poi il divieto di «usare il marchio in modo contrario alla legge, né, in specie, in modo da ingenerare un rischio di confusione sul mercato con altri segni conosciuti come distintivi di imprese, prodotti o servizi altrui, o da indurre comunque in inganno il pubblico, in particolare circa la natura, qualità o provenienza prodotti o servizi, a causa del modo e del contesto in cui viene utilizzato, o da ledere un altrui diritto di autore, di proprietà industriale, o altro diritto esclusivo di terzi». *Cfr*. sentenze C-236/08 del 23.3.2010, C- 206/01 del 12.11.2002, C-487/07 del 18.6.2009, C-17/06 del 11.9.2007. nonché. CGUE, Sez. 3, del 11.9.2013, C-657/11; CGUE, Sez. 5, 11.4.2019, C-690/17.

[11] Corte di Giustizia CE, Sez. Grande, 23.3.2010, Sentenze C-236/08 a C-238/08, punto 52 (cause riunite Google France SARL e Google Inc. c. Louis Vuitton Malletier SA (C-

ii) l'uso "commerciale", come sopra inteso, vi è anche nel caso in cui, attraverso l'uso del segno identico al marchio come parola chiave, l'inserzionista «non miri a presentare i propri beni agli utenti di Internet come un'alternativa rispetto ai beni del titolare del marchio ma, al contrario, intenda indurre in errore gli utenti di Internet sull'origine dei propri prodotti e servizi, lasciando loro credere che gli stessi provengano dal titolare del marchio o da un'impresa economicamente legata a quest'ultimo»[12]; iii) sussiste una violazione «quando l'annuncio non consente o consente soltanto difficilmente all'utente di Internet normalmente informato e ragionevolmente attento di sapere se i prodotti o i servizi a cui l'annuncio si riferisce provengano dal titolare del marchio o da un terzo»[13]; iv) è indebito il vantaggio ricavato da terzi che si inseriscono nella scia di un marchio che gode di notorietà «al fine di beneficiare del suo potere attrattivo, nonché al fine di sfruttare, senza qualsivoglia compensazione economica, lo sforzo commerciale effettuato dal titolare del marchio per creare e mantenere l'immagine di detto marchio (c.d. parassitismo)»[14].

Dunque, il titolare del marchio può opporsi all'uso di un segno identico al marchio se tale uso è «idoneo a compromettere una delle funzioni del marchio in questione» e fra dette funzioni «è da annoverare non solo la funzione essenziale del marchio consistente nel garantire ai consumatori l'origine del prodotto o del servizio (la 'funzione di indicazione di origine'), ma anche le altre funzioni del marchio, segnatamente quella di garantire la qualità del prodotto o del servizio di cui trattasi, o quelle di comunicazione, investimento o pubblicità»[15].

236/08), Google France SARL c. Viaticum SA e Luteciel SARL (C-237/08), Google France SARL c. Centre national de recherche en relations humaines (CNRRH) e altri (C-238/08), CGUE, sez. I, 22.9.2011, n.323, C-323/09.

[12] Corte di Giustizia CE, Sez. Grande, 23.3.2010, sentenze C-236/08 a C-238/08, punto 72 e Corte di Giustizia CE, sentenza 11.9.2007, causa C-17/06, Céline, punto 23, CGUE, Sez. 1, 22/09/2011, n.323, C-323/09.

[13] Corte di Giustizia CE, Sez. Grande, 23.3.2010, sentenze C-236/08 a C-238/08, punto 84 e Corte di Giustizia CE, sentenza 11.9.2007, causa C-17/06, Céline, punto 27.

[14] Corte di Giustizia CE, Sez. Grande, 23.3.2010, sentenze C-236/08 a C-238/08, punto 102 e Corte di Giustizia CE, sentenza del 18.6.2009, L'Oréal e a. (C-487/07) punto 49.

[15] Corte di Giustizia CE, Sez. Grande, 23.3.2010, sentenze C-236/08 a C-238/08, punti 49 e 77 e Corte di Giustizia CE, sentenza del 18.6.2009, L'Oréal e a. (C-487/07) punto 58.

5.2. *L'orientamento dei Tribunali italiani*

Anche la giurisprudenza nazionale è intervenuta in questioni relative all'utilizzo di marchi altrui come *keywords* del servizio *AdWords*, ritenendo, in generale, che l'uso del marchio di un terzo come parola chiave nell'ambito di un servizio di posizionamento su Internet costituisce violazione del marchio se ne compromette una delle funzioni tipiche del marchio stesso e generi confusione nella clientela[16].

In particolare, il Tribunale di Genova con ordinanza del 5 settembre 2018, ha dichiarato che:

> l'uso di una parola chiave identica al marchio altrui è vietato quando comporti, a carico dell'utente "medio", una situazione di confusione circa la provenienza dei beni o dei servizi pubblicizzati nell'annuncio a pagamento" poiché "nel caso di produttori particolarmente popolari (e il caso di Interflora viene addirittura citato come caso di riferimento) la presenza di un marchio piuttosto che di un altro rende assolutamente evidente, anche nel contesto della singola riga che compare tra i risultati del motore di ricerca, che si ha a che fare con un determinato operatore commerciale.

L'adito Tribunale genovese, fa riferimento a «l'utente di Internet normalmente informato e ragionevolmente attento», così escludendo che l'annuncio sia valutato «con riguardo alle capacità di un utente particolarmente competente o per converso a quella del più sprovveduto": l'utente "medio" «non deve essere identificato con riguardo alla universale popolazione di coloro che accedono a Internet, bensì facendo riferimento all'insieme dei soggetti interessati alla ricerca compiuta con l'impiego delle parole chiave di cui si tratta».

Inoltre si segnala anche il provvedimento reso dal Tribunale di Milano, sez. spec. Imprese, in data 8.11.2019, n. 10130 nel caso Jeunesse Global Holdings Llc – società statunitense operativa nel settore della produzione e del- la commercializzazione di prodotti anti-età, integratori alimentari e cosmetici – e dalla sua controllata italiana Jeunesse Global Italy s.r.l. – società che gestisce la rete di vendita a domicilio sul territorio nazionale dei prodotti della controllante – nei confronti del titolare dell'impresa individuale Jeunesse Italia. In detto giudizio il tribunale meneghino ha censurato la condotta della convenuta che ha

[16] Tribunale di Milano, Sezione Specializzata in materia di Impresa, con sentenza 3280 del 2009; Tribunale di Milano, Sezione Specializzata in materia di Impresa, con sentenza 40348/2013 del 22.4.2016.

utilizzato illecitamente i marchi e, in particolare, il segno distintivo "*Jeunesse*", impiegato anche all'interno del nome a dominio del sito di *e-commerce* (www.jeunesseitalia.com), oltreché degli indirizzi e-mail sia ordinaria che certificata della ditta e quale *keyword*, ciò in quanto l'uso non era autorizzato e vi era stato anche lo sviamento di clientela, tanto da esser riconosciuto, nel giudizio di merito, anche il risarcimento del danno.

Nel panorama nazionale è di ulteriore interesse l'ordinanza resa dal Tribunale di Bari, il 27 aprile 2021, dove ha statuito che:

> il pregiudizio al marchio "Interflora" ed alla sua notorietà è indubbiamente presente, posto che i consumatori che digitano all'interno del motore di ricerca Google il marchio "Interflora" ritrovano tra i vari risultati anche il link www.internationalflora.it, che, per l'appunto, riconduce alla pagina web dell'odierna resistente International Flora, che offre i medesimi servizi di vendita di fiori e piante on line, con consegna a domicilio, in Italia ed all'estero;
>
> tali elementi di fatto comprovano, con sufficiente verosimiglianza, che l'uso del marchio "Interflora" come keyword da parte di International Flora pregiudica, in particolar modo, non solo la funzione essenziale del marchio di garantire ai consumatori la provenienza del prodotto (v. CGUE, 22/09/11 in C-323/09, Interflora, CGUE 12/11/2002 in C-206/01, Arsenal Football Club), ma anche quella di garantire la qualità dei loro prodotti o servizi, con effetto confusorio e pregiudizio dell'affidabilità del marchio. È indubbio che una delle funzioni principali del marchio sia quella di consentire agli utenti/consumatori che scorrono i vari annunci pubblicati su Internet di distinguere i prodotti/servizi del titolare del marchio da quelli di altra provenienza: pertanto detto titolare deve poter vietare la visualizzazione di annunci di terzi che gli utenti di Internet rischiano di percepire erroneamente come provenienti da lui;
>
> proprio a causa dei suddetti motivi, International Flora – con una sorta di c.d. "parassitismo" – tragga indebitamente vantaggio dalla notorietà del marchio "Interflora", ricevendo ordini da clienti che in un mercato concorrenziale non confusorio si sarebbero rivolti ad Interflora. Dunque, allo stato degli atti, sussiste il presupposto del fumus boni iuris, ossia l'illegittimità della condotta di International Flora, per violazione dei diritti nascenti dal marchio "Interflora" e per concorrenza sleale confusoria ai sensi dell'art. 2598 c.c.

In tale materia, è altresì intervenuta l'Autorità per le garanzie nelle comunicazioni (AGCOM) esprimendosi sul caso di utilizzo di marchi altrui come parole chiave di *Adwords*. In particolare, l'Autorità, con provvedimento n. 25349/2015, ha ritenuto che la condotta posta in es-

sere dalla società inserzionista fosse ingannevole e determinasse confusione tra i consumatori, così configurando un'ipotesi di pratica commerciale scorretta, ai sensi degli artt. 20, comma 2, e 21, comma 1, lettere a) ed f), e comma 2, lettera a), del Codice del Consumo[17].

Da ultimo è intervenuto il Tribunale di Milano che con l'ordinanza del 2 agosto 2021 ha ritenuto come:

> è ormai opinione consolidata quella secondo la quale l'impiego del marchio altrui quale keyword nelle pratiche commerciali e promozionali possa essere considerato in sé lecito ed anche svolgente spesso una funzione proconcorrenziale. La giurisprudenza comunitaria ha rilevato che nei casi in cui il consumatore inserisca il nome di un marchio quale parola da ricercare, esso si prefigge di trovare informazioni od offerte sui prodotti o sui servizi di tale marchio. Pertanto, quando sono visualizzati, sopra o a lato dei risultati naturali della ricerca, link pubblicitari verso siti che offrono prodotti o servizi di concorrenti del titolare di detto marchio, l'utente di Internet, se non esclude subito tali link in quanto non pertinenti e non li confonde con quelli del titolare del marchio, può percepire che detti link offrano un'alternativa rispetto ai prodotti o ai servizi del titolare del marchio (Corte di Giustizia UE, 23.03.2010 Caso Google France e Google).

Si può dunque affermare che la violazione dei diritti di esclusiva del titolare del marchio da parte dell'inserzionista, si avrà nel caso in cui: i) l'annuncio del terzo lasci intendere l'esistenza di un collegamento economico in realtà insussistente tra tale terzo e il titolare del marchio; ii) l'annuncio, pur non suggerendo esplicitamente l'esistenza

[17] L'art. 20, comma 2, sancisce che: «una pratica commerciale è scorretta se è contraria alla diligenza professionale, ed è falsa o idonea a falsare in misura apprezzabile il comportamento economico, in relazione al prodotto, del consumatore medio che essa raggiunge o al quale è diretta o del membro medio di un gruppo qualora la pratica commerciale sia diretta a un determinato gruppo di consumatori». L'art. 21, comma 1, lettere a) ed f), e comma 2, lettera a), sancisce che: «è considerata ingannevole una pratica commerciale che contiene informazioni non rispondenti al vero o, seppure di fatto corretta, in qualsiasi modo, anche nella sua presentazione complessiva, induce o è idonea ad indurre in errore il consumatore medio riguardo ad uno o più dei seguenti elementi e, in ogni caso, lo induce o è idonea a indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso: a) l'esistenza o la natura del prodotto; f) la natura, le qualifiche e i diritti del professionista o del suo agente, quali l'identità, il patrimonio, le capacità, lo status, il riconoscimento, l'affiliazione o i collegamenti e i diritti di proprietà industriale, commerciale o intellettuale o i premi e i riconoscimenti» e che «2. è altresì considerata ingannevole una pratica commerciale che, nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, induce o è idonea ad indurre il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso e comporti: a) una qualsivoglia attività di commercializzazione del prodotto che ingenera confusione con i prodotti, i marchi, la denominazione sociale e altri segni distintivi di un concorrente, ivi compresa la pubblicità comparativa illecita».

di un collegamento economico, sia così vago sull'origine dei beni in questione che un utente di Internet normalmente informato attento non sia in grado di sapere, sulla base del *link* pubblicitario e del messaggio commerciale allegato, se l'inserzionista rappresenti un terzo rispetto al titolare del marchio o, al contrario, sia economicamente legata a quest'ultimo[18]; iii) vi sia un rischio di confusione, quando sussiste il rischio che il pubblico possa credere che i prodotti o i servizi di cui si tratta provengano dalla stessa impresa o, eventualmente, da imprese economicamente collegate[19].

6. Responsabilità del prestatore di un servizio di posizionamento

Oltre ai due concorrenti, occorre considerare anche la responsabilità del prestatore di un servizio di posizionamento su web, che memorizza come parola chiave un segno identico ad un marchio registrato e organizza, a partire dalla stessa parola chiave, la visualizzazione di annunci riconducibili ad aziende concorrenti, tenuto conto che l'utilizzo illecito di marchi altrui produce anche un beneficio per il prestatore di servizi che in tal modo vende più spazi pubblicitari e a un costo superiore.

In tale contesto la responsabilità di Google che, sebbene ritenga contraria ai propri Termini di servizio[20] la pubblicazione di contenuti illeciti o lesivi dei diritti di soggetti terzi, e si riservi il diritto di sospendere la fornitura di ogni servizio nei confronti degli utenti che violino tali regolamentazioni, sussiste nel caso di omesso intervento a seguito delle specifiche segnalazioni trasmesse dalla società lesa.

Tali conclusioni sono peraltro confermate dall'ordinanza con cui il Tribunale di Milano ha ritenuto sussistente la responsabilità del gestore di una piattaforma che non aveva proceduto a rimuovere contenuti

[18] Così, il Tribunale di Milano, con la sentenza 3280 del 2009, ha ritenuto illegittimo l'utilizzo, come parola chiave in una campagna AdWords del marchio di nota società di noleggio, da parte di società concorrente; scelta che, secondo il Tribunale era evidentemente tesa a sfruttare la notorietà del marchio a proprio vantaggio configurando, nel caso specifico, un'attività confusoria, sviamento della clientela e violazione del marchio per l'individuazione di servizi offerti dall'inserzionista, sicuramente affini a quelli della società il cui marchio era stato inserito come parola chiave.

[19] Corte di Giustizia UE, sentenze *Lloyd Schuhfabrik Meyer* del 22.6.1999, *Medion* del 22.10.2015, *adidas AG* e *adidas Benelux* del 23.10.2003.

[20] Disponibili al link: *https://policies.google.com/terms?hl=it*.

del cui carattere illecito era venuta «a conoscenza su segnalazione del soggetto interessato»[21]. Sul punto, è intervenuta anche la Corte di Giustizia UE[22] stabilendo che «al fine di verificare se la responsabilità del prestatore del servizio di posizionamento possa essere limitata ai sensi dell'art. 14 della Direttiva 2000/31, occorre esaminare se il ruolo svolto da detto prestatore sia neutro, in quanto il suo comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza»[23].

Nel rispondere a tale quesito, la Corte UE ha ritenuto rilevante, al fine di determinare se la fornitura del servizio AdWords comportasse la conoscenza dei dati memorizzati, «il ruolo svolto dalla Google nella redazione del messaggio commerciale che accompagna il link pubblicitario o nella determinazione o selezione di tali parole chiave».

Anche l'Avvocato Generale presso la Corte di Giustizia, nel rassegnare le proprie conclusioni sul caso succitato, ha evidenziato che, per le sue concrete modalità operative, «AdWords non è più un veicolo neutro di informazioni […] pertanto, l'esenzione di responsabilità per gli host di cui all'art. 14 della direttiva 2000/31 non va applicata al contenuto presentato nell'AdWords»[24].

Anche a voler prescindere dal ruolo attivo o neutro svolto da Google nella gestione del detto servizio pubblicitario, la Corte europea ha ritenuto che Google debba essere in ogni caso ritenuta responsabile nell'ipotesi in cui «essendo venuta a conoscenza della natura illecita di tali dati o di attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi»[25].

[21] Cfr. Tribunale di Milano, ordinanza del 23.6.2017.

[22] Si tratta della pronuncia resa nei procedimenti riuniti C-236/08, C-237/08 e C238/08 sul caso *Google France SARL* e *Google Inc*. contro *Louis Vuitton Malletier SA*.

[23] Cfr. punto 114, C-236/08, C-237/08 e C238/08 sul caso *Google France SARL* e *Google Inc*. contro *Louis Vuitton Malletier SA*.

[24] Cfr. punti 145 e 146 delle conclusioni rassegnate il 22.9.2009.

[25] Cfr. punti 109 e 120 delle conclusioni rassegnate il 22.9.2009.

7. Conclusioni

La giurisprudenza comunitaria e nazionale, quindi, non considera di per sé illecito l'uso del marchio altrui quale parola chiave nel servizio Google AdWords (o anche come *keyword*), ma solo ove ricorrano specifiche condizioni:

> per quanto importante essa possa essere, la protezione offerta dall'art. 5, n. 1, lett. a), della direttiva mira solo a consentire al titolare del marchio d'impresa di tutelare i propri interessi specifici in quanto titolare di quest'ultimo, ossia garantire che il marchio possa adempiere le sue proprie funzioni. L'esercizio del diritto esclusivo conferito dal marchio deve essere riservato ai casi in cui l'uso del segno da parte di un terzo pregiudichi o possa pregiudicare le funzioni del marchio e, in particolare, la sua funzione essenziale di garantire ai consumatori la provenienza del prodotto[26].

Anche a voler prescindere dal ruolo attivo o neutro svolto da Google nella gestione del detto servizio pubblicitario, la Corte di Giustizia e ha comunque ritenuto che Google debba essere in ogni caso ritenuta responsabile nell'ipotesi in cui «essendo venuta a conoscenza della natura illecita di tali dati o di attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi»[27].

Nei casi in cui si subisce un uso illecito di marchi in contesti di *digital advertising*, la prova informatica va dunque raccolta mediante adeguate procedure di informatica forense che oltre a garantire integrità e immodificabilità, possano consentire la verifica successiva di un dato che per sua natura è estremamente volatile.

[26] Cfr. punto 37 sentenza della Corte di Giustizia UE, nel caso *Interflora* contro *Marks & Spencer* (C-323/09) nonché si veda la sentenza 12 novembre 2002, causa C-206/01, Arsenal Football Club, Racc. pag. I-10273, punto 51.

[27] Cfr. sentenza della Corte di Giustizia 23.3.2010, *Google France SARL* e *Google Inc*. contro *Louis Vuitton Malletier SA* (C-236/08).

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643015
pp. 281-300 (gennaio 2022)

Un modello per la gestione del trattamento dei dati prodotti e raccolti dall'Internet of Things nell'e-Health

Rosa Domina[1]

1. Introduzione

Delineare l'analisi prospettica del ruolo e dell'importanza che l'uso dell'*IoT (Internet of Things)* può rappresentare nello sviluppo di nuovi prodotti e nuovi servizi da immettere sul mercato della tecnologia digitale è senza dubbio un esercizio che richiede una chiara presa di coscienza soprattutto se si considera che i dispositivi elettronici hanno una dimensione sempre più ridotta a fronte di una performance, sul piano prestazionale, sempre più alta.

Le nostre automobili, i nostri elettrodomestici, le nostre abitazioni, i nostri vestiti, per restare in un ambiente noto, sono dotati di sensori che raccolgono dati di funzionamento, di posizionamento, dei nostri movimenti, delle nostre decisioni quotidianamente.

I paragrafi seguenti delineano un percorso che sfocia nella definizione di un *framework* per la gestione del trattamento dei dati prodotti e raccolti dall'*Internet of Things* in ambito *e-Health*, che sia conforme al quadro normativo in materia di tutela della *privacy* e protezione dei dati personali e contestualmente adeguato sotto il profilo della sicurezza informatica tanto da essere uno strumento di riferimento nelle indagini investigative e forensi.

[1] Dottore di ricerca in Informatica Giuridica, presso l'Università di Bologna e Referente Giuridico amministrativo DPO, Aziende Sanitarie Metropolitane di Bologna.

2. *Internet of Things* (IoT) tra presente e futuro: ruolo e ambiti di impiego

L'impiego dell'*IoT (Internet of Things)* sempre più pervasivo rappresenta, nello sviluppo di nuovi prodotti e nuovi servizi da immettere nel mercato digitale tecnologico, un elemento di forte impatto sia perché i dispositivi elettronici hanno una dimensione sempre più ridotta a fronte di altissime performance, sia perché viviamo tutto questo con una tale naturalità che non avvertiamo minimamente la loro presenza ma piuttosto rischiamo di andare in ansia se la connessione si interrompe.

Siamo entrati nel "mondo dell'*IoT*". Considerando che questa tecnologia dimostra in maniera sempre più incisiva la sua forza e si sta affermando come "strumento" privo di un perimetro funzionale e applicativo, non si può che prevedere un suo uso crescente ed un impiego in svariati ambiti di attività, tra i quali il settore dell'*e-Health*[2].

In questo campo le potenzialità d'uso, sia in termini di incidenza sui servizi di assistenza sanitaria fruibili che sull'impatto che avranno nello sviluppo tecnologico futuro, sono si molteplici ma in parte limitati ad ambiti circoscritti e in fase di studio.

2.1. *IOT: un nuovo paradigma socio-tecnico*

Il cambiamento della cultura del dato e la rapidità con cui si evolvono i sistemi tecnologici di produzione e condivisione impongono una attenta riflessione sul ruolo che i vari attori assumono nell'ecosistema *IoT*. Si vive una nuova prospettiva per la sanità, fondata su un modello che pone al centro dei percorsi di diagnosi e cura il paziente, un soggetto consapevole e capace di acquisire maggior controllo delle proprie condizioni di salute anche attraverso una diretta gestione dei propri dati e delle varie opzioni diagnostiche e terapeutiche che le nuove tecnologie offrono.

Moltissimi oggetti di uso comune ne fanno parte e sono veicolo di dati e informazioni e nel momento in cui sono collegati ad internet e interagiscono con il mondo circostante l'*Internet of Thing* lascia il passo ad un nuovo paradigma, all'*Internet of Everything,* più esteso nel

[2] M. Mancarella, *e-Health e diritti*: *l'apporto dell'informatica giuridica,* Carocci, Roma, 2013; M. Moruzzi, *Smart Health: matrici, road map e altri attrezzi per ri-progettare la sanità*, Franco Angeli, 2017; W. Gatti, *Sanità e web: Come internet ha cambiato il modo di essere medico e malato in Italia*, Springer Verlag, 2012; F. Castiello, V. Tenore, *Manuale di Diritto Sanitario*, Giuffrè Editore, 2 ed., 2018.

quale gli oggetti "dialogano" e possono "imparare" dai comportamenti rilevati. Si stima che entro il 2030 gli oggetti in grado di comunicare ed interagire supereranno la soglia dei 24 miliardi[3].

Da ciò ne deriva che l'elemento caratteristico dell'*IoT* è la possibilità che ogni oggetto è perfettamente in grado di scambiare in modo autonomo informazioni con gli oggetti circostanti, potendo anche modificare il proprio comportamento in funzione degli input ricevuti dagli altri oggetti con i quali interagisce.

L'*IoT* ha in sé un grande potenziale, in particolare quello di estendere, virtualizzare e attivare nuovi processi di prevenzione e cura (nel campo dell'assistenza domiciliare, nella medicina preventiva e predittiva, nei trattamenti farmaceutici personalizzati o gestiti da remoto) e trasformarli in servizi configurando quello che si può definire una nuova era per l'assistenza sanitaria: una Sanità 4.0[4].

L'*IoT* offre molte potenzialità e il suo impiego apre a molte sfide, innanzitutto perché può garantire che il trattamento corretto dei dati personali raggiunga i pazienti in modo adeguato e nel momento giusto e in secondo luogo perché consente di sviluppare nuove capacità di elaborazione dei dati sanitari fino a tracciare un profilo del paziente che beneficia della cosiddetta *precision medicine*[5] intesa come un approccio innovativo di terapie sempre più mirate che consentono ai professionisti sanitari di definire specifici trattamenti per ciascun paziente tenendo in considerazione parametri provenienti dal paziente stesso, dal suo stile di vita, da fattori ambientali, quindi non solo fisici.

Il mondo dell'*IoT* è in grado di dare risposte tempestive a domande complesse, grazie alla capacità di analizzare e correlare enormi quantità di dati, operazioni queste che per la criticità a cui possono andare incontro vanno governate e gestite tenendo conto delle norme che regolano la materia nel complesso e delle norme specifiche di settore.

[3] https://transformainsigh.ts.com/news/iot-market-24-billion-usd15-trillion-revenue-2030.

[4] Piano Nazionale Industria 4.0 https://www.mise.gov.it/images/stories/documenti/guida_industria_40.pdf settembre 2019.

[5] La presa in carico del paziente e il processo di cura sono tanto più precisi quanto più si tiene in considerazione il singolo caso concreto. L'obiettivo è quello di connettere le informazioni biologiche e genetiche della persona con l'ambiente in cui vive e il suo stile di vita. President Obama's Precision Medicine Initiative, 2015, pubblicato online su The White House Web site e consultabile all'indirizzo: https://obamawhitehouse.archives.gov/ the-press-office/2015/01/30/fact-sheetpresident-obama-s-precision-medicine-initiative.

2.2. *IoT: questioni di privacy e contesto normativo di riferimento*

L'uso di sistemi tecnologici così avanzati e così pervasivi nella sfera personale deve necessariamente porre l'attenzione su svariati interrogativi in termini di sicurezza e di integrità dei dati, di corretto trattamento, di proprietà del dato poiché sono tutti elementi imprescindibili nelle varie fasi di una indagine forense, ed è innegabile che lo sviluppo dell'*IoT* porta in sé una vulnerabilità che richiede una gestione più accurata dei dati personali e in special modo dei dati di natura particolare (ex dati personali sensibili), così come pone molti interrogativi sul controllo e governo del rischio derivante dai processi informatici.

Chi sarà chiamato a rispondere in caso di danni? Gli ingegneri che hanno progettato il sistema? I gestori o i manutentori che operativamente gestiscono gli oggetti? O chi ha certificato e di conseguenza ne ha autorizzato l'utilizzo, assumendosi ogni rischio conseguente? [6]

Dare una risposta ai quesiti posti non è semplice, ricostruire l'esatta filiera non è sempre possibile in quanto i dispositivi elettronici e medici generano una quantità di dati senza precedenti, la tutela e la protezione di questi dati deve essere parte integrante dei processi di responsabilizzazione della gestione dei rischi incentrati sull'*IoT*, va garantito un uso responsabile e vanno soprattutto definiti limiti e attribuzioni tra i rischi in capo ai cittadini-pazienti e ai rischi e responsabilità di natura prettamente professionale-aziendale-istituzionale.

I quesiti posti in precedenza devono trovare soluzione nella corretta applicazione delle norme, delle linee guida, degli standard di riferimento, che in mancanza di una disciplina specifica di settore dovranno essere adattate e applicate quindi in analogia.

Considerando la peculiarità del settore, è necessaria una analisi degli assetti giuridici e normativi internazionali, europei e nazionali nel quale si colloca il complesso dell'*IoT*, in rapporto al suo utilizzo in campo *e-Health*.

Se si analizza l'aspetto sotto il profilo della tutela del trattamento dei dati personali non possiamo che fare riferimento al D.Lgs. n. 196/2003 – "Codice in materia di protezione dei dati personali" (di seguito denominato "Codice") così come novellato dal D.Lgs. n. 101/2018 in adesione alle disposizioni del Regolamento UE 2016/679 GDPR (*General Data Protection Regulation*).

[6] Cfr. Corte di Cassazione (Cass. pen. Sez. IV, Sent., ud. 03-12-2015, 21-01-2016, n. 2541) ricostruisce una vicenda di "morte per telemetria".

Il Codice ha subito una profonda innovazione sia in termini concettuali sia di interpolazione, in particolare il Capo I e il Capo II sono innovativi e sostitutivi di tutta la Parte I del vecchio Codice e riguardano sostanzialmente principi e disposizioni generali, disposizioni in materia di diritti degli interessati, titolare e responsabile del trattamento.

Cambia sostanzialmente la visione, si passa da un processo di tipo reattivo, nel senso che, ante GDPR, si dava risposta ad un evento, di minaccia o di danno conclamato, mettendo in atto le misure di sicurezza indentificate, solo al verificarsi di quel dato evento, ad un approccio basato sul rischio o *risk based approach*[7], capace di reagire ad un evento secondo un modello di *compliance* proattivo[8].

Le nuove norme impongono un sistema fondato sul principio di "responsabilizzazione", "dell'*accountability*", secondo il quale spetta alle organizzazioni individuare le misure tecniche e organizzative più adeguate a proteggere i dati personali oggetto del loro trattamento, sia che svolgano il ruolo di Titolare del trattamento, sia che siano stati designati responsabili esterni al trattamento.

Entra a far parte dei soggetti posti a salvaguardia della tutela dei diritti e delle libertà degli interessati la figura del *Data Protection Officer*, prevista dall'art. 38 del GDPR che, tra le molteplici funzioni assegnategli, deve possedere conoscenze e competenze specialistiche della normativa e delle prassi in materia di protezione dei dati personali nonché la capacità di svolgere i compiti di cui all'articolo 39, ovvero:

[7] Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso uno specifico processo di valutazione (artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. Si veda a tal proposito il considerando 71 del GDPR.

[8] La capacità di reazione secondo un modello proattivo consiste nella predisposizione di piani di azione volti a limitare il verificarsi degli eventi a rischio e di conseguenza di violazioni di dati personali che tengono conto di una serie di fattori quali: la tipologia di dati, il contesto e le modalità del trattamento, il grado di probabilità e di gravità dei potenziali rischi ai quali è esposto l'interessato. A tal proposito di particolare interesse quanto contenuto nelle Linee guida e pareri emanati dall'*European Data Protection Board* (EDPB) che spingono ad interpretare e applicare il GDPR in una logica sempre più proattiva. Si vedano, appunto in questa prospettiva, EDPB, *Statement of the EDB on the data protection impacts of economic concentration*, del 27 agosto 2018, Opinione 23/2018 *on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters* (art. 70.1.b) del 26 settembre 2018, *Opinion* 3/2019 *concerning the Questions and Answers on the interplay detween the Clinical Trials Regulation (CTR) and the General Protection regulation* (GDPR) (art. 70.1.b), del 23 gennaio 2019, EDPB-EDPS*, Joint Opinion 1/2019 on the processing of patients' data and role of the European Commission within the health Digital Service Infrastructure* (eHDSI), del 12 luglio 2019.

- informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti autorizzati che trattano i dati personali;
- sorvegliare l'osservanza della normativa comunitaria e nazionale nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento riguardanti anche "l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo";
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante nazionale;
- fungere da punto di contatto per l'autorità Garante nazionale per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il Codice inoltre subisce un'ulteriore sostanziale modifica, le misure minime di sicurezza, previste nell'Allegato B, vengono abrogate e sostituite dall'obbligo generico, in capo al Titolare, di mettere in atto misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato e commisurato al rischio.

A supporto di tali indicazioni possiamo anche fare riferimento al Parere 2/2013 del WP29 sulle applicazioni per dispositivi mobili, (oggi rinominato EDPT *European Data Protection Board*), che chiarisce il quadro giuridico applicabile al trattamento dei dati personali nello sviluppo, nella distribuzione e nell'utilizzo di applicazioni su dispositivi intelligenti quali sono gli *IoT*.

Il parere è formulato come una sorta di Linee Guida a cui gli sviluppatori di applicazioni per *smart device* (principalmente *smartphone, smartwatch, tablet, wearable, smart-tv*, automobili, allarmi, sistemi di domotica, ecc..) devono attenersi al fine di garantire il rispetto dei principi connessi al trattamento dei dati personali.

Gli aspetti fondamentali a cui il parere dedica maggiore attenzione invitando gli attori coinvolti nel processo di progettazione, realizzazione, certificazione e utilizzo sono:

- adottare informative adeguate al fine di fornire una informazione corretta agli utenti finali;

- necessità di acquisire il consenso (ove applicabile);
- limitazione della finalità e minimizzazione dei dati;
- adozione di adeguate misure di sicurezza, tecniche ed organizzative, volte a ridurre al minimo i rischi legati a violazioni che potrebbero di per sé configurarsi come *data breach*[9], (come ad es. accessi non autorizzati, cancellazione o distrazione massiva di dati);
- rispetto dei diritti dell'interessato, con particolare riguardo alla possibilità di cancellazione della app e dei relativi dati;
- definizione a priori dei periodi di conservazione dei dati;
- definizione delle modalità di trattamento dei dati provenienti da minori ovvero ad essi relativi.

Il parere in questione è stato inoltre la base di partenza che ha consentito all'Autorità Garante per la protezione dei dati personali italiano l'emanazione di un primo provvedimento sulla "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie" Registro dei Provvedimenti n. 229 dell'8 maggio 2014.

Nello specifico è in capo agli *App store* la responsabilità di rendere visibile l'informativa, anche in forma sintetica, immediatamente al primo accesso e comunque prima della completa installazione dell'applicazione. L'informativa deve contenere nel testo un link che rimandi alla *Privacy Policy* integrale. Tale responsabilità è insita anche negli sviluppatori dell'app poiché entrambi devono garantire che ogni applicazione fornisca le informazioni essenziali ed esaustive inerenti alla finalità per cui è in essere quel determinato trattamento di dati personali.

In considerazione del fatto che l'uso delle app e quindi la navigazione in internet fa si che il fornitore di servizi installi sui dispositivi file di testo i "cosiddetti *cookies*", il parere indica la necessità di richiedere il consenso per i *cookies* di profilazione mentre per l'installazione dei c*ookies* tecnici non è richiesto il consenso degli utenti, ma è necessario dare l'informativa (art. 13 GDPR) con l'espressa indicazione dell'eventuale trasferimento dei dati a terze parti.

[9] Per *data breach*, si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, regolamentata dagli artt. 33 e 34 del GDPR.

Una recente sentenza del Corte di giustizia dell'Unione Europea[10] ha stabilito che per «l'installazione di cookies è necessario il consenso attivo degli utenti di Internet. Una casella di spunta preselezionata è pertanto insufficiente». La suddetta sentenza costituisce certamente un importante precedente in quanto dal primo ottobre 2019 l'uso di dispositivi connessi a internet è condizionato dall'ottenere il consenso esplicito degli utenti per raccogliere i loro dati personali in quanto i giudici hanno stabilito che non è sufficiente mostrare una casella con un segno di spunta per consentirgli di raccogliere le informazioni digitali degli utenti ma il consenso va raccolto con una azione attiva dell'interessato.

3. IoT e *governance* della sicurezza dei dati

La tutela della sicurezza delle informazioni è un elemento imprescindibile in ambito sanitario, ambito nel quale la triade RID costituita dalla Riservatezza-Integrità-Disponibilità si fondono, a garanzia della protezione dei dati personali e di quelli di natura particolare dei cittadini-pazienti[11].

Il che significa avere a disposizione organizzazioni in grado di rispondere tempestivamente ai rischi derivanti dall'impiego di *smart device* come l'*IoT* nelle quali le politiche di sicurezza sono conosciute, condivise, adottate, monitorate costantemente ed eventualmente riprogettate per rispondete efficacemente alle minacce, alle vulnerabilità o agli incidenti che possono verificarsi.

Allo stato attuale l'impiego di sistemi *IoT* nel campo sanitario istituzionale non ha riscontrato una particolare applicazione, sono ancora poche le esperienze rilevate nel servizio sanitario nazionale, sostanzialmente si tratta di progetti nei quali l'*IoT* è utilizzata dai pazienti e dalle equipe mediche con l'obiettivo di intensificare percorsi

[10] Sentenza della Corte (Grande Sezione) del 1° ottobre 2019 (Causa C-673/17) «Rinvio pregiudiziale - Direttiva 95/46/CE - Direttiva 2002/58/CE - Regolamento (UE) 2016/679 - Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche - Cookie - Nozione di consenso dell'interessato - Dichiarazione di consenso mediante una casella di spunta preselezionata» https://curia.europa.eu/juris/document/document.jsf;jsessionid=2C7779F24F325525EB8BECDC8A9D206E?text=&docid=221353&pageIndex=0&doclang =IT&mode=req&dir=&occ=first&part=1&cid=37992731.

[11] R. Brighi, *Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati, in: Diritto e tecnologie informatiche*, in Questioni di informatica giuridica, prospettive istituzionali e sfide sociali, Wolters Kluwer CEDAM, 2021.

diagnostici e terapeutici di assistenza, che fruiscono dei trattamenti ospedalieri da casa, senza interruzioni nella continuità assistenziale. Principalmente sono in uso[12]:

- applicazioni in grado di geolocalizzare in tempo reale la posizione dei pazienti in modo da lasciare maggiore libertà di movimento e al contempo garantendo il controllo e la sicurezza degli stessi;
- dispositivi medici integrati internamente ovvero pacemaker e altri dispositivi impiantati nel paziente (impiantabili) ma che comunicano con l'esterno in modalità wireless;
- dispositivi medici fissi. Questi *device*, quali stazioni di erogazione di chemioterapie all'interno dell'ospedale o apparecchi per il monitoraggio cardiaco domiciliare dei pazienti cronici, spesso utilizzano i più tradizionali *network wireless* come il *WiFi* negli ospedali o a casa del paziente;
- dispositivi in grado di gestire gli ambienti nelle sale operatorie regolando temperatura, luci, aereazione; o ancora dispositivi medici che sono in grado di dialogare con strumenti di chirurgia robotica e che agiscono a seconda dei dati rilevati: concentrazione di ossigeno nel sangue del paziente, parametri vitali, test di analisi chimico-cliniche.

Se analizziamo sotto il profilo della sicurezza i già menzionati impieghi possiamo evidenziare le possibili vulnerabilità quali ad esempio pone la geolocalizzazione in termini di esattezza della posizione in cui si trova il soggetto, senza contare che l'uso di *IoT* che monitora, influenza o regola funzioni vitali espone ad un rischio maggiore l'intero ecosistema sanitario e di conseguenza la vita del paziente.

Una attenta analisi dei possibili rischi è stata affrontata dal WP29 nel Parere n. 8/2014. Il documento prende in esame i principali rischi legati alla protezione dei dati prodotti dall'*IoT* e sostiene che tutti gli *stakeolder* coinvolti nell'intero processo, che va dalla progettazione, alla realizzazione, alla commercializzazione, devono assicurare le massime garanzie possibili per gli utenti, i quali devono poter avere il completo controllo dei propri dati personali durante tutto il ciclo di vita del

[12] Una prima disamina è stata tracciata da P. Colli Franzone, *The healthcare digital revolution*, 2018.

prodotto. Deve essere ben specificata l'informativa e raccolto il consenso al trattamento che deve quindi essere informato, libero e specifico.

L'*IoT* suscita inoltre serie preoccupazioni in materia di sicurezza, in quanto eventuali violazioni possono comportare la compromissione dei dati e la conseguenza di gravi rischi per i diritti e le libertà dell'interessato. Il parere afferma ancora che: «Più in generale, l'interazione degli oggetti tra loro, tra gli oggetti e i dispositivi delle persone, tra le persone e altri oggetti e tra oggetti e sistemi di back-end porterà alla creazione di flussi di dati che possono difficilmente essere gestiti dai classici strumenti utilizzati per garantire una tutela adeguata degli interessi e dei diritti degli interessati» e a parere di chi scrive non è semplice garantire, lungo tutta la catena del flusso delle informazioni, che aspetti di disponibilità e integrità dei dati siano efficacemente presidiati e tutelati.

Fatto che innegabilmente comporta un rischio di mancanza di controllo e di eccessiva esposizione per l'utente senza contare che l'*IoT* tramite impostazioni predefinite e opportuni programmi informatici potrebbe avviare automaticamente la comunicazione tra gli oggetti, senza che il diretto interessato ne sia al corrente e che di conseguenza possa avere alcun controllo su ciò che accade. La perdita della disponibilità dei propri dati è evidente così come il rischio potenziale di intrusioni e violazioni con conseguente furto o compromissione di dati personali.

La gestione della sicurezza delle informazioni è fondamentale e deve essere un processo che vede coinvolte tutte le parti interessate, quali progettisti e produttori di dispositivi, piattaforme sociali, applicazioni di terzi, titolari o fornitori di dispositivi, istituzioni pubbliche e private e non da ultimo l'interessato.

Come riporta il Rapporto Clusit 2021 sulla sicurezza ICT in Italia, rispetto al 2020, gli attacchi di sicurezza informatica in ambito "Healthcare" sono aumentati del 12%, questo dato è estremamente significativo e deve far riflettere tutte le parti coinvolte, e considerare la gestione della sicurezza fin dalle fasi iniziali del processo in un ottica di *security by design* e *by default*[13], sicurezza e controllo dei dati sono

[13] Il concetto è ben descritto nei considerando 75-78 del GDPR nei quali si rileva che rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso uno specifico processo di valutazione (artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.

fattori fondamentali al fine di garantire una maggiore funzionalità di tutte le apparecchiature che sfruttano la tecnologia *IoT*.

Per una adeguata progettazione di sistemi di gestione di sicurezza delle informazioni in campo *IoT*, possiamo prendere a riferimento il *Framework* Nazionale per la *Cybersecurity*[14] derivante dal *Cybersecurity Framework* NIST[15], specifiche norme ISO come ad esempio la ISO/IEC 27001:2017, la ISO/IEC 27002:2018, la ISO/IEC 27005:2018, e i documenti prodotti dell'Enisa[16] quali: *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* del 2017 e le *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, pubblicate nel 2018. Brevemente si riporta quanto ogni documento indica.

Al fine della gestione della sicurezza il *Cybersecurity Framework* NIST offre un approccio completo e programmatico per raggiungere gli obiettivi aziendali sia di sicurezza in relazione agli obblighi di conformità sia nel supportare servizi e prodotti che intervengono nei processi di adeguamento ai cambiamenti tecnologici e alle *policy* adottate. Preme sottolineare come il suddetto framework fornisca elementi essenziali nella valutazione dei processi di analisi forense degli applicativi informatici pertanto il modello proposto non si sostituisce ma integra gli altri standard di controllo della sicurezza del settore ed è flessibile, nel senso che può essere utilizzato da qualsiasi organizzazione intervenga nel processo e può essere adattato per soddisfare al meglio le esigenze aziendali; il *Framework* Nazionale per la *Cybersecurity* fornisce uno strumento operativo per gestire i processi di *cybersecurity* ed è adattabile ad ogni tipo di organizzazione pubblica e privata, di qualunque dimensione, essendo uno strumento operativo che ben si presta ad essere di supporto alle organizzazioni nel definire

[14] Il Framework Nazionale per la Cybersecurity nasce nel 2015. A dargli vita è una collaborazione tra enti pubblici, accademia e impresa. All'interno del panorama nazionale italiano il Framework Nazionale per la Cybersecurity e la Data Protection rappresenta un punto di riferimento adottato da realtà fortemente eterogenee (dalla grande P.A. alla piccola impresa) come strumento per l'organizzazione della propria strategia di difesa rispetto alle minacce cibernetiche.

[15] La prima versione del framework NIST è stata redatta dal National Institute of Standards and Technology del Dipartimento del Commercio degli Stati Uniti nel febbraio del 2014, mentre la seconda versione corrente aggiornata nell'aprile del 2018. Sostanzialmente il Framework è un insieme completo di linee guida con le quali le organizzazioni possono prevenire, rilevare e rispondere agli attacchi informatici.

[16] L'ENISA da centro di consulenza per la sicurezza informatica in Europa a vera e propria agenzia per la cybersecurity dell'Unione dal 2019 con il Cyberscurity Act.

un percorso volto alla *cybersecurity* e alla protezione dei dati in quanto *compliant* alla normativa vigente in materia.

La norma ISO/IEC 27001:2013, con l'ultimo aggiornamento del 2017, rappresenta la norma di riferimento internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni, ed è uno dei più dettagliati standard di *best-practice* al momento disponibile, la corretta applicazione degli standard definiti dalla norma aiuta le aziende a identificare e contrastare i rischi per la sicurezza e proteggere i dati personali.

Tutte le altre ISO/IEC sempre della famiglia della ISO/IEC 27001, citate in precedenza, sono norme che integrano le funzioni a supporto del sistema di gestione della sicurezza delle informazioni, fungono da linee guida e modelli di riferimento[17].

Gli studi su citati, condotti da ENISA, nel delineare quali sono le misure strategiche che devono essere adottate dai produttori di hardware del settore *IoT* e gli sviluppatori di software già in fase di progettazione, in un ambito di *Industry 4.0, e indicare* le tassonomie e le definizioni chiave consolidando le informazioni circa le *good practices*, forniscono una mappatura delle minacce, dei rischi e gli scenari futuri dei possibili attacchi.

Il quadro delle norme e linee guida, fin qui tracciato, trova parziale completamento con l'analisi del Piano Triennale 2019-2021 per l'informatica nella Pubblica Amministrazione pubblicato da AGID. Il Piano è uno strumento essenziale per promuovere la trasformazione digitale della P.A. italiana in un'ottica di interazione a livello europeo è necessario offrire l'accesso online ai beni e servizi a cittadini e imprese e creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi in piena sicurezza infrastrutturale.

Il Piano individua come uno dei principali approcci per aumentare il livello di sicurezza, la razionalizzazione delle risorse ICT attraverso la riduzione della "superficie" esposta agli attacchi informatici rendendo il sistema o il software più difficile da violare e di conseguenza meno vulnerabile. Nel dettaglio le principali azioni da adottare consistono nel:

- predisporre l'inventario dei dispositivi autorizzati e non autorizzati;
- predisporre l'inventario dei software autorizzati e non autorizzati;

[17] G. Modotti, *"ISO 27001 e GDPR, Linee guida per mettere al sicuro i dati aziendali"*, sito di NetworkDigital360, febbraio 2019.

- adottare policy di protezione per le configurazioni di *hardware* e *software* sui dispositivi mobili, *laptop, workstation* e *server;*
- effettuare la valutazione e correzione continua delle vulnerabilità, attraverso azioni di monitoraggio e miglioramento;
- definire l'uso appropriato dei privilegi di amministratore attraverso una distribuzione granulare delle responsabilità;
- adottare azioni di *awareness* per il personale per la difesa contro *malware*;
- implementare procedure standardizzate per effettuare copie di sicurezza programmate;
- adottare misure tecniche ed organizzative dirette alla protezione dei dati personali.

Da quanto fin qui descritto si denota una mancanza di organicità giuridica della materia sia in termini di protezione dei dati personali sia in termini di sicurezza delle informazioni prodotte o gestite dall'*IoT*. A parere di chi scrive tale mancanza è in parte da ricondurre all'uso recente di tali tecnologie e allo scollamento a cui spesso si assiste tra il progresso tecnologico e sociale e l'adeguamento del nostro sistema giuridico, posto a disciplinare la materia. La frammentarietà e lentezza del diritto è tanto più evidente quanto più veloci corrono i cambiamenti ma non si può negare che allo stato attuale qualunque intervento potrebbe rivelarsi prematuro (e potenzialmente erroneo) a causa della limitata conoscenza da parte del legislatore di fenomeni in fase di formazione e sviluppo di cui non sono state sinora valutate in modo approfondito tutte le possibili implicazioni e "ricadute" di natura sociale e culturale.

4. Framework per la gestione del trattamento dei dati prodotti e raccolti *dall'Internet of Things (IoT*) nell'e-*Health*

Un *framework* per la valutazione della *privacy*, in tale ambito, dovrà avere la caratteristica di essere dinamico in relazione alla velocità con cui l'innovazione tecnologica produce dispositivi sempre più *smart*, inoltre per essere *compliant* alla normativa vigente in materia di trattamento dei dati personali e che al contempo tenga conto degli aspetti di sicurezza informatica sarà necessaria una preliminare valutazione degli *asset* aziendali.

L'analisi degli asset presenti nell'organizzazione e delle relative misure di sicurezza costituirà una buona base per rilevare il livello di rischio e predisporre un piano di intervento adeguato e su misura. Inoltre, la registrazione e la mappatura degli *asset* aziendale è una attività necessaria per la redazione del registro dei trattamenti che costituisce l'unità centrale su cui verrà applicato il modello di gestione.

Nell'ecosistema *IoT* il modello avrà l'ulteriore funzione di gestire il trattamento dei dati che provengono non solo dal singolo dispositivo ma dall'interazione di essi, tenendo conto di tutte le possibili variabili legate alla protezione di questa mole di dati che si viene a creare.

Esempio ne sia l'interazione dei dispositivi che regolano i flussi di gas, l'illuminazione, la perfusione di farmaci, la rilevazione di parametri vitali nelle sale operatorie o nelle terapie intensive, oppure nei sistemi di telemedicina o teleassistenza.

4.1. *Analisi del profilo giuridico*

Le principali criticità legate allo sviluppo e all'ecosistema dell'*IoT* riguardano la tutela dei dati personali degli utenti e la sicurezza. Il Titolare del trattamento oltre a trattare dati personali ai sensi dell'art. 5 del GDPR deve mettere in atto e applicare politiche trasparenti e accessibili con particolare riguardo all'esercizio dei diritti dell'interessato.

Le informazioni devono essere facilmente accessibili e di semplice comprensione, l'interessato deve poter comprendere le implicazioni della raccolta dei dati connessa al prodotto *IoT* ed essere in condizioni di valutare effettivamente la convenienza o meno dell'acquisto e/o uso del prodotto, specie considerati gli usi in campo *e-Health*.

La fiducia e l'accettazione dell'interessato aumenterà[18] se saranno:

- specificati i possibili rischi dei sistemi *IoT* (ad esempio valutazione dell'impatto sulla protezione dei dati, politiche sulla privacy);
- mostrati i meccanismi in grado di limitare eventuali profilazioni (ad esempio modelli di consenso preselezionate, trasparenza al-

[18] L'informativa prevista agli articoli 13 e 14 del GDPR è strettamente connessa al rispetto del principio di trasparenza sancito all'art. 12. Nello specifico le prescrizioni atte a garantire l'adozione di misure tecniche e organizzative dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione devono essere rese in modo esplicito, con un linguaggio intellegibile, semplice e chiaro.

goritmica e strumenti antidiscriminazione nelle decisioni automatizzate);
- mostrate le azioni correttive per mitigare i rischi se il sistema è compromesso (ad esempio rischi informatici, modalità di notifica di *data breach*).

Al momento dell'acquisto e comunque prima dell'uso dei dispositivi collegati ad internet è necessario leggere l'informativa che dovrà contenere quegli elementi previsti dall'art. 13 del GDPR e che ogni azienda-titolare del trattamento ha l'obbligo di fornire prima di mettere a disposizione un prodotto associato ad uno specifico servizio.

Vanno specificati gli strumenti utilizzati per analizzare i dati, i benefici che contraddistinguono la connettività e gli eventuali vantaggi connessi alla raccolta dei dati (quali ad esempio esigenze di adattare piani terapeutici, strategie diagnostiche, ecc.). L'utente deve conoscere anche i maggiori rischi a cui viene esposto ed essere informato dell'eventuale cessione a terzi dei dati per altre finalità e deve essere messo in condizione di scegliere consapevolmente.

Altro elemento da tenere presente è l'osservanza del principio della *privacy by design.* Quindi per un prodotto *IoT* al momento di determinare le finalità e i mezzi del trattamento e all'atto del trattamento stesso, il Titolare del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, deve mettere in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al regolamento e assicuri la tutela dei diritti dell'interessato e limitati esclusivamente all'uso in conformità al principio di minimizzazione. In particolare, se all'interessato è lasciata facoltà di scelta relativamente al trattamento dei dati personali, il Titolare o il Responsabile del trattamento garantiscono che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vada oltre il minimo necessario per le finalità perseguite[19].

[19] Cfr. Corte di Cassazione - I sezione civile, ordinanza del 13.01.2021, n. 368; Corte di Cassazione, VI sezione civile, ordinanza del 21.10.2019, n. 26778, nonché i numerosi Provvedimenti dell'Autorità Garante https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1044344.

4.2. *Analisi della Governance nell'IoT*

I modelli di *governance* nell'*IoT* devono tendere a sviluppare una strategia tecnica e una architettura di riferimento appropriate per guidare la standardizzazione e le migliori pratiche in tutte le iniziative *IoT* all'interno dell'organizzazione. L'identificazione dei ruoli le correlate responsabilità i processi e le politiche adeguate sono elementi fondamentali per governate efficacemente e gestire tutte le attività. Il monitoraggio del ciclo di vita del dispositivo è una delle funzioni chiave nella gestione della *governance IoT* la registrazione di nuovi dispositivi, l'aggiornamento degli esistenti e la disattivazione di dispositivi vecchi o obsoleti, la generazione dei dati nei dispositivi, l'invio dei dati dalle piattaforme *IoT* alla rete sono tutte fasi che vanno tenute sotto stretto controllo per poter gestire efficacemente il rischio di data breach.

Qualsiasi soluzione di *governance IoT* deve affrontare i problemi di privacy e sicurezza, tenendo presente i requisiti normativi e di conformità. Di seguito due fasi fondamentali da osservare per garantire che il percorso di *governance* sia rispondente ai principi e alle norme generali e di settore[20].

(1) Audit

Un dispositivo medico, oltre a rispondere alla normativa vigente[21], prima di essere acquistato e connesso alla rete deve essere confrontato con gli standard di sicurezza interni dell'organizzazione e se risponde a tali standard. Il dispositivo deve essere conforme ai criteri relativi alle password, ai criteri di blocco degli account e ad altri controlli di sicurezza che l'organizzazione considera essenziali.

[20] Oltre all'art. 35 del GDPR si vedano norme come la ISO 25010 e alcuni *framework* internazionali come Cobit19 dedicato *all'IT Governance* che trattano tematiche riconducibili rispettivamente alla "Qualità dei dati e ai software di gestione" e al "Data management".

[21] Dal 26 maggio 2021 è pienamente applicabile il Regolamento (UE) 2017/745. Il regolamento modifica le norme che disciplinano il sistema dei dispositivi medici, tenendo conto degli sviluppi degli ultimi vent'anni, con l'obiettivo di garantire un quadro normativo solido, idoneo a mantenere un elevato livello di sicurezza.

(2) Valutazione d'impatto del trattamento (DPIA)[22].

La valutazione d'impatto (DPIA) dovrebbe essere eseguita prima di qualsiasi acquisizione del sistema al fine di convalidare che il dispositivo possiede i necessari controlli di sicurezza, garantendo che i dati dei pazienti siano raccolti, archiviati e trasmessi in conformità alle norme in modo coerente e in adesione alla politica organizzativa. Laddove applicabile, dovrebbe essere data la preferenza alle soluzioni progettate tenendo conto dei principi di *privacy e security by design e default*. L'uso di una DPIA inteso come un processo di revisione continua è fondamentale sia come strumento per evidenziare la conformità sia come elemento di monitoraggio continuo del processo di protezione dei dati per impostazione predefinita.

Le DPIA dovrebbero essere accessibili ai soggetti interessati al fine di poterne valutare direttamente i rischi così come dovrebbero avere il controllo dei meccanismi di salvaguardia contro la profilazione e il monitoraggio, il diritto di accesso per conoscere quali e se sono stati raccolti dati personali, gli scopi per i quali vengono raccolti, la possibilità di personalizzare i tipi di dati raccolti ed elaborati, il diritto alla disabilitazione del tracciamento e in generale alla disconnessione[23].

4.3. *Analisi della sicurezza delle informazioni*

Uno dei modi migliori per preservare la sicurezza di qualsiasi ambiente sanitario è adottare misure proattive atte a prevenire l'introduzione delle vulnerabilità della sicurezza garantendo che vengano utilizzati solo i dispositivi che forniscono una adeguata misura di sicurezza limitando innanzitutto l'accesso al dispositivo, sia fisico che logico, al

[22] La *Data Protection Impact Assessement* disciplinata dall'art. 35 del GDPR è obbligatoria quando un trattamento prevede l'uso di nuove tecnologie oppure considerati la natura, l'oggetto, il contesto e le finalità del trattamento può rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche (es: trattamenti automatizzati di profilazione sistematica degli interessati, sorveglianza sistematica su larga scala di una zona accessibile al pubblico, trattamenti di dati personali particolari, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, relativi a condanne penali e a reati).

[23] S. WACHTER, *The GDPR and the Internet of Things: A Three-Step Transparency Model, SSRN, 2018.* Il documento propone un modello di trasparenza in tre fasi basato sui rischi noti della privacy dell'*IoT*, sulle debolezze delle pertinenti disposizioni giuridicamente vincolanti nel GDPR e sui principi che regolano il GDPR. Undici linee guida rivolte agli sviluppatori *IoT* e ai responsabili del trattamento dei dati sono descritte affrontando come le informazioni sulla funzionalità dei dispositivi e dei servizi *IoT* dovrebbero essere condivise con gli utenti.

solo personale autorizzato. È auspicabile che i dati memorizzati sui dispositivi siano crittografati al fine di garantire la riservatezza dei dati, oltre a utilizzare procedure di pseudonimizzazione per le comunicazioni, elaborazione e archiviazione di dati sulla rete.

Vanno analizzati i seguenti elementi[24]:

- *Firewall.* I *firewall* perimetrali devono garantire che le comunicazioni tra dispositivi medici e risorse esterne siano limitate alle sole comunicazioni essenziali per il corretto funzionamento del dispositivo o completamente negate.
- Server proxy/filtro web.Per i dispositivi che comunicano con risorse esterne tramite http e/o https, un *server proxy* può consentire un controllo ancora più preciso delle comunicazioni rispetto a un firewall. Inoltre, molti *server proxy* hanno la capacità di eseguire scansioni antivirus del traffico web.
- Segmentazione della rete. La segmentazione della rete è estremamente utile per prevenire la diffusione di *malware* e altre minacce ed è utile nel contenere una minaccia nel caso in cui parte della rete o un dispositivo sia compromesso o violato. Tutti i dispositivi medici devono trovarsi su un segmento di rete isolato che limita la comunicazione dei dispositivi ai soli sistemi necessari per il funzionamento del dispositivo o alla loro interazione.
- *Firewall* integrati. I *firewall* integrati possono essere utilizzati per migliorare la segmentazione della rete e limitare ulteriormente le comunicazioni dei dispositivi ai soli sistemi (interni ed esterni) con cui devono interagire.
- Monitoraggio del registro. Relativamente al controllo è necessario eseguire un periodico monitoraggio della sicurezza, della gestione degli eventi e analisi dei dati raccolti. Ad esempio, un alto numero di tentativi di accesso non riusciti su un dispositivo così come un alto numero di accessi riusciti (al di

[24] S. WACHTER, *The GDPR and the Internet of Things: a three-step transparency model*, in Law, Innovation and Technology 10 (2), 2018, pp. 266-294. Questo documento propone un modello basato sui rischi noti della privacy dell'IoT, sulle debolezze delle pertinenti disposizioni giuridicamente vincolanti nel GDPR e sui principi che regolano il GDPR. Le indicazioni derivanti dalle linee guida sono descritte con un approccio tecnico-pratico, affrontando cioè come le informazioni sulla funzionalità dei dispositivi e dei servizi *IoT* dovrebbero essere condivise con gli utenti.

fuori della manutenzione programmata) può essere indicativa di un attacco da *malware*. L'analisi del registro può anche svolgere un ruolo nelle indagini sugli incidenti in caso di *data breach*.

- Scansione delle vulnerabilità. I dispositivi medici devono essere regolarmente sottoposti a scansione per garantire che siano configurati correttamente e che un *software* obsoleto non li lasci suscettibili di attacchi.
- Disponibilità e possibilità di modifica credenziali predefinite. La disponibilità serve a garantire che i dati possano essere raggiunti dagli utenti autorizzati ogni volta che vengono richiesti. Tutti i dispositivi devono avere le credenziali predefinite modificabili al loro primo utilizzo. Le credenziali dell'*account* utilizzate al posto delle impostazioni predefinite devono essere conformi alle politiche relative alle password dell'organizzazione e bloccare l'account dopo un numero definito di accessi falliti. I dispositivi devono essere configurati per inviare dati solo in un formato sicuro e attraverso protocolli sicuri come ad esempio *https* (*HyperText Transfer Protocol*).
- *Backup* di *firmware/software*. Nel caso in cui un dispositivo venga compromesso o si verifichi un problema sul *software*, disporre di un *backup* del *firmware* o del *software* del dispositivo è fondamentale per ripristinarne lo stato funzionale in modo tempestivo.
- Prove di sicurezza.Tutti i controlli sono inutili se basati su configurazioni errate, programmare test di sicurezza sono fondamentali per rilevare carenze e vulnerabilità nei dispositivi o nella configurazione.
- *Penetration Test.* È una metodica utile per valutare l'efficacia delle configurazioni del dispositivo e della rete nel respingere un attacco ai dispositivi medici installati sulla rete dell'organizzazione. I risultati possono essere utilizzati per migliorare ulteriormente le difese e possono rivelare difetti nel dispositivo che necessitano di patch di aggiornamento.
- Archiviazione. Anche la fase di archiviazione su dispositivi *storage* deve essere effettuata solo dopo avere messo in atto procedure e sistemi di protezione analoghi a quelli dei sistemi di produzione.

5. Conclusioni

Il forte sviluppo dell'*IoT* nel campo dell'*e-Health* pone sempre più in evidenza quanto sia determinante poter condurre indagini forensi sui dispositivi *"indiziati"* per risolvere casi giudiziari in campo civilistico e penale posto che possono diventare testimoni ma anche protagonisti di illeciti e reati.

L'informatica forense chiamata ad analizzare i comportamenti prodotti dall'*IoT* dovrà essere in grado di produrre prove attraverso processi e procedure che ne garantiscano autenticità e veridicità. Nei casi di accertamento di compromissione o violazione dei dati prodotti nell'ambito dell'*IoT* il modello proposto potrà essere utilizzato per identificare le tracce, individuare le possibili cause e le modalità di accadimento e rintracciare tutti gli elementi che ci permettano di delineare un quadro il più realistico e inattaccabile possibile per individuare responsabilità da attribuire e vulnerabilità dei sistemi da evidenziare.

Attraverso l'analisi forense dei dati non è sempre facile comprendere quali siano stati i comportamenti non conformi o illeciti poiché spesso il produttore dei sistemi coinvolti o incriminati potrebbe essere l'unico in grado di comprendere quei dati, quindi, l'utilizzo di uno strumento che standardizzi le fasi e le informazioni da analizzare potrebbe rivelare comportamenti dolosi.

L'interesse per *e-Health*, l'evoluzione tecnologica e di conseguenza il nuovo modo di fare sanità, richiede un forte impegno nell'approfondire le specifiche tematiche tenendo presente in particolare i rischi e le implicazioni giuridiche che da una gestione così pervasiva della vita quotidiana e delle informazioni di salute derivano.

Un ringraziamento speciale va al mio mentore, Prof. Cesare Maioli per la saggezza con cui ha guidato il mio percorso accademico e alla Prof.ssa Raffaella Brighi per la fiducia e il sostegno che dimostra nel permettermi di continuarlo.

Parte III

PROSPETTIVE DELLA ARTIFICIAL INTELLINGENCE FORENSICS

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643016
pp. 303-321 (gennaio 2022)

Policing via Multi-Agent Systems: un nuovo volto per la *digital forensics* (e non solo)?

GIULIA LASAGNI[1]

1. Oltre il fenomeno predittivo: alla ricerca di nuovi paradigmi investigativi

Se in principio era solo fantascienza, oggi ricordarlo pare quasi banale: grazie a capacità di analisi statistica che non trovano confronti sul piano umano e ad una capillarità paragonabile a quella del diritto stesso[2], Intelligenza Artificiale (IA) e algoritmi stanno trasformando alla radice le attività umane, a partire dai paradigmi decisionali[3].

Il processo penale[4] non sfugge al fenomeno, anzi; queste tecnologie costituiscono ormai un elemento costante dei dibattiti sullo svilup-

[1] Ricercatrice in procedura penale presso l'Università di Bologna.

[2] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Riv Trim Dir pen cont* 2020, 4, p. 76-77.

[3] J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data,* 78, *Ohio St L J* 2017, p. 1219; L. FLORIDI, *The 4th Revolution. How the Infosphere Is Reshaping Human Reality*, New York, OUP 2014, p. 1-24; M. HILDEBRANDT, *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Cheltenham-UK, Northampton-MA, Edward Elgar 2015, p. 42 ss.

[4] Specialmente nella fase preliminare e in misura minore, in quella esecutiva, mentre rispetto alla fase dibattimentale e più precisamente alla decisione sul merito, la materia penale si presenta (ancora?) come un campo tendenzialmente sperimentale, specialmente se confrontato con altri settori, come quello civile (dove famoso è ad esempio il sistema estone, v. E. NILLER, *Can AI Be a Fair Judge in Court? Estonia Thinks So*, in *Wired*, 25/03/2019). Negli ultimi anni, infatti, la maggior parte delle più autorevoli ricerche condotte in questo senso si attesta su livelli di accuratezza dei risultati, cioè sulla capacità del sistema informatico di replicare le decisioni umane di riferimento, stimabili intorno all'80% (v. D.M. KATZ, M.J. BOMMARITO II, J. BLACKMAN, *A general approach for predicting the behavior of the Supreme Court of the United States*, in *PLoS ONE* 2017, 12(4): e0174698, p. 14 (70,2%); R. GUIMERÀ, M. SALES-PARDO, *Justice Blocks and Predictability of U.S. Supreme Court Votes*, in *PLoS ONE* 2011, 6(11): e27188m, p. 4 (71 to 83%); N. ALTREAS, D. TSARAPATSANIS, D. PREOȚIUC-PIETRO, V. LAMPOS, *Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective*, in *PeerJ Comp Sc Op Acc* 2016, p. 2 (79%)). Tali livelli di accuratezza, anche al netto di altre considerazioni (ad es. che la compa-

po delle politiche di giustizia criminale. Ciò è evidente soprattutto rispetto a talune tecnologie, cosiddette "predittive", cioè a quegli strumenti che mirano ad identificare *ex ante* taluni profili fattuali dell'attività illecita (tempo e luogo di commissione, tipologia delle vittime)[5] o la possibile occorrenza di comportamenti individuali (tipico, l'esempio della recidiva)[6].

Numerose sono le voci che, in letteratura, hanno evidenziato le significative criticità derivanti dall'uso di questi mezzi: dal rischio di discriminazione[7] alla possibilità, soprattutto nella loro dimensione individuale, di rendere meramente illusori alcuni pilastri fondanti del giusto processo, quali la presunzione di innocenza, il diritto alla motivazione[8] o quello ad un rimedio effettivo[9].

La giusta attenzione data a tali strumenti non deve però suggerire che la componente predittiva rappresenti necessariamente il principale apporto che l'IA può fornire al processo penale.

Da un lato perché, come rilevato, il termine stesso "predizione" tende a creare false aspettative, se riferito alla costruzione di scenari sì

rabilità fra le percentuali riportate è tutto sommato limitata, considerando che le ricerche non sono state sviluppate sulla base di metodologie necessariamente omogenee) hanno fatto ritenere "premature at the current time to imagine such systems replacing judges" (COE, *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in particular algorithms) and Possible Regulatory Implications*, 6/10/2017, p. 11).

[5] Fra cui *PredPol*, *XLaw* (*Delia), CAS*, *PreCobs*, *CAPP-PGH, KLB-Operativ*…l'uso di questi sistemi è talmente comune che in alcune giurisdizioni sono stati creati database per chiarire quali software sono utilizzati da quali forze di polizia. Cfr. https://atlasofsurveillance.org/search?utf8=%E2%9C%93&location=&technologies%5B86%5D=on.

[6] Famigerato, in tal senso, il caso di COMPAS, ma gli esempi sono numerosi (tra cui HART, SASSI, LSI-R, PSA,).

[7] Cfr., *ex multis*, A.Z. HUQ, *Racial Equity in Algorithmic Criminal Justice*, 6 *Duke Law Journal* 2019, 68, p. 1109; S. BRAYNE, *Big Data Surveillance: The Case of Policing*, 82 *Am Soc Rev* 2017, 5, p. 977; C.R. EPP, S. MAYNARD-MOODY, D. HAIDER-MARKEL, *Pulled Over: How Police Stops Define Race and Citizenship*, Chicago, University of Chicago Press 2014, p. 117-119.

[8] V., *ex multis*, C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* New York, Crown Publishers 2016; W.S. ISAAC, *Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice*, 15 *Ohio St J Crim L* 2018, p. 543 ss; S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, Springer 2020, p. 94 ss; M. CAIANIELLO, *Dangerous Liaisons. Potentialities and risks deriving from the interaction between Artificial Intelligence and preventive justice*, in *EJCCLCJ* 2021, 29, 1; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei rischi assessment tools tra Stati uniti ed Europa*, in *Dir pen cont,* 29.05.2019.

[9] G. CONTISSA, G. LASAGNI, *When it is (also) algorithms and AI that decide on criminal matters: In search for an effective remedy*, in *EJCCLCJ* 2020, 28, 3, p. 280 ss.

accurati, ma inesorabilmente riferiti alla descrizione del passato[10]. Dall'altro, perché le potenzialità dell'IA sembrano aprire la strada a forme di interazione ben più profonde fra uomo e macchina. I sistemi di riconoscimento facciale, ad esempio, rappresentano certamente un primo tentativo di ridefinizione dei paradigmi investigativi, peraltro costellato da numerose criticità[11] e sviluppato principalmente nell'ottica dell'inquirente.

Il presente contributo vuole indagare sulle potenzialità di un diverso approccio, che prende le mosse dai caratteri fondanti di taluni sistemi IA noti come *Multi-Agent Systems* (MAS)[12].

Dopo una breve ricognizione delle principali caratteristiche di questa tecnologia, si dirà innanzitutto come tali strumenti si stiano già dimostrando un supporto essenziale per taluni segmenti investigativi (§ 2).

A fronte delle sfide immani poste dalla gestione dei *big data*, infatti, i limiti (umani, economici e temporali) delle risorse messe in campo nella quotidianità delle indagini rendono estremamente concreto il rischio di non riuscire ad identificare (del tutto, o in tempi utili) le informazioni veramente rilevanti.

Ciò è particolarmente evidente in alcuni ambiti, come l'antiriciclaggio o la lotta al finanziamento del terrorismo, nei quali la difficoltà di gestire enormi masse (potenzialmente) informative si sposa a talune criticità peculiari, che, come si dirà, richiedono anche agli strumenti di IA di assumere una veste particolarmente strutturata per poter fornire un apporto significativo (§3).

[10] Cfr. S. QUATTROCOLO, Intervento alla *Conversazione del 20 ottobre 2020,* in *Processo penale e Intelligenza Artificiale*, Position Paper 1, Fondazione Leonardo 2020, p. 17-18; CAIANIELLO, *op. cit.*, p. 8: "[statistics] cannot tell us with precision anything that concerns the position of a single individual".

[11] Cfr. I. NERONI REZENDE, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective,* in *NJECL* 2020, 11, 3, p. 375 ss; J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *Sist pen* 28 marzo 2020.

[12] Con l'espressione "Multi-agent systems" ci si riferisce a sistemi informatici complessi, risultanti dall'interazione di diversi agenti artificiali "intelligenti"; essi costituiscono oggetto di studio e ricerca da parte della più attenta letteratura sin dalla fine degli anni '90 (cfr., ad es., R. CONTE, R. FALCONE e G. SARTOR, *Introduction: Agents and Norms How to Fill the Gap*, in *Artificial Intelligence and Law* 1999, 7, p. 1–15; C. CEVENINI e A. OSKAMP, *Proceedings of the 4th International Workshop on the Law of Electronic Agents*, LEA 2005), sebbene le potenzialità di questi strumenti nell'ambito penale di cui qui si tratta siano emerse solo successivamente e rimangono, in gran parte, inesplorate.

La tecnologia MAS, tuttavia, presenta in nuce profili ben più rivoluzionari per la (ri)definizione dei paradigmi investigativi all'interno del processo penale.

Nel contributo, in particolare, si suggerisce come questi strumenti (e soprattutto alcune applicazioni specifiche, come i *MultiAgent Digital Investigation Toolkits*) potrebbero rivelarsi uno strumento formidabile per ampliare la nozione di *fairness,* e quindi la tutela dei diritti di difesa, già nella fase delle indagini. Intervenendo nel processo di formulazione, valutazione e selezione delle ipotesi investigative, i MAS potrebbero infatti contribuire ad evitare, o almeno a ridurre, alcuni errori tipicamente umani dei processi investigativi, spesso causa di veri e propri errori giudiziari, come il cosiddetto *tunnel vision effect* (§ 4).

Naturalmente, l'ambito limitato di questa analisi consente solo di iniziare a far luce su tale potenziale; le effettive capacità degli strumenti MAS nel settore giuridico, e penale nello specifico, dovranno essere accuratamente testate prima che ciò si possa eventualmente trasformare in realtà operativa.

E tuttavia, se pure le macchine non hanno (ancora?) una vera capacità di previsione e le capacità diagnostiche umane si confermano piuttosto limitate, il giurista non può esimersi oggi dal tentare di proporre una visione per un loro futuribile utilizzo.

Tutto fa presagire che la tecnologia IA sia qui per restare; le forme di tale convivenza, però, non sono ancora definite o, almeno, non completamente.

In questo spazio precario può, e forse deve, insinuarsi la possibilità di immaginare nuovi modi per mettere la tecnologia automatizzata al servizio di una giustizia penale non solo più efficiente sul lato repressivo, ma anche più consapevole della necessità di non arrendersi alle proprie, numerose, fragilità. Una giustizia, tutto sommato e forse paradossalmente, più umana.

2. I sistemi "multi-agente"

Ci sono problemi troppo complessi per essere risolti con impostazioni di ragionamento predefinite e che richiedono invece approcci strutturati ma, al tempo stesso, dotati di una certa versatilità. Con qualche approssimazione, questa considerazione può ritenersi alla base dello

sviluppo di quella forma complessa di tecnologia IA, chiamata *Multi-Agent Systems*[13].

Già a partire da tale vocazione, questi sistemi presentano quindi alti profili di interesse per contesti incerti come le indagini penali, in cui la ricerca di soluzioni non segue logiche chiaramente precostituite. Le analogie con la materia penale, però, non si fermano qui.

Visto dall'ottica del penalista, infatti, il funzionamento interno dei MAS presenta punti in comune non irrilevanti con l'organizzazione delle squadre investigative di polizia.

Innanzitutto, i MAS si fondano sull'azione coordinata di diversi "agenti" automatizzati. Per ottenere il risultato desiderato, questi ultimi cooperano e interagiscono tra loro, rimanendo, tuttavia, autonomi. Ad ogni agente è assegnato un compito specifico; ed è l'*intenzione* di raggiungere questo obiettivo a modellare, in modo razionale ma non necessariamente predefinito, l'azione di ciascuno[14].

Gli agenti MAS, inoltre, devono anche essere "in qualche modo" organizzati[15]. A tal fine, il loro operato si estrinseca sul tracciato di un set dato di norme: ad esempio, gli agenti potrebbero essere inquadrati in una struttura gerarchica, al cui vertice si trova un manager operativo, che si occupa anche della distribuzione dei compiti[16].

Non stupisce pertanto che questa tecnologia, fra le molteplici applicazioni, trovi un terreno particolarmente fecondo in campo investigativo, anche nella materia penale.

[13] K.V. HINDRIKS, *The Shaping of the Agent-Oriented Mindset: Twenty Years of Engineering MAS*. In Dalpiaz F, Dix J, van Riemsdijk MB (eds), *Engineering Multi-Agent Systems*, Revised Selected Papers, Cham, Springer 2014, p. 4.

[14] Cfr. HINDRIKS, *op. cit*., p. 2; M. WOOLDRIDGE, N.R. JENNINGS, *Intelligent agents: Theory and practice*, in *The Knowl Eng Rev* 1995, 10, p. 115; A.S. RAO, M.P. GEORGEFF, *Modeling Rational Agents within a BDI-Architecture*. In Allen J, Fikes R, Sandewall E (eds), *Proceedings of the 2nd International Conference on Principles of Knowledge Representation and Reasoning* (KR 22-25 aprile 1991), Cambridge, USA, Morgan Kaufmann, p. 473 ss.

[15] Così HINDRIKS, *op. cit*., p. 4.

[16] B.W.P. HOELZ, C. GHEDINI RALHA, R. GEEVERGHESE, *Artificial Intelligence Applied to Computer Forensics*, Proceedings of the 2009 *ACM symposium on Applied Computing*, p. 884. La specifica struttura organizzativa può ovviamente variare a seconda delle esigenze da soddisfare e della complessità dei problemi di riferimento (v., ad es., la struttura articolata illustrata da V. GANESCH, *A Cyber Crime Evidence Collection and MultiAgent Digital Investigation Toolkit*, in *IJCRT* 2018, 6, Issue 1, p. 97).

2.1. *MAS e digital forensics*

L'analisi dei dati trova oggi nell'impiego di strumenti di IA un drastico fattore di cambiamento, che coinvolge sia le modalità di ricerca della prova, sia, di conseguenza, la delimitazione delle concrete aspettative di riservatezza dei singoli.

A fronte di una massiccia e costante produzione di dati digitali in ogni aspetto della vita privata e professionale, lo sforzo investigativo per analizzare tali informazioni sembra infatti doversi necessariamente affidare all'IA per mantenere qualche speranza di successo[17]. Ed in effetti, in questo senso si iscrivono già numerosi applicativi, come l'*Open Computer Forensics Architecture* (OCFA)[18], il *Digital Forensics Framework* (DFF)[19], *Fiwalk*[20] o l'*Advanced Automated Disk Investigation Toolkit* (AUDIT)[21].

Spesso, però, gli investigatori devono operare in contesti nei quali la sfida principale è rappresentata non tanto dall'identificazione della potenziale soluzione del caso, quanto dalla necessità di selezionare gli elementi rilevanti a tal fine[22]. Ciò è tanto più frequente in caso di dati informatici, dove è evidente la sproporzione fra le enormi quantità di informazioni e le risorse limitate degli inquirenti, che per di più devono ormai svolgere simili attività nella gran parte delle inchieste penali. In questo senso, i *Multi-Agent Systems* sembrano offrire un contributo particolarmente promettente[23].

[17] Fra i primi a proporre simili applicazioni, v. T. STALLARD, K. LEVITT, *Automated analysis for digital forensic science: Semantic integrity checking*, Washington, DC: IEEE Computer Society 2003, p. 160 ss. Cfr. anche le successive proposte di N. LIAO, S. TIAN, T. WANG, *Network forensics based on a fuzzy logic and expert system*, in *Comp Comm* 2009, vol 32, 17, p. 1881 ss e J. FIZAINE, N. CLARKE, *A crime-dependent automated search engine for digital forensics*, in *Adv Comm, Comp, Net Sec* 2013, vol 10, p. 73.

[18] O. VERMAAS, J. SIMONS, R. MEIJER, *Open computer forensic architecture a way to process terabytes of forensic disk images*, in E Huebner, S Zanero (eds.), *Open Source Software for Digital Forensics*, New York, Springer 2010, p. 45 ss.

[19] www.digital-forensic.org, Francia, 2016.

[20] S. GARFINKEL, *Automating disk forensic processing with SleuthKit, XML and Python*, in *Proc Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering* 2009, p. 73 ss.

[21] KARABIYIK-AGGARWAL, *op. cit*., p. 381 ss.

[22] Così, recentemente, R. BRIGHI, M. FERRAZZANO, *Digital Forensics: Best Practices and Perspective*. In Caianiello M, Camon A (eds), *Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Wolters Kluwer/CEDAM 2021, p. 43 ss.

[23] Cfr. N. BEEBE, J.G. CLARK, *A hierarchical, objectives-based framework for the digital investigations process*, in *Dig Inv* 2005, 2(2), p. 147 ss; U. KARABIYIK, S. AGGARWAL, *Ad-*

Tra la vasta gamma di tecnologie MAS, si pone qui l'attenzione ad uno specifico strumento, il *MultiAgent Digital Investigation toolKit* (MADIK).

I sistemi MADIK sono composti da un insieme di agenti software intelligenti, impostati per eseguire diverse analisi di *digital forensics*. L'idea alla base dell'uso di tale tecnologia è quella di facilitare la catalogazione dei dati, attraverso l'attribuzione di un punteggio che li classifica da "*Absolutely Irrelevant*" a "*Probably Case-Relevant*"[24]. Per far ciò, ogni agente si fonda su di un set di regole e conoscenze derivate dall'esperienza umana (grazie, ad esempio, al *training* effettuato con agenti di polizia).

Strumenti come i MADIK possono quindi risultare preziosi per il processo penale, così come in tutte le forme di indagine digitale (si pensi alle controversie sul luogo di lavoro).

Simili tecnologie mostrano però un alto potenziale anche sul fronte della prevenzione, dove le applicazioni IA sono largamente invocate e spesso già in uso. Forse il riferimento più immediato in questo senso va alle indagini condotte sui *social media,* per identificare potenziali criminali o modelli di condotte criminose e ridurre la vittimizzazione[25]. Le applicazioni, però, possono essere assai varie: dal controllo dei cd. *hate crimes*, al contrasto del terrorismo o del crimine organizzato[26].

Non sempre, però, l'adozione di sistemi "semplici" di IA sembra riuscire a rispondere alle concrete esigenze del settore di riferimento. Esempio significativo in questo senso è quello della lotta contro il fi-

vanced Automated Disk Investigation Toolkit. In Peterson G., Shenoi S. (eds) *Advances in Digital Forensics*, vol 484, Cham, Springer, 2016, p. 379 ss.

[24] HOELZ *e a., op. cit.*, p. 883 ss; GANESCH, *op. cit*., p. 96 ss.

[25] Cfr. M. RIFKIND, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby*. House of Commons, Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office, 2014, p. 143 ss.; A. TOOR, *Automated Systems Fight ISIS Propaganda, but at What Cost?*, in *The Verge* 2016 (ultimo accesso online settembre 2021).

[26] V., ad es., le proposte formulate da J.R. GONÇALVES EVANGELISTA, R.J. SASSI, M. ROMERO, D. NAPOLITANO, *Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence*, in *J App Sec Res* 2020, p. 1 ss; R. SCRIVENS, T. GAUDETTE, G. DAVIES, R. FRANK, *Searching for Extremist Content Online Using the Dark Crawler and Sentiment Analysis*. In Deflem M, Silva DMD (eds), *Methods of Criminology and Criminal Justice Research*, Emerald Publishing 2019, p. 179 ss; A. PANAGIOTOU, B. GHITA, S. SHIAELES, K. BENDIAB, *FaceWallGraph: using machine learning for profiling user behaviour from Facebook Wall*. In O Galinina, S Andreev, Y Koucheryavy and S Balandin (eds), *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, vol 11660, Springer 2019, p. 125 ss; L. BALL, *Automating social network analysis: A power tool for counter-terrorism*, in *Sec J* 2016*,* 29, p. 147 ss.

nanziamento del terrorismo e il riciclaggio di denaro, dove l'uso dell'IA sembra ormai imprescindibile, ma dove pure talune circostanze sembrano ridurne drasticamente l'effettivo potenziale. A fronte di tali perplessità, la struttura composita dei sistemi MADIK, e delle tecnologie MAS in generale, presenta oggi profili di grande interesse.

3. Un ambito di applicazione problematico: la lotta al riciclaggio e al finanziamento del terrorismo

Sebbene una disamina puntuale dei meccanismi di prevenzione AML/CFT[27] vada ben oltre i limiti del presente contributo, vale qui la pena ricordare brevemente alcune delle caratteristiche di questo sistema, che lo rendono tanto appetibile, quanto ostico alla applicazione di strumenti IA.

Come noto, tali regimi si fondano oggi sui cd. meccanismi di Segnalazione delle Operazioni Sospette (SOS).

Essenzialmente, il fulcro di tali modelli è rinvenibile nel dovere di alcuni privati qualificati (fra cui banche e istituzioni finanziarie) di notificare alle autorità di contrasto attività potenzialmente illecite. Nella maggior parte dei casi, queste autorità si identificano con le *Financial Intelligence Units* (FIU), agenzie appositamente create – su stimolo degli standard FATF[28] – per fungere da centri di ricezione e analisi delle segnalazioni[29].

Secondo opinione largamente condivisa, non è necessariamente il numero di SOS a determinare la maggiore o minore efficienza preventiva e repressiva dell'intero sistema. Fattori ben più significativi, a tal fine, sono piuttosto identificati nella qualità delle segnalazioni prodotte, così come nella disponibilità di risorse che le

[27] Anti-Money Laundering and Countering the Financing of Terrorism, AML/CFT in breve. Per una recente analisi comparata e approfondita, v. B. VOGEL, J.B. MAILLART (eds), *National and International Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, Intersentia, Cambridge–Antwerp–Chicago 2020.

[28] Si vedano le definizioni (p. 122 ss) e la *Recommendation* (29) e le relative note interpretative (p. 95 ss) degli International standards on combating money laundering and the financing of terrorism & proliferation elaborati dalla FATF nel 2012.

[29] Per una ricostruzione generale delle diverse tipologie e funzioni delle *FIU*, cfr. volendo, G. LASAGNI, *Banking Supervision and Criminal Investigation. Comparing the EU and US Experiences*, Cham, Springer 2019, p. 93 ss.

FIU posso impiegare nella propria analisi, ad esempio in termini di tempo e di personale disponibile[30].

L'attuale paradigma sanzionatorio in questo ambito genera però oggi alcune distorsioni: mentre la mancanza o scarsa cooperazione è punita, anche severamente, l'*overproduction* di SOS non è causa di responsabilità per le entità obbligate. In diversi ordinamenti si riscontrano quindi oggi fenomeni di cd. *umbrella reporting*[31], cioè l'invio alla FIU di segnalazioni in grandi quantità che, più che mirare alla prevenzione dei fenomeni criminosi, tendono a ridurre la potenziale responsabilità penale e amministrativa dei soggetti obbligati.

L'uso difensivo delle SOS si riflette però inevitabilmente in segnalazioni di scarsa qualità, che non apportano contributi sostanziali all'attività di contrasto[32]. Una simile conclusione è tanto più aggravata alla luce delle risorse limitate a disposizione delle FIU, soprattutto in termini di personale dedito all'analisi dei dati ricevuti.
In tale contesto, con transazioni finanziarie che hanno assunto una dimensione digitale preponderante, l'adozione di tecnologie di IA è da più parti presentata come la panacea in grado di porre rimedio a tutte (o quasi) le inefficienze del settore.

Tale passaggio, per la verità, non è necessariamente di facile attuazione. Sul piano legale, soprattutto, la generalizzata mancanza di basi giuridiche non consente oggi di assicurare un uso dell'IA rispettoso dei diritti fondamentali. Anche quando pensati per fini preventivi e quindi formalmente estranei alla materia penale[33], infatti, l'adozione

[30] V. *ex multis*, ONU, Seventh Report *of the Analytical Support and Sanctions Monitoring Team*, Est pursuant to Sec Counc Res 1526 (2004)' (2007) S/2007/677; ID., Eighth Report *of the Analytical Support and Sanctions Monitoring Team*, Est pursuant to Sec Counc Res 1526 (2004)' (2008) S/2008/324. Per dati relativi all'UE, a titolo esemplificativo, C. TAVARES, G. THOMAS, M. ROUDAUT, *Money laundering in Europe: Report of work carried out by Eurostat and DG Home Affairs*, *Eurostat Methodologies & Working Paper EC* 2010, p. 1 ss; G. FAVAREL-GARRIGUES, T. GODEFROY, P. LASCOUMES, *Reluctant partners? Banks in the fight against money laundering and terrorism financing in France*, *Sec Dial* 2011, 42, 2, p. 179 ss.

[31] Su cui v. FAVAREL *e a*, *op.cit.,* p. 179 ss; O. BURES, *Public-private partnerships in the fight against terrorism*, *Cr L Soc Change* 2013, 60, p. 444; S. RIONDET, *The value of public-private partnerships for financial intelligence*, *J Fin Compl* 2018, 2, 2, 148.

[32] Nell'UE, ad es., solo una minima parte di SOS (ca 10%) porta ad ulteriori approfondimenti (es. apertura di indagini), cfr. Europol, *From suspicion to action: Converting financial intelligence into greater operational impact,* 2017.

[33] Sebbene da tempo si sottolinei l'esigenza di tenere in considerazione la circolazione degli elementi probatori fra procedimenti di diversa natura, v. per tutti R. ORLANDI, *Atti e in-*

di questi strumenti non può esimersi quantomeno dal rispetto degli standard di tutela formulati dalla Corte di giustizia a partire dalla nota pronuncia *Digital Rights Ireland*[34].

In attesa di verificare l'esito delle recenti proposte legislative europee in materia,[35] tale carenza oggi genera un contesto in cui le autorità di contrasto sono tendenzialmente limitate a forme di sperimentazione[36], mentre nel settore privato, di fatto non regolamentato, l'adozione di simili tecnologie è relativamente frequente[37].

Ciò è dovuto anche alla convinzione che l'IA potrebbe rivelarsi determinante nell'assicurare una analisi dei dati più rapida ed accurata, consentendo di identificare a costi inferiori i potenziali indicatori delle condotte a rischio.

Caratteri tipici delle transazioni, come ammontare, posizione geografica, identità dei soggetti coinvolti e deviazioni dalle attività medie degli operatori finanziari, potrebbero infatti essere analizzati con più profitto, si dice, dall'intelligenza artificiale[38].

Da un lato, questa tecnologia potrebbe procedere ad una prima scrematura delle informazioni, lasciando solo un numero limitato di

formazioni della autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite, Giuffrè, Milano 1992, p. 79 ss.

[34] *Digital Rights Ireland*, 8 aprile 2014, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, applicata al caso specifico da W. MAXWELL, A. BERTRAND, X. VAMPARYS, *Are AI-based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights?*, *ICML 2020 Law & ML Workshop*, 2020, Vienna, p. 5 ss.

[35] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, Brussels, 21.4.2021, COM(2021) 206 final 2021/0106 (COD).

[36] Si vedano ad esempio i casi dell'autorità inglese FCA nel febbraio 2021 (DigitalSandbox Pilot), dell'australiana AUSTRAC o di quella di Singapore, riportati da FSB, *Artificial intelligence and machine learning in financial services. Market developments and financial stability implications*, 2017, p. 23-24. Anche la Banca d'Italia non è estranea da questa tendenza, avendo lanciato la costruzione di un sistema IA per la identificazione di indicatori di rischio basato sulla cd. *fuzzy logic* (cfr. FATF, *Opportunities and Challenges of New Technologies for AML/CFT*, Parigi, 2021, p. 23).

[37] V. per tutti, IBM, *Fighting financial crime with AI. How cognitive solutions are changing the way institutions manage AML compliance, fraud and conduct surveillance* 2019 e Deloitte, *The case for artificial intelligence in combating money laundering and terrorist financing. A deep dive into the application of machine learning technology* 2018. Secondo EBA, *Report on Big Data and Advanced Analytics*, 2020, EBA/REP/2020/01, p. 8, soluzioni di *Big Data and Advanced Analytics* sono già utilizzate dal 64% delle istituzioni finanziarie.

[38] M. TEITLER, *ML for AML: Is Artificial Intelligence Up to the Task of Anti-Money Laundering Compliance?,* in *The Global Anticorruption Blog*, 31 maggio 2021.

casi alla successiva verifica umana[39]. Dall'altro, l'IA potrebbe anche, grazie alle tecniche di *data mining*, contribuire alla scoperta di *pattern* sospetti ulteriori rispetto a quelli già identificati dai membri delle FIU[40]. Tutto ciò dovrebbe quindi consentire una vigilanza di maggiore qualità, cioè al tempo stesso più capillare, rapida e rispettosa delle limitate risorse umane a disposizione[41].

3.1. *Limiti del settore e potenzialità dei MAS*

Nonostante queste premesse, alcuni profili specifici del settore AML/CFT impongono un atteggiamento cauto nel valutare l'effettivo potenziale dei sistemi di IA, almeno nella loro accezione "non distribuita".

Non si intende qui fare riferimento alle criticità, ampiamente commentate, che caratterizzano oggi tutti gli strumenti di intelligenza artificiale, dalla mancanza di *explainability*, al rischio discriminatorio.[42] Sono piuttosto alcuni tratti distintivi della materia a sollevare dubbi sulla effettiva possibilità di addestrare macchine IA a produrre risultati di qualità in questo ambito.

Nel processo di *training*, infatti, la verifica del risultato emesso (nel caso specifico, la classificazione di una determinata transazione come "sospetta" o di determinate condotte come "rischiose") costituisce una fase imprescindibile. Ciò presuppone, tuttavia, che la componente umana sia in grado di definire in termini piuttosto precisi il cd. *known truth value*, cioè la corretta assegnazione alla relativa categoria.

Nei regimi AML/CFT, però, questo compito è particolarmente arduo poiché, a fronte di una gamma di dati particolarmente variegata[43],

[39] Naturalmente gli usi potenziali non si limitano a quelli qui indicati, ma potrebbero, ad esempio, coinvolgere anche le ordinarie obbligazioni di Costumer Due Diligence, come sottolineato da FATF, *op. cit.*

[40] Così FATF, *op. ult. cit*., p. 67; MAXWELL *e a*., *op. cit*., p. 13-14; FSB, *op. cit.*, p. 23; N. AN LE KHAC, S. MARKOS, M.T. KECHADI, *A Data Mining-Based Solution for Detecting Suspicious Money Laundering Cases in an Investment Bank,* 2nd International Conference on Advances in Databases, Knowledge, and Data Applications 2010, p. 235 ss.

[41] FATF, *op. ult. cit*., p. 20 ss; v. anche i risultati preliminari di M.K. WEBER *e a*., *Scalable Graph Learning for Anti-Money Laundering: A First Look,* NeurIPS Workshop on Challenges & Opportunities for AI in Financial Services, Montreal, Canada 2018, p. 3, secondo cui "working with private bank data, we have found these methods can reduce false positives by 20–30% when performed by expert analysts".

[42] Fra la sterminata letteratura in materia, v. V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia,* in U Ruffolo, *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, Giuffrè 2020, p. 551 ss.

[43] E non sempre raccolta in modo strutturato, v. EBA, *op. cit*., p. 25.

simili valutazioni sono spesso compiute in modo unilaterale dal soggetto obbligato (la banca). Quest'ultimo, tuttavia, nella maggior parte (se non nella quasi totalità) dei casi *non* riceve dalle autorità di contrasto un feedback sulla utilità o accuratezza delle segnalazioni fatte, o quantomeno non lo riceve in tempi utili (dovendo attendere, ad esempio, la caduta del segreto istruttorio)[44]. Il privato, quindi, difficilmente sarà in grado di misurare con certezza la pertinenza della condotta segnalata.

Senza un mutamento di approccio, i sistemi IA per la selezione degli indicatori di rischio potrebbero pertanto rimanere "as good as the previous bank compliance team"[45].

La comprensione dei fenomeni di riciclaggio e finanziamento del terrorismo, inoltre, richiede sovente un'analisi continuativa nel tempo o riferita alla condotta di multipli soggetti. La complessità di questi illeciti li rende infatti difficilmente identificabili ad un esame parcellizzato, che non tenga conto del contesto. Per apportare un contributo davvero significativo alla selezione delle operazioni sospette, quindi, l'analisi automatizzata dovrebbe essere in grado di sostenere una certa complessità di visione.

Pur rifuggendo da soluzioni semplicistiche, la struttura ramificata dei *Multi-Agent Systems* sembrerebbe offrire, in tal senso, un interessante modello di riferimento.

Si potrebbe immaginare, ad esempio, un sistema composito di identificazione automatica degli indicatori di rischio, in cui la parte di analisi viene distribuita fra più agenti artificiali, sottraendo alla componente umana una attività ad alto costo in termini di tempi e professionalità richieste.

[44] G. Lasagni, Public Private Partnerships *nell'antiriciclaggio e antiterrorismo: una nuova forma di* outsourcing *del processo penale?, Riv. Trim. Dir. pen. cont*., 3, 2021.

[45] Cfr. Maxwell *e a*., *op. cit*., p. 14-23. Vi è anche chi non manca di sottolineare come i casi ML/FT non costituiscano un numero significativo per poter addestrare in modo efficace un sistema IA; se tale considerazione può mantenere un certo valore in relazione alle condotte terroristiche (Bures, *op. cit*., p. 439 ss), perlomeno rispetto al fenomeno del riciclaggio la mancanza di dati sembra però spesso derivare più dalla scarsa capacità di (talune) FIU di segnalare le condotte sospette all'autorità giudiziaria, piuttosto che alla effettiva carenza di tali condotte criminose (v., per tutti, il recente caso tedesco: https://m.tagesspiegel.de/politik/kennt-man-sonst-nur-von-populistischen-staaten-laschet-geht-scholz-wegen-ministeriums-durchsuchung-scharf-an/27596548.html).

L'applicazione di talune forme di MAS, anche sul modello MADIK, potrebbe inoltre comportare un miglioramento significativo in termini di qualità dei risultati prodotti.

Questo non tanto per una (tendenziale) maggiore accuratezza dei sistemi informatici in sé, ma per il grande potenziale di questa particolare tecnologia nella riduzione dei margini di errore dei procedimenti di selezione. Come si argomenterà di seguito, infatti, i MAS sembrano avere un potenziale sinora inespresso in ambito penale, che potrebbe portare ad un livello di integrazione, finora senza precedenti, tra capacità umane e artificiali nella fase investigativa.

4. Un approccio *AI-oriented* all'incertezza delle indagini

Particolarmente interessante, a questo proposito, è la "natura distribuita" del citato sistema MADIK.

L'idea alla base di questa caratteristica si riferisce al fatto che un compito (ad esempio l'identificazione di informazioni rilevanti su un dispositivo) non viene svolto solo da un agente alla volta, ma, contemporaneamente, da più agenti, che producono ciascuno la propria valutazione.

Questo modello organizzativo ha un impatto diretto sulla struttura del processo decisionale del sistema. Infatti, poiché agenti diversi possono produrre risultati divergenti, spetta al responsabile operativo del sistema (anch'esso automatizzato) trovare una soluzione. Diverse regole possono essere stabilite a questo proposito.

Ad esempio, Hoelz *e a*. descrivono un sistema in cui si decide di affidarsi a quegli agenti che – a causa del loro specifico addestramento – hanno eseguito meglio in passato compiti simili. Se i risultati forniti da uno specifico agente sono ritenuti imprecisi, la "fiducia" del manager sulla sua capacità di rispondere al dato problema diminuirà. Le sue prestazioni avranno quindi probabilmente meno peso in future interrogazioni dello stesso tipo. Al contrario, quando le prestazioni dell'agente sono ritenute positive, la fiducia del manager aumenta, e questo apprezzamento sarà richiamato anche in indagini future[46].

Questo modello non rappresenta naturalmente l'unico paradigma possibile. Ad esempio, si potrebbe scegliere di non dare un peso pre-

[46] HOELZ *e a., op. cit.*, p. 886; v. anche GANESCH, *op. cit*., p. 97.

ponderante all'operato precedente, onde evitare di fare eccessivo affidamento su valutazioni compiute in contesti diversi.

A prescindere dai criteri adottati in tale procedimento decisorio, però, ciò che qui più rileva è la capacità dei MAS di far leva sulla nozione di conflitto, invece di evitarlo.

Tale caratteristica rappresenta un elemento fondamentale per misurare l'impatto di questa tecnologia nel processo penale.

Coloro che promuovono il ricorso all'IA e ai sistemi informatici spesso lo fanno con l'intento (la speranza) di rendere più oggettivo ed efficiente l'assai imperfetto sistema umano di accertamento penale, mirando al raggiungimento di risultati più accurati. In altre parole, di ottenere una giustizia più equa, meno soggetta a influenze variabili, soggettive e potenzialmente discriminatorie[47]. Questo è certamente un obiettivo positivo e desiderabile, che si pone a favore di un dispiegamento consapevole dell'IA alla materia in questione.

I MAS, tuttavia, e soprattutto i sistemi MADIK, aprono anche a una prospettiva diversa, cioè ad un uso della tecnologia IA non per perseguire la certezza (giuridica), ma per gestire razionalmente l'incertezza del procedimento.

Detto altrimenti, i MAS ci mostrano come la trasformazione dell'attività prognostica umana in calcolo statistico o la capacità di processare enormi quantità di dati non siano, di per sé, l'unico e forse più significativo approccio con cui guardare all'interazione con le macchine in questo settore.

Tecnologie come i *Multi-Agent Systems*, in effetti, sembrano capaci di convivere con un certo grado di complessità e imprevedibilità, tipico delle vicissitudini umane, fra cui anche le indagini penali. Partendo da tale caratteristica, si potrebbe quindi prevedere un ulteriore utilizzo degli strumenti MADIK (o simili): un impiego volto a preservare il

[47] Così C.R. SUNSTEIN, *Algorithms, Correcting Biases*, in *Soc Res: An International Quarterly*, vol. 86, 2, 2019, p. 499 ss; v. anche la significativa considerazione di C. DESKUS, *Fifth Amendment Limitations on Criminal Algorithmic Decision-Making* 2018, 21 *N.Y.U. J. Legis. & Pub. Pol'y*, vol. 21, p. 243: "A judge's bad day or heavy docket does not affect the algorithm"; sulla rilevanza di circostanze quotidiane comuni (come gli orari dei pasti) sulla severità delle sanzioni imposte da giudici umani, v. D. EAGLEMAN, *The Brain. The Story of You*, New York, Pantheon Books and Edinburgh, Canongate Books 2015, p. 266; v. anche G. SARTOR, F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto, in Intelligenza artificiale*. In Ruffolo, *op. cit*., p. 63 ss.

necessario grado di incertezza tipico delle prime fasi del processo investigativo.

Questo segmento del procedimento, infatti, è notoriamente sensibile a margini di errore elevati. In gran parte, ciò è dovuto alla ovvia difficoltà di individuare in via preliminare quale – tra le possibili ipotesi investigative – si rivelerà essere quella corretta.

Tale difficoltà è riconducibile alla stessa natura umana: filosofi e scienziati sociali hanno difatti riconosciuto come il nostro intelletto sia di solito piuttosto in difficoltà nell'affrontare contesti ad opzioni multiple. Si è osservato, in particolare, come una volta adottata una certa interpretazione dei fatti, i passaggi logici successivi siano spesso più orientati alla ricerca di conferme, che alla disamina delle eventuali e, non di rado, persino numerose possibili alternative[48].

Questa tendenza pressoché involontaria alla semplificazione ha ripercussioni significative nelle indagini penali: non è un caso che gli psicologi forensi individuino nella capacità degli investigatori di non predeterminare i propri giudizi nelle prime fasi del procedimento una salvaguardia essenziale contro la commissione di errori giudiziari[49].

Ci si riferisce, in particolare, al cosiddetto *tunnel vision effect*, cioè a quella tendenza per cui gli attori del processo penale tendono a concentrarsi relativamente in fretta su uno specifico sospetto o su una data pista investigativa. Il significato delle prove e degli indizi che po-

[48] Per tutti, F. BACON, *Novum organum*. In EA Burtt (ed.), *The English philosophers from Bacon to Mill* New York, Random House (1939, opera originale del 1620), p. 36: "[Once] adopted an opinion, [it] draws all things else to support and agree with it. And though there be a greater number and weight of instances to be found on the other side, yet these it either neglects and despises, or else by some distinction sets aside and rejects; in order that by this great and pernicious predetermination the authority of its former conclusions may remain inviolate"; più recentemente v. R. NICKERSON, *Confirmation Bias. A Ubiquitous Phenomenon in Many Guises*, 2 *Rev Gen Psyc* 1998, 2, p. 176 ss.

[49] Così, *ex multis*, P.C. WASON, *On the failure to eliminate hypotheses in a conceptual task*, 12 *Quart J Exp Psyc* 1960, 3, p. 129 ss; E.J. LANGE, *The Illusion of Control*, 32 *J Pers Soc Psyc* 1975, 2, p. 311 ss; NICKERSON, *op. cit*., p. 193 ss; C.A. MEISSNER, S.M. KASSIN, *"You're Guilty, So Just Confess! Cognitive and Behavioural Confirmation Biases in the Interrogation Room*, in GD Lassiter (ed.), *Interrogations, Confessions and Entrapment*, New York, Springer 2004, p. 85 ss; K. FINDLEY, M. SCOTT, *The Multiple Dimensions of Tunnel Vision in Criminal Cases*, in *Wisc L Rev* 2006, vol. MMVI, 108, p. 291 ss; I.E. DROR, D. CHARLTON, A.E. PÉRON, *Contextual Information Renders Experts Vulnerable to Making Erroneous Identifications*, in *For Sc Inter* 2006, vol. CLVI, 1, p. 74 ss; A. FORZA, *La psicologia nel processo penale*, Milano, Giuffrè 2008, p. 395 ss.

trebbero costruire il caso a sostegno di tale intuizione tende così ad essere ingigantito, mentre gli elementi che appaiono incoerenti con la ricostruzione prescelta finiscono per essere trascurati o liquidati come irrilevanti o inaffidabili[50].

La *tunnel vision*, tuttavia, più che causata da deliberata malizia o indifferenza, si rivela assai spesso il prodotto della combinazione fra i suddetti limiti di elaborazione cognitiva e le pressioni (politiche, sociali) derivanti dallo specifico contesto[51].

4.1. *MAS: uno strumento per realizzare indagini "più giuste"?*

Gli scienziati sociali evidenziano come la tendenza umana a considerare solo un'ipotesi alla volta, spesso assumendo sin in radice che tale ipotesi sia quella giusta, possa trovare almeno parziale correttivo con adeguato allenamento. Esercitarsi ad identificare ipotesi alternative sin dall'inizio del processo di valutazione può infatti ridurre in modo significativo i margini di errore (anche giudiziario)[52]. In questo contesto, la tecnologia MAS potrebbe essere un modo per rendere più concrete queste aspirazioni.

A tal fine, lo stesso approccio sviluppato per le operazioni di *digital forensics* potrebbe essere applicato dai *Multi-Agent Systems* anche per quanto riguarda le ipotesi investigative.

In questo senso, l'IA potrebbe essere utilmente impiegata per supportare le decisioni degli attori dediti alle indagini, *garantendo che le divergenze nel processo decisionale di selezione delle ipotesi investigative rimangano irrisolte, almeno fino a un certo punto*.

Come si è detto, infatti, le diverse ricostruzioni prodotte dagli agenti artificiali vengono ricondotte ad unità solo con l'intervento del responsabile operativo. Fino ad allora, la natura distribuita del MAS potrebbe essere sfruttata per individuare e sviluppare il maggior numero possibile di scenari esplicativi.

[50] V. D.L. MARTIN, *Lessons About Justice from the "Laboratory" of Wrongful Convictions: Tunnel Vision, the Construction of Guilt and Informer Evidence* 2002, 70 *UMKC L Rev*, p. 847-48; M. RAEDER, *What Does Innocence Have to Do With It?: A Commentary on Wrongful Convictions and Rationality* 2003 *Mich St L Rev*, p. 1327-28.

[51] FINDLEY-SCOTT, *op. cit*., p. 292.

[52] NICKERSON, *op. cit*., p. 211.

Ad esempio, i sistemi multi-agente potrebbero fornire supporto alle forze dell'ordine nella gestione delle piste investigative, non tanto identificando quella statisticamente più probabile di essere "corretta", ma al contrario assicurandosi che nessuna di esse venga esclusa troppo presto dal novero di quelle da tenere in considerazione.

Naturalmente, come è il caso per tutte le applicazioni IA, la tecnologia MAS o MADIK non contiene una formula magica, capace di cancellare in un colpo solo l'effetto dei limiti e dei pregiudizi umani.

In primo luogo, la concreta potenzialità di tali sistemi di operare come "mind-openers" dipende in modo significativo dalla qualità del training ricevuto (dagli esperti umani)[53].

La possibilità di individuare diverse ipotesi investigative alternative e plausibili, ad esempio, dipende largamente dal successo nel comporre una "squadra investigativa artificiale" sufficientemente diversificata. Ciò richiede uno sforzo agli operatori umani che, nell'addestrare gli agenti-macchina, devono cercare di differenziarne sufficientemente i profili, pur mantenendone alta la competenza.

Se ciò venisse garantito, però, il potenziale della tecnologia MAS potrebbe essere dirompente.

L'analisi effettuata dagli agenti automatizzati potrebbe infatti aiutare a testare la fondatezza di ipotesi investigative divergenti o ad identificare ricostruzioni non immediatamente visibili ad occhio umano.

Le competenze dell'IA potrebbero essere utilizzate, in ipotesi, in quei contesti dove le forze dell'ordine, per motivi strutturali o circostanziali, potrebbero in alternativa contare su un personale limitato o, perché no, troppo omogeneo (ad esempio per genere, o etnia).

Ancora, la tecnologia MAS potrebbe aiutare a decifrare le scene del crimine più complesse, dove gli indizi o il materiale rilevante sono scarsi da reperire o difficili da interpretare.

[53] Questo profilo è comunque una questione "risalente", identificata come critica per il buon funzionamento di tutte le tecnologie di apprendimento automatico, e non specificamente dei MAS, cfr., ad es., K. MILLER, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm* 2014, 19 *J Tech L & Pol'y*, p. 106 ss; S. QUATTROCOLO, *Artificial Intelligence, cit.*, p. 67 e, da ultimo, M. ROBERTS, D. DRIGGS, M. THORPE *e a.*, *Common pitfalls and recommendations for using machine learning to detect and prognosticate for COVID-19 using chest radiographs and CT scans,* in *Nat Mach Intell* 2021, 3, p. 199 ss.

In altre parole, il paradigma investigativo dei sistemi multi-agente potrebbe essere utilizzato per evitare che intuizioni potenzialmente di valore vadano perse in una fase iniziale del procedimento, a causa di tempo o di risorse limitati.

Non da meno, i *Multi-Agent Systems* potrebbero essere impiegati in questo senso non sono nell'ottica degli inquirenti.

Questa tecnologia potrebbe infatti essere sfruttata con successo anche dall'imputato, o dalla vittima, per verificare se tutte le potenziali piste investigative siano state debitamente perseguite da chi ha la responsabilità delle indagini. O, in mancanza, per raccogliere elementi significativi su cui fondare l'impugnazione futura delle decisioni fondate su atti di indagine irragionevolmente incompleti.

5. Spunti conclusivi

Questa breve analisi ha cercato di sollevare un velo su un diverso e possibile impiego dell'intelligenza artificiale nell'ambito delle indagini penali e preventive.

Cercare di immaginare nuovi percorsi di tutela per i principi della giustizia penale nella nostra mutevole *hyperhistory*[54] è naturalmente un percorso che porta in questo ambito su sentieri inesplorati e non privi di incidenti.

L'errore è all'ordine del giorno in questa ricerca e le opzioni che sulla carta sembrano facilmente realizzabili, non necessariamente condividono lo stesso destino nella pratica. Questa consapevolezza non può, però, far desistere dalla ricerca di nuove forme di riconoscimento per i diritti fondamentali, che sappiano riaffermarne il valore universale in un mondo in rapida evoluzione tecnologica.

I sistemi multi-agente, per esempio, sembrano aprire prospettive interessanti e potenzialmente innovative su una dimensione tecnologicamente avanzata dell'antico metodo socratico.

La falsificazione come modo per raggiungere la "verità", o ciò che con tale termine viene accolto nel processo penale, è un metodo essenziale per la moderna giustizia democratica. Nella maggior parte

[54] Per il termine, v. FLORIDI, *op. cit.,* p. 24.

degli ordinamenti giuridici, tuttavia, il principio del contraddittorio trova solo una limitata applicazione nella fase delle indagini.

I MAS potrebbero contribuire ad estenderne la portata, includendovi talune fasi iniziali delle indagini e fornendo nuovi strumenti alle forze dell'ordine, così come alle parti, per svolgere con più effettività i rispettivi ruoli.

Naturalmente, le capacità tecniche di questi strumenti dovranno essere ulteriormente testate; così come certamente complessa si prospetta la definizione di un percorso di *training* investigativo altamente specializzato e parimenti necessario per trasformare il potenziale illustrato in realtà operativa.

A fronte di tali incertezze, chi teme che le procedure investigative possano essere svilite da un'eccessiva dipendenza dall'automazione, perlomeno, potrebbe sentirsi rassicurato: la componente umana, infatti, è ben lungi dal diventare irrilevante nel processo penale.

Anzi, quello che i *Multi-Agent Systems* sembrano suggerire è che, talvolta, esitazioni e titubanze, così tipiche della nostra specie, non sono solo *a flaw in the judgment*[55].

Talvolta proprio il "rumore" è invece necessario, per ricordare il valore del dubbio e l'umanità che pulsa dietro le norme e i principi.

Forse, paradossalmente, potrebbero essere proprio le macchine ad aiutarci a non dimenticarlo.

[55] Libera citazione da D. KAHNEMAN, O. SIBONY, C.R. SUNSTEIN, *Noise: A Flaw in Human Judgment*, Little Brown Spark, New York-Boston-London 2021.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643017
pp. 323-342 (gennaio 2022)

Deep Learning per l'analisi del *sentiment*

CORRADO FEDERICI [1]

1. Introduzione

L'analisi del sentiment (AS) è una specialità dell'elaborazione del linguaggio naturale orientata a valutare lo stato d'animo dell'autore di un testo, spesso scritto in risposta ad una precedente pubblicazione. Casi tipici sono i commenti in calce ad un articolo apparso su un blog o ad un post presente nella bacheca di un profilo Facebook. I campi di applicazione dell'AS sono praticamente illimitati, potendo spaziare dal marketing per stabilire il posizionamento di un marchio, alla politica per valutare l'orientamento dell'elettorato su specifici argomenti, alla business intelligence per suggerire i prodotti più aderenti alle esigenze del cliente, fino alle scienze mediche per permettere alle strutture ospedaliere di fornire servizi migliori. Come avviene per gli altri domini applicativi, anche la pubblica sicurezza può beneficiare delle tecniche di AS per cercare di rilevare se le grandi piazze virtuali, in particolare i social media, divengono teatro campagne architettate da organizzazioni criminali mosse, dal fine economico o politico, per orientare il consenso, diffamare, incitare all'odio o creare proselitismo. Tuttavia, la crescita verticale della quantità di contenuti pubblicati ogni giorno, soltanto i tweet superano gli 800 milioni[2], rende del tutto improponibile per qualunque organizzazione un'attività manuale identificazione del materiale rilevante ed anche il ricorso a metodi semplicistici, come le parole chiave o le espressioni regolari[3], potrebbe rivelarsi una modalità di filtraggio grossolana, poco flessibile ed oltremodo esposta ai falsi positivi. Un approccio molto più promettente nell'identificazione dell'esigua quantità di informazioni veramente

[1] Arma dei Carabinieri; Dottore di ricerca in Diritto e nuove tecnologie, Università di Bologna.
[2] Fonte: *Internet Live Stats* Agosto 2021.
[3] Sequenza di simboli utilizzata dai programmatori per identificare stringhe con una struttura definita come email o numeri di telefono.

interessanti consiste invece nel considerare le crescenti potenzialità delle tecnologie di Machine Learning (ML) che consentono di creare modelli decisionali addestrati in base ad un set di dati di esempio e non in base a rigide regole predefinite. Negli ultimi anni l'interesse del mondo accademico e dell'industria per le applicazioni di ML implementate in particolare mediante Reti Neurali Artificiali (RNA) è cresciuto notevolmente, grazie alla grande abbondanza di dati di esempio su cui basare la fase di addestramento, alla possibilità di velocizzare le elaborazioni mediante calcolo parallelo compiuto dalle Unità Grafiche di Processo (GPU) e, non da ultima, alla disponibilità di algoritmi molto efficienti resi disponibili agli sviluppatori mediante strumenti software molto efficienti e facili da usare. L'AS ha trovato anche interessanti applicazioni nel campo della Digital Forensics. Nel caso di indagini conseguenti ad un incidente informatico, acquisite tutte le possibili fonti di prova, l'investigatore forense, tra l'altro, costruisce una timeline degli eventi in base a tutti i file di log del sistema operativo e delle applicazioni presenti nelle immagini delle memorie di massa acquisite[4]. Poiché i record presenti nei file di log potrebbero essere milioni, è evidente che la ricerca degli eventi di interesse mediante ispezione manuale è impraticabile ed anche ricerche testuali tramite parole chiave o espressioni regolari potrebbero rivelare solo una parte delle informazioni utili ad identificare le tracce dell'attacco. Per contro, un approccio basato su metodologie di AS orientate a far emergere sentimenti negativi nei testi presenti nei file di log come "autenticazione fallita" o "accesso negato", potrebbero aumentare di molto l'efficacia e la tempestività dell'analisi. Un altro esempio consiste nell'applicare l'AS ai messaggi di testo scambiati da un dispositivo mobile di cui è stata acquisita l'immagine forense[5]. Riportando il sentiment dei messaggi sulla linea temporale è possibile ricavare in forma grafica l'andamento nel tempo dell'umore di un individuo ed apprezzarne immediatamente gli eventuali repentini mutamenti.

Dal punto di vista dell'intuizione, l'analisi del sentiment consiste nel procurarsi preliminarmente un corposo insieme di testi ed attribuire ad ognuno di essi un'etichetta che ne connota il tenore, di norma positivo, neutro o negativo, ma è possibile cogliere sfumature e stati

[4] H. Studiawan et. al., *Sentiment analysis in a forensic timeline with deep learning*, IEEE Access, 2020.

[5] O. Aboluwarin et al., *Optimizing Short Message Text Sentiment Analysis for Mobile Device Forensics*, Springer, 2014.

d'animo anche più sottili. La corretta esecuzione di questa fase è cruciale, ma richiede tempo ed attenzione, motivo per cui si trovano in rete dei corpus documentali già etichettati che possono essere riutilizzati in molti ambiti applicativi. Questa "base esperienziale" viene poi utilizzata per creare un algoritmo, facilmente integrabile all'interno di programma per computer, in grado di classificare, per esempio, ogni nuovo tweet nell'ambito di un certo hashtag oppure ogni nuovo post comparso in una serie di blog di interesse. Si tratta pertanto nella trasposizione di informazione non strutturata, quale è un testo scritto in linguaggio naturale, in informazione strutturata, dal momento che il risultato della classificazione consiste in tre numeri reali compresi tra 0 ed 1 che rappresentano la probabilità che il sentiment sia rispettivamente positivo, neutro o negativo. Il seguito è dedicato ad una panoramica di alcuni concetti propri del ML, prerequisito indispensabile per apprezzare appieno la successiva presentazione di un caso pratico di applicazione in ambito sportivo.

2. Dall'Artificial Intelligence al Deep Learning

Consideriamo la tassonomia riportata in Figura 1.

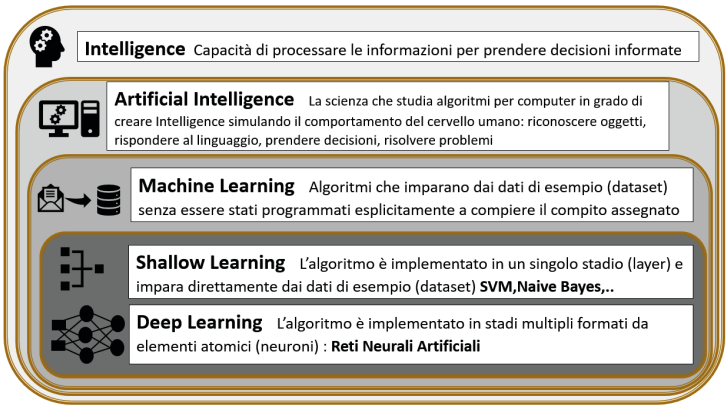


Figura 1. Una tassonomia dell'intelligenza artificiale.

Se intendiamo come *Intelligence* la disponibilità di dati rilevanti per il contesto prescelto e la capacità di processarli al fine di prendere decisioni informate, allora possiamo definire *Artificial Intelligence*

(AI) l'abilità di progettare algoritmi per computer in grado di creare Intelligence[6], simulando il comportamento del cervello umano: fare previsioni, riconoscere oggetti, rispondere a tono nella conversazione con un interlocutore umano, prendere decisioni oppure generare nuove immagini o sequenze musicali. Uno specifico settore dell'AI riguarda il ML, la cui definizione è spesso attribuita ad Arthur L. Samuel che in un paper apparso sull'IBM Journal of Research and Development[7] l'avrebbe coniata come «*il campo di studio che conferisce ai computers l'abilità di imparare senza essere stati esplicitamente programmati*». Pur essendo evidentemente il frutto di una parafrasi poiché nel documento non appare, questa frase rende bene il pensiero dell'autore secondo cui i computer possono essere istruiti per comportarsi in un modo che assomiglia al processo di apprendimento degli esseri umani. Samuel era convinto che la capacità di imparare "dall'esperienza" potesse alla fine consentire di superare i limiti della programmazione tradizionale che impongono al programmatore lo sforzo di prevedere dettagliatamente il comportamento della macchina in ogni condizione. Possiamo intendere con esperienza il risultato di una fase di apprendimento iterativo (training), all'esito della quale viene ottimizzato il valore di un certo numero di parametri previsti da un modello matematico che viene successivamente utilizzato per prendere decisioni o fare previsioni con un certo grado di accuratezza. In sostanza durante il training la macchina apprende in base a dati di esempio e, alla fine, sarà in grado di fare previsioni su dati che non ha mai visto prima.

2.1. *Tipologie di apprendimento*

Il carburante che alimenta gli algoritmi di ML è il *Dataset,* una grande quantità di dati rilevanti per il contesto prescelto che, nel caso dell'apprendimento *supervisionato,* sono gli esempi necessari per l'addestramento. Il Dataset è talvolta[8] costituito da un insieme di N vettori a D componenti e pertanto rappresentabile con una tabella in cui le N righe sono i campioni di esempio e le D colonne sono le *caratteristiche* di ogni campione. Se volessimo costruire un modello di

[6] MIT, *Deep learning course 6.S191*, 2021, *http://introtodeeplearning.com.*

[7] A. L. SAMUEL, *Some Studies in Machine Learning Using the Game of Checkers*, IBM. Journal of Research and Development, 1959.

[8] La forma più generale del dataset è un array a T dimensioni (tensore) con T>2.

ML diciamo per prevedere se gli studenti di quest'anno del corso di Informatica Forense passeranno l'esame basandoci sui 10000 che hanno già affrontato, avremmo una tabella di 10000 righe e 3 colonne, in cui ogni colonna rappresenta una caratteristica, come il numero di ore di lezione, studio e laboratorio spese dallo studente. Naturalmente il criterio secondo cui vengono prescelte le caratteristiche è del tutto arbitrario, ma è evidente che deve essere in qualche modo descrittivo dell'ambito prescelto per poter dare seguito a previsioni affidabili, cosa che potrebbe non accadere se avessimo privilegiato il colore dei capelli dello studente o il comune di residenza. Nell'apprendimento *supervisionato* ad ogni vettore X_i (i=1,..N) avente D caratteristiche $\{x_1,\ldots x_D\}$ è associata un'etichetta Y_i (i=1,..N) detta *label*, anch'essa un vettore a K componenti$\{y_1,\ldots y_k\}$, che rappresenta il risultato del fenomeno osservato. Nel precedente caso dell'esame di Informatica Forense, la label potrebbe essere 1 se lo studente ha passato l'esame e 0 in caso contrario. Si intuisce quindi che esiste un legame tra l'ingresso e l'uscita, una funzione *F* che la fase di apprendimento ha lo scopo di approssimare al meglio con una funzione F*, in modo che per ogni nuovo vettore X si possa prevedere la corrispondente Y come *F**(X). Si parla di *regressione* quando l'etichetta ha solo una componente (K=1) e corrisponde quindi ad un numero reale. Esempi di applicazioni di regressione sono la previsione del voto dell'esame di Informatica Forense oppure il costo di un immobile quando il modello sia stato addestrato considerando come caratteristiche l'anno di costruzione, le coordinate GPS ed il numero dei vani. Se invece K>1 si è in presenza di *classificazione* e il problema consiste nel predire a quale classe appartiene un nuovo vettore di caratteristiche X che il modello non ha visto prima. Se K=2 la classificazione è binaria, come nel caso classico della predizione dello spam della posta elettronica ove una label prevista su un nuovo messaggio email [*spam, non spam*] potrebbe essere [0.1,0.9] se il messaggio viene ritenuto genuino al 90% dalla previsione del modello. Un'altra applicazione deriva dalla classificazione delle immagini, nella quale si tratta di prevedere se una nuova fotografia possa corrispondere ad una classe predefinita, utilizzando per l'addestramento ad esempio il dataset CIFAR-10, reso pubblicamente disponibile dal Canadian Institute For Advanced Research (CIFAR)[9] per incoraggiare lo sviluppo di modelli di ML orientati all'

[9] https://www.cs.toronto.edu/~kriz/cifar.html.

image recognition, che contiene 60000 immagini a colori bidimensionali 32x32 pixels suddivise equamente in 10 classi (quindi K=10) predefinite [aerei, automobili, uccelli, gatti, cervi, cani, rane, cavalli, navi, camion]. In quest'ultimo caso un esempio di label prevista quando si debba classificare la fotografia di un cane potrebbe essere Y= [0.01, 0.02, 0.02, 0.05, 0,02,0.80, 0.01, 0.05, 0.01, 0.01] ossia la probabilità più alta (80%) corrisponde alla classe cane. Naturalmente se si stesse cercando di classificare un'immagine appartenente ad una classe non prevista dal dataset tutti i valori delle componenti della label sarebbero molto bassi. La Figura 2 raffigura degli esempi di classificazione, in cui è importante che il confine che separa le classi (*decision boundary*) sia il più definito possibile e di regressione, in particolare lineare, in cui è invece importante definire la funzione che "meglio rappresenta" i campioni del dataset di esempio.

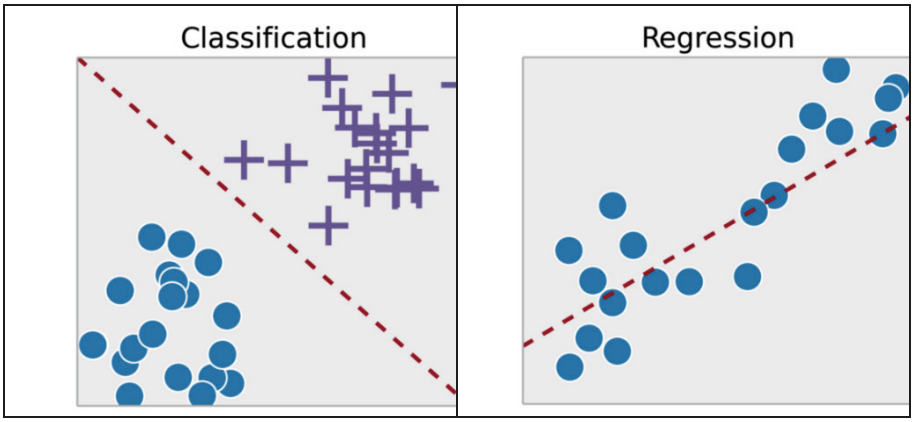


Figura 2. Esempi di classificazione e regressione. Fonte: towardsdatascience.com.

Nell'apprendimento *non supervisionato* invece il dataset è ancora formato dall'insieme di N vettori di esempio a D componenti, ma poiché ad essi non è associata alcuna etichetta, lo scopo dell'algoritmo di ML è quello di comprendere la struttura profonda dei dati, per esempio raggruppando quelli che mostrano delle similitudini (*clustering*) oppure rilevando gli elementi che costituiscono un'anomalia perché hanno valori che si discostano significativamente dal valore "tipico" che rappresenta il dataset (*anomaly detection*). Si intuisce quindi che se lo scopo dell'apprendimento supervisionato è quello di stabilire per esempio "questa immagine rappresenta un orologio", lo scopo

dell'apprendimento non supervisionato è quello di stabilire se esiste similarità tra immagini o trovare quelle che si discostano dal gruppo (Figura 3).

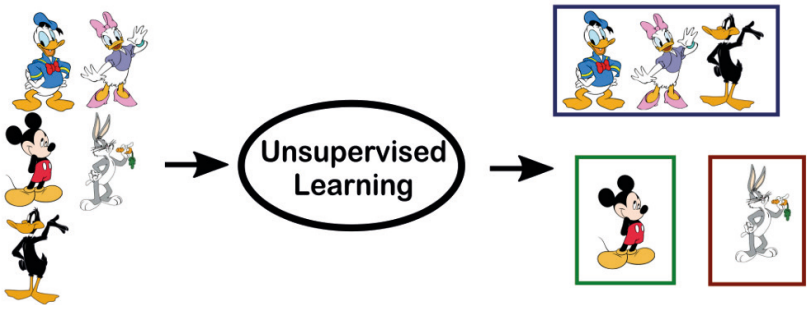


Figura 3. Apprendimento non supervisionato. Fonte: towardsdatascience.com.

Esistono naturalmente molti altri tipi di apprendimento. Citiamo di passaggio l'apprendimento *semi supervisionato,* in cui il dataset è formato sia da campioni dotati di etichetta Y che da campioni non annotati e l'apprendimento *rinforzato*, nel quale un *agente* si trova in un *ambiente* circostante di cui può misurare lo stato e in cui può compiere azioni, ognuna caratterizzata da una diversa *ricompensa*. Lo scopo è quello di apprendere una strategia che, all'esito di vari tentativi ed errori (*trial and error*), per ogni stato conduca al valore massimo possibile della ricompensa. Questo tipo di apprendimento trova diversi settori di applicazione, dai veicoli a guida autonoma, alla determinazione del momento migliore per comprare o vendere azioni, al trattamento dei pazienti con patologie croniche e, in generale, in molte problematiche di ottimizzazione.

2.2. *Le reti neurali artificiali*

Come spesso avviene, le basi di una tecnologia moderna vengono gettate molto tempo prima della sua pervasiva adozione e le reti neurali (RN) non fanno eccezione. Il primo concetto di RN risale addirittura agli anni 40, quando il neurofisiologo Warren S. McCulloch ed il matematico Walter H. Pitts per primi ne ipotizzarono la struttura sulla scorta del funzionamento del cervello umano[10], mentre il *Percettrone,*

[10] H. Ohta, *Reevaluation of McCulloch–Pitts–von Neumann's clock*, Elsevier, 2015.

mattone fondamentale di una RN, è stato concepito nel 1958 da Frank Rosenblatt professore di neurobiologia alla Cornell University[11]. Le reti neurali hanno potuto tuttavia contribuire al successo della moderna intelligenza artificiale solo recentemente, grazie all'avvento dei "Big Data" necessari per l'addestramento, all'enorme incremento prestazionale conosciuto dalle GPU[12] e all'invenzione di algoritmi estremamente efficienti per il calcolo del valore ottimale dei parametri della rete, resi disponibili in librerie di programmazione molto facili da usare perché in grado di schermare completamente l'enorme complessità matematica sottostante. Le RN vengono utilizzate non solo nei campi di applicazione tipici dell'apprendimento supervisionato e non, di cui si è detto, ma trovano, tra l'altro, una grande utilità nella:

- comprensione del linguaggio naturale, in particolare la generazione di riassunti compatti di un testo, il riconoscimento di entità (persone, organizzazioni, numeri di telefono, email, targhe), l'attribuzione di uno scritto ad un autore, la partecipazione ad una conversazione con la controparte umana (chatbots) e, non per ultima, la traduzione di testi in lingue diverse;
- visione artificiale, per esempio la guida autonoma di veicoli, la generazione delle didascalie che descrivono il contenuto di un video (*captioning*), il miglioramento della qualità di un'immagine, la definizione dei contorni degli oggetti;
- fonica computazionale, che comprende la conversione dell'audio nel corrispondente testo o il riconoscimento dei parlatori.

Una rete neurale artificiale è costituita da un insieme di percettroni, fortemente interconnessi, i quali hanno un ruolo che si ispira evidentemente al funzionamento del neurone del cervello umano, poiché ricevono informazioni dal livello precedente e si attivano in base ad un'opportuna funzione. Come indicato in Figura 4, l'uscita U del percettrone è data da una funzione di attivazione (di norma) non lineare **g** che agisce sulla combinazione lineare degli ingressi mediante un vettore di pesi $\{w_0, w_1, \ldots w_n\}$ il cui valore è dapprima incognito e viene determinato al termine della fase di addestramento in base ad un criterio di ottimizzazione definito dall'analista:

[11] CORNELL CHRONICLE, Professor's perceptron paved the way for AI – 60 years too soon.
[12] Anche grazie alle applicazioni legate alla creazione delle criptovalute.

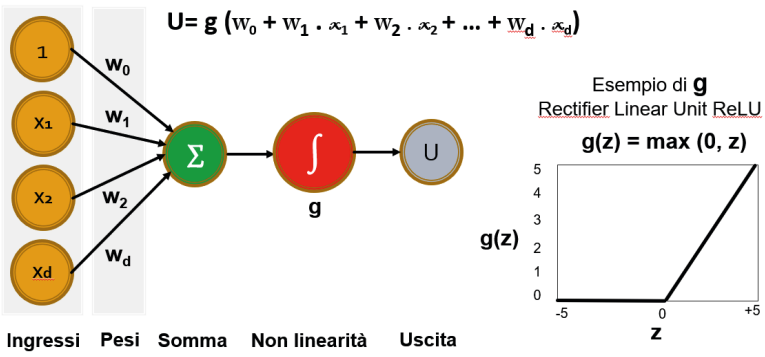


Figura 4. Il percettrone.

I percettroni sono organizzati in livelli densi (*dense layers*), nel senso che ognuno di essi è collegato in ingresso ed in uscita con ogni altro percettrone del livello precedente e successivo. I livelli che non sono connessi agli ingressi o alle uscite sono detti nascosti (*hidden*) e quando i livelli nascosti sono almeno due la rete neurale è strutturata per un apprendimento profondo (*Deep Learning*). L'utilizzo di funzioni di attivazione non lineari deriva da fatto che esse meglio si adattano all'intrinseca non linearità dei dati e, grazie al Teorema di Approssimazione Universale, consentono di approssimare qualunque funzione[13] F che, come detto al paragrafo 2.1, la fase di apprendimento ha lo scopo di dedurre. Infatti, in molti casi la distribuzione dei dati non consente la separazione o la rappresentazione mediante una retta come descritto nella Figura 2, ma richiede l'utilizzo di funzioni poligonali piuttosto complesse che possono essere sintetizzate solo con una rete neurale con almeno un livello nascosto. In Figura 5 è rappresentata una rete a tre livelli, di tipo *Feed Forward* perché caratterizzata da flusso dell'informazione unidirezionale dagli ingressi alle uscite, senza cicli di elaborazione. La presenza di livelli successivi comporta che ogni uscita U_i sia descritta da una funzione complessiva degli ingressi e dei pesi G(X,W), che deriva dalla concatenazione delle funzioni g descritte in Figura 4 di ogni percettrone.

[13] K. Hornik et al., *Universal Approximation of an Unknown Mapping and Its Derivatives Using Multilayer Feedforward Networks*, Caltech, 1989.

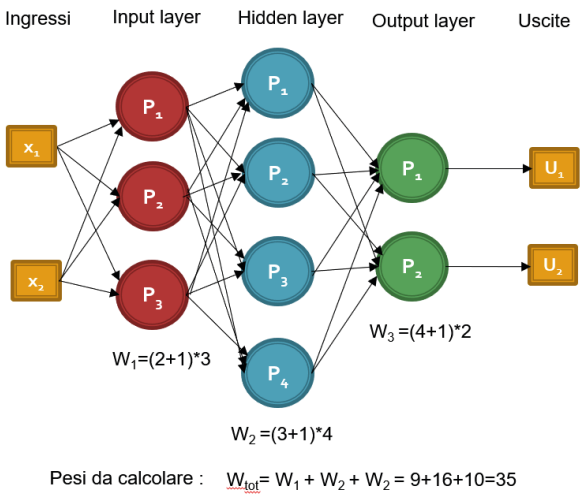


Figura 5. Rete neurale feed forward a tre livelli.

La determinazione del numero di livelli e del numero di percettroni per ognuno di essi è una questione architetturale fondamentale, ma per la quale tuttavia non esistono formule definite ed è di norma necessaria una fase di sperimentazione ed ottimizzazione per dimensionare la rete in modo che l'accuratezza dei risultati sia soddisfacente. Tranne che per le problematiche più semplici, almeno un livello nascosto è da prevedere, anche se un numero compreso tra 2 e 5 è di norma necessario per dataset complessi. Anche per il numero di percettroni per ogni livello valgono regole qualitative dettate dall'esperienza, in base alle quali il numero deve essere decrescente da un livello al successivo e dovrebbe essere compreso tra il numero di componenti D dell'ingresso (vettore delle caratteristiche) e K dell'uscita (vettore delle etichette). Per esempio una rete a tre livelli in cui D=512 e K=3, il numero di percettroni potrebbe essere 128, 64, 3 ed il numero di pesi da calcolare ammonta a 74.115.

2.3. *Addestramento della rete neurale*

Il fine ultimo della fase di addestramento è fornire alla rete neurale un criterio per decidere quando i valori delle previsioni non sono corretti, cosa che certamente avverrà nella fase iniziale in cui il valore dei pesi non è determinato, in modo che essa possa progressivamente correggersi e via via migliorare l'accuratezza dei dati in uscita. Nell'appren-

dimento supervisionato, questo comporta in qualche modo la definizione di una penalità che dia conto della differenza tra la predizione della rete $G(X_i,W)$ quando è alimentata con l'i-mo vettore di esempio X_i e l'etichetta Y_i associata a tale vettore. La somma delle penalità su tutti gli N esempi determina una funzione di *costo* complessivo $J(X_i,W)$, in cui gli X_i sono i termini noti e il vettore dei pesi W è la variabile indipendente. Il minimo della funzione di costo corrisponde ad un valore ottimo W* dei pesi ed equivale al termine della fase di addestramento. Per esempio, nelle questioni di regressione, in cui come detto la rete deve prevedere un singolo valore, la funzione costo è il noto scarto quadratico medio tra l'uscita prodotta della rete ed il valore delle etichette:

$$J(W) = 1/N * \Sigma_{i=1, N} (Y_i - G(X_i, W))^2$$

L'addestramento richiede la determinazione del valore dei pesi W* che corrispondono al minimo della funzione J(W). Come è facilmente intuibile, il calcolo del minimo assoluto di una funzione che potrebbe tranquillamente avere centinaia di migliaia di variabili e centinaia di minimi locali è stato un problema di fatto intrattabile fino all'ultimo decennio, quando sono apparse pubblicazioni su metodi di ottimizzazione dell'algoritmo di calcolo del gradiente di una funzione[14] (Stochastic Gradient Descent, 1952). Il processo di convergenza verso il minimo della funzione di costo è iterativo e comporta ben più di un *epoch*, ossia una presentazione completa in ingresso alla rete neurale di tutti gli N vettori di esempio X_i. Anche Il numero di epochs è un parametro non determinabile a priori, ma va affinato per tentativi partendo da un numero ragionevole (per esempio 10 o 20). Se il numero di epochs è troppo basso il modello non è ottimizzato e si verifica il fenomeno dell'*underfitting*, a causa del quale la rete neurale non è in grado di prevedere correttamente neanche i valori di esempio[15]. Se invece il numero di epochs è troppo alto di verifica il fenomeno contrario, l'*overfitting*[16] ove invece la rete neurale si "abitua" troppo al data-

[14] Vedasi ad esempio D. KINGMA et al., *Adam: A method for stochastic optimization*, ResearchGate, 2014.

[15] L'underfitting si verifica anche quando l'architettura di rete è troppo semplice rispetto alla complessità dei dati oppure se le caratteristiche dei dati di esempio non sono adeguate.

[16] L'overfitting è anche causato da un'architettura della rete con troppi livelli oppure da un dataset con un alto numero D di caratteristiche, ma poco numeroso.

set di addestramento e non generalizza correttamente, ossia non prevede accuratamente le uscite in presenza di ingressi che non ha mai visto prima. Per evitare quest'ultima eventualità sono state previste tecniche di regolarizzazione[17], mediante le quali il 50% pesi vengono randomicamente azzerati durante l'addestramento per non rendere alcun percettrone più importante di un altro oppure, registrando il valore dei pesi ad ogni passaggio, si seleziona il valore di epoch dopo il quale l'accuratezza delle previsioni comincia a degradare.

3. Un esempio di applicazione

L'esempio che intendiamo considerare è tratto dall'ambito sportivo, ma gli aspetti concettuali sono validi per qualunque dominio applicativo di interesse. Il dataset è quindi costituito da circa 260.000 Tweets in italiano riguardanti le squadre di calcio del campionato di serie A, raccolti mediante Twitter API tra il maggio ed il settembre 2018[18] ed annotati con sentiment positivo, neutrale e negativo[19]. Come anticipato nell'introduzione, sono pubblicamente disponibili svariati analoghi corpus documentali già prontamente utilizzabili[20], anche se potrebbe non essere possibile reperire materiale adeguato in una lingua diversa da quella inglese e sarebbe quindi necessaria una fase preliminare di raccolta ed annotazione di scritti rilevanti per il contesto prescelto. Il progetto è stato realizzato come descritto nel seguito mediante il linguaggio di programmazione Python 3.7 e varie librerie open source tra cui Tensorflow[21], mediante la quale è possibile creare, addestrare e valutare le prestazioni di modelli di ML utilizzabili in numerosi contesti di apprendimento. L'architettura della rete non richiede risorse di calcolo particolari: la presenza di una GPU riduce i tempi di addestramento, ma non è necessaria. Il codice sorgente è liberamente disponibile su GitHub: https://github.com/783919/dl4sa.

[17] Dropout ed Early Stopping.
[18] https://github.com/charlesmalafosse/open-dataset-for-sentiment-analysis.
[19] Sono stati defalcati i tweet annotati con sentiment "mixed" il cui numero è trascurabile.
[20] https://analyticsindiamag.com/10-popular-datasets-for-sentiment-analysis/.
[21] https://www.tensorflow.org/.

3.1. *Precisazione sulla composizione del dataset*

Il problema fondamentale del Machine Learning è quello di creare un modello in grado di descrivere al meglio la tipologia di dati oggetto di studio, partendo da un sottoinsieme significativo di essi, in modo da fare previsioni su dati dello stesso ambito mai visti prima. Se la capacità previsionale è buona il modello generalizza bene sui nuovi dati, altrimenti si ha overfitting quando il modello tende a memorizzare eccessivamente i dati di addestramento oppure underfitting quando i dati di esempio non hanno sufficiente capacità informativa. Per raggiungere pertanto il miglior adattamento possibile dei dati di esempio al modello il dataset viene in realtà suddiviso in tre parti[22]:

- *training*: utilizzato nella fase di addestramento per calcolare i pesi W del modello. Di norma costituisce dal 70% al 90% del dataset;
- *validation:* utilizzato nella fase di ottimizzazione dei pesi, come la citata fase di regolarizzazione;
- *test:* è impiegato per fare le prove dell'accuratezza del modello, ossia quanto bene esso generalizzi su nuovi dati, prima dell'impiego sul campo.

Il sottoinsieme di validation e test non partecipano quindi alla fase di costruzione del modello, ma concorrono alla sua ottimizzazione ed alla valutazione della capacità di generalizzare.

3.2. *Il Progetto*

Il progetto che intendiamo realizzare è articolato nelle quattro fasi descritte in Tabella 1. Riprendendo le definizioni del paragrafo 2.1 abbiamo quindi un dataset complessivo costituito da un insieme di 260.000 vettori a 5 componenti (*tweet_date_created, tweet_id, tweet_text, language, sentiment_score*), rispettivamente la data di creazione del tweet, un identificativo univoco, il testo del tweet, la lingua (italiano) e uno score associato alla label *sentiment*, che indica quale sia il valore più probabile (positivo, negativo o neutro), secondo la classificazione operata automaticamente dalla Amazon AWS Com-

[22] A. Burkov, *The Hundred-Page Machine Learning Boo*k, self-published, 2019.

prehend API. Infatti il testo dei tweet non è stato annotato manualmente da un operatore umano, operazione lunga e tediosa, ma da uno strumento di ML.

Tabella 1. Le quattro fasi del progetto.

a. Preparazione dei dataset	Selezione delle caratteristiche
	Ordinamento casuale
	Bilanciamento dei campioni
	Creazione dei tre dataset
	Word Embedding
b. Disegno della rete	Scelta del modello
	Definizione dei livelli
	Scelta della funzione di costo
	Scelta del criterio di ottimizzazione
	Regolarizzazione
c. Addestramento	Scelta del numero di epochs
	Metrica di valutazione del modello
	Valutazione del modello
d. Predizione	Scelta del testo da classificare
	Classificazione
	Valutazione della predizione

3.2.1 *Preparazione del dataset*

A proposito della capacità informativa dei vettori delle caratteristiche si può notare che, a parte il testo del tweet, tutte le altre quattro sono del tutto irrilevanti nella valutazione del sentiment e possono quindi essere eliminate per consentire al modello di concentrarsi solo sugli aspetti importanti della base esperienziale. Nelle questioni di classificazione inoltre, contrastare il fenomeno dello sbilanciamento del dataset è molto importante per la correttezza delle previsioni. In molti ambiti infatti capita che gli esempi appartenenti ad una classe di esempio siano molto più numerosi di quelli di un'altra, come per esempio potrebbe avvenire per un modello di previsione delle transazioni fraudolente con carta di credito che di norma potrebbero essere inferiori all'1% del totale. Il rischio di dataset sbilanciati risiede nella possibilità che la rete neurale non classifichi correttamente i nuovi valori appartenenti ad una classe di addestramento con troppi pochi esempi.

Anche il dataset del nostro progetto è afflitto da sbilanciamento, anche se non estremo[23], perché i tweet di esempio sono distribuiti come in Tabella 2.

Tabella 2. Distribuzione dei campioni nelle 3 classi.

Tweet positivi	22883	8,8% del totale
Tweet negativi	9441	3,6% del totale
Tweet neutri	226868	87,6% del totale
Tweet totali	259192	

Esistono tecniche particolari basate per esempio sull'utilizzo nell'addestramento di pesi diversi per campioni di classi di diversa numerosità, ma in questa sede per semplicità espositiva livelleremo banalmente i campioni delle tre categorie sul numero di quella meno numerosa, ottenendo un dataset complessivo di 28.323 campioni complessivi, rimescolati casualmente per non favorire un ordine specifico secondo il quale potrebbero essere stati raccolti ed equamente distribuiti tra tweet positivi, negativi e neutri. Il dataset viene poi suddiviso in addestramento, validazione e test secondo la proporzione 90%, 5%, 5% dei tweet totali.

Un aspetto fondamentale della preparazione del dataset connesso con l'elaborazione del linguaggio naturale consiste nel fatto che i dati in ingresso ad una rete neurale non possono essere stringhe di caratteri, ma obbligatoriamente numeri reali. Questo comporta che è necessaria una preliminare elaborazione che trasformi il testo di ogni tweet in un vettore di caratteristiche puramente numeriche. Una delle tecniche più popolari è detta Word Embedding[24] (WE) che consente nel convertire una parola o anche un'intera frase in un vettore di numeri reali, in modo che testi semanticamente simili corrispondono a vettori quasi sovrapponibili (esempio in Figura 6). Esistono modelli di WE già calcolati per diverse lingue e, in questa sede, verrà utilizzato l'Universal Sentence Encoder di Google[25], disponibile in 16 lingue ed in grado di convertire qualunque frase in un vettore a 512 componenti.

[23]https://developers.google.com/machine-learning/data-prep/construct/samplingsplitting/im- balanced-data.

[24] F.Almeida G.Xexéo ,*Word Embeddings: A Survey*, ResearchGate, 2019.

[25] https://tfhub.dev/google/universal-sentence-encoder-multilingual-large/3.

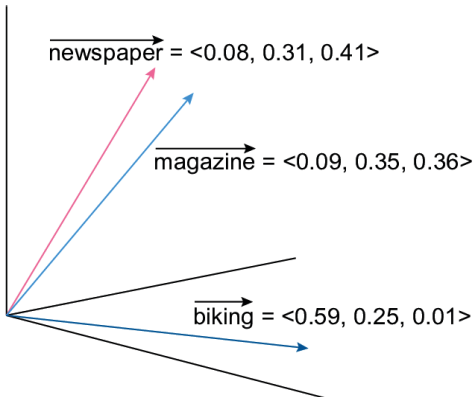


Figura 6. Esempio di word embedding su singoli termini. Fonte: researchgate.net.

Ricapitolando, osserviamo che il dataset è complessivamente costituito da vettori X_i (i=1, 28.323) a 512 componenti, ottenuti dalla conversione dell'unica caratteristica rilevante *tweet_text*. Anche i tre valori possibili della label *sentiment* (positivo, negativo, neutro) devono essere convertiti dal formato testuale a quello numerico, mediante l'applicazione della tecnica di One-Hot Encoding, a seguito della quale la label verrà codificata in un formato 1 su 3 come in Tabella 3.

Tabella 3. Conversione di formato della label sentiment.

Sentiment	**POS**	**NEG**	**NEU**
Positivo	1	0	0
Negativo	0	1	0
Neutro	0	0	1

Ogni label Y_i diventa quindi un vettore a tre componenti, solo una delle quali è 1, mentre le altre due hanno valore 0.

3.2.2 *Struttura della rete*

Il modello individuato è analogo a quello descritto in Figura 5 ossia una rete neurale feed forward a tre livelli (Figura 7), che potranno essere aumentati se la successiva fase di valutazione l'accuratezza non sarà soddisfacente, ognuno rispettivamente composto da 128, 64, 3 percettroni. È consigliabile partire con un modello semplice aggiungendo eventualmente livelli, per evitare il problema della scarsa capacità di generalizzare sui dati di test dovuto all'overfitting.

Abbiamo già avuto modo di vedere che se il vettore degli ingressi possiede 512 componenti il numero di pesi da calcolare ammonta a 74.115.

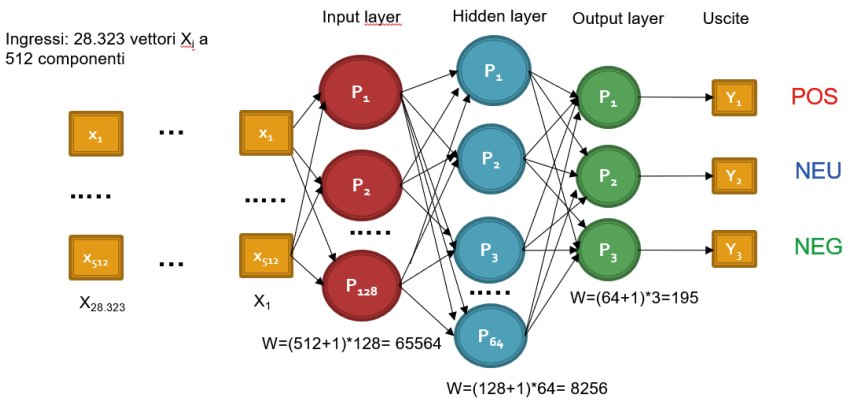


Figura 7. Struttura della rete neurale del progetto.

Le funzioni di attivazione **g** del primo e secondo livello saranno le già richiamate ReLU (Figura 5), mentre i percettroni dell'ultimo stadio avranno una funzione di attivazione di tipo *softmax,* in modo che, quando la rete viene utilizzata per predire a quale categoria appartenga un nuovo testo, ogni valore di uscita corrisponda alla probabilità che il tweet appartenga alla classe di sentiment positivo, neutro o negativo. La funzione di costo da minimizzare non è lo scarto quadratico medio tra l'uscita prodotta della rete ed il valore delle etichette come nel citato caso della regressione, ma *categorical cross-entropy*, in cui lo scarto è tra due distribuzioni di probabilità. La funzione di costo verrà minimizzata mediante l'algoritmo di calcolo del gradiente denominato Adam (si veda la nota a piè di pagina numero 11), mentre la regolarizzazione viene realizzata mediante Dropout al 50% sulle uscite dei primi due livelli.

3.2.2 *Addestramento della rete*

La fase di training verrà condotta su un numero di 20 epochs, in ognuna delle quali i campioni del dataset non verranno presentati insieme, ma per migliorare la velocità di convergenza di Adam saranno suddivisi in gruppi denominati *batch* composti da 32 campioni. La

metrica individuata per la valutazione della fase di addestramento del modello è basata sull'*accuratezza*, ossia il numero di label correttamente classificate in rapporto al numero totale di label del dataset. Per quanto riguarda la valutazione del modello, affidandosi ai grafici prodotti da *TensorBoard* strumento di diagnostica integrato in Tensorflow, si può notare in Figura 8 che la funzione di costo calcolata sul dataset di training (linea arancione) è sempre decrescente, mentre quella calcolata sul dataset di validation (linea blu) è superiore alla precedente già dopo epoch 4, momento in cui si ha la migliore configurazione di pesi W prima dell'inizio dell'overfitting.

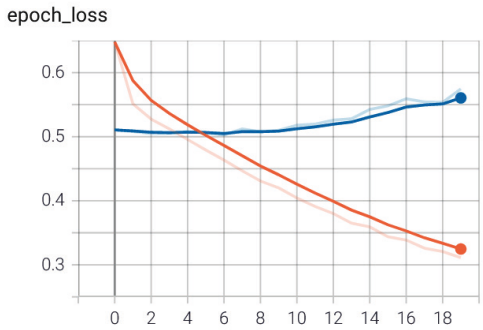


Figura 8. Funzione di costo al variare degli epochs.

3.2.2 *Predizione*

Dopo aver registrato un livello di accuratezza sul dataset di test del 77,3% possiamo procedere alla fase di previsione in cui presentiamo alla rete tre Tweet inediti da classificare (Figura 9 e Tabella 4).

```
Test Loss:  0.6717632412910461
Test accuracy:  77.33050584793091
Andatevene tutti , maledetti mercenari, fate schifo non merita
te quella maglia , siete una vergogna
[[9.3890631e-01 6.0652182e-02 4.4148887e-04]]
Forza e bellezza.... cos insieme non si erano mai viste
[[9.9478541e-09 1.1702482e-01 8.8297510e-01]]
Lo stadio Noucamp riaprir al pubblico dopo un anno di restauri
.
[[1.6979588e-08 9.9969542e-01 3.0456099e-04]]
Press any key to continue . . .
```

Figura 9. Previsione su Tweet inediti.

Tabella 4. Prospetto della previsione.

Testo del Tweet da classificare	POS	NEG	NEU
Andatevene tutti, maledetti mercenari, fate schifo non meritate quella maglia, siete una vergogna	00,04%	93,90%	06,06%
Forza e bellezza.... così insieme non si erano mai viste	88,30%	00,00%	11,70%
Lo stadio Noucamp riaprirà al pubblico dopo un anno di restauri	00,03%	00,00%	99,97%

La valutazione delle predizioni è molto buona sui testi selezionati, dal momento che la rete classifica correttamente il sentiment dei Tweet, spaziando dall'88% al quasi 100% di confidenza. Naturalmente esperimenti ripetuti su testi diversi porterebbero a percentuali di classificazione diverse, ma il livello di accuratezza sul dataset di test vicino all'80% lascia presagire che la rete, senza ulteriori aggiustamenti architetturali, sarà in grado di classificare ragionevolmente bene ulteriori testi inediti della stessa tipologia.

4. Conclusioni

Il cyberspazio è diventato parte fondamentale della vita del genere umano, dal singolo individuo alle organizzazioni complesse, nonché la principale fonte di informazione oggi disponibile. Ogni giorno milioni di persone esprimono le proprie opinioni e sentimenti partecipando a forum, blog, social network ed altre risorse del web[26]. Queste manifestazioni del pensiero possono avere risvolti molto rilevanti in campo sociale, politico, economico e di pubblica sicurezza ed è per questo molto importante valutare lo stato d'animo mostrato dagli autori. Le tecniche di Deep Learning applicate all'analisi del sentiment possono consentire di creare strumenti automatici in grado sia di monitorare in maniera affidabile i contenuti pubblicati su web e social media, sia di aumentare l'efficacia e la tempestività della fase di analisi di un investigatore forense. Questo grazie al superamento delle limitazioni imposte da metodi semplicistici basati su regole predeterminate e la proposizione all'analista dei contenuti verosimilmente di

[26] M.Birjali et al., *A comprehensive survey on sentiment analysis: Approaches, challenges and trends*, Elsevier, 2021.

maggior interesse. Negli ultimi anni le applicazioni basate su reti neurali hanno registrato un incremento verticale, raggiungendo risultati senza precedenti, come nel caso della guida autonoma di veicoli o nell'elaborazione del linguaggio naturale. Tuttavia, l'impego delle reti neurali è non solo connotato da risvolti positivi dal momento che:

- seppure in epoca di Big Data, non sempre è possibile disporre della quantità di dati di addestramento rilevanti che sia necessaria per il contesto prescelto. Inoltre la progettazione e costruzione del dataset di esempio è un'attività gravosa e che richiede una certa creatività, poiché, come abbiamo visto, non tutte le caratteristiche hanno lo stesso contenuto informativo;
- i criteri di progetto non sono del tutto definiti, per esempio in termini di numero di livelli e di percettroni per livello. Questo può comportare un complesso iter di ottimizzazione dell'accuratezza che comporta molti tentativi ed uno sforzo computazionale molto intenso.

In ultima analisi, una rete neurale potrebbe essere assimilata ad una magica scatola nera, perché la fase di apprendimento consente alla rete di comprendere autonomamente la struttura intima dei dati, come per esempio i tratti di un volto, senza alcun intervento del programmatore. Inoltre il comportamento della rete potrebbe essere non deterministico, perché sessioni di addestramento ripetute possono portare all'individuazione di punti di minimo della funzione costo diversi, quindi diversi valori dei pesi calcolati (cfr. paragrafo 2.3) e infine previsioni con accuratezze differenti.

Questo contributo ha inteso descrivere sommariamente quali siano i meccanismi che sottendono al concetto di apprendimento applicato ai computer, mostrando un esempio di impiego tratto dall'ambito sportivo ed i limiti entro cui le previsioni possono ritenersi affidabili.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643018
pp. 343-361 (gennaio 2022)

L'IA applicata all'analisi dei metadati: un'alternativa alla rottura della crittografia per le autorità di contrasto alla criminalità*

Isadora Neroni Rezende[1], Pier Giorgio Chiara[2]

1. Introduzione: la natura prismatica delle esigenze di sicurezza nell'era dell'Internet delle cose

Questo elaborato esamina l'impatto, in termini di diritti fondamentali, di alcune tecnologie crittografiche di sicurezza digitale e analisi dei metadati nel contesto delle attività di informatica forense attuate dalle autorità di contrasto. Lo studio della disciplina normativa – unitamente ad un'analisi più tecnica – mira a chiarire se l'impiego di modelli di intelligenza artificiale (IA) nell'analisi del traffico telematico criptato possa essere d'aiuto per ridurre l'invasività delle operazioni di sorveglianza delle forze dell'ordine.

L'analisi proposta assume particolare rilevanza alla luce della progressiva diffusione dei dispositivi dell'Internet delle cose – meglio noto nell'acronimo inglese "IoT", ovvero *Internet of Things* – sempre più incorporati in ambienti definiti "intelligenti" (ad esempio, le cd. *smart cities*). L'IoT è, in via di prima approssimazione, una complessa

* Il presente lavoro è stato discusso dagli autori alla conferenza internazionale *TILTing Perspectives 2021*, organizzata dall'Università di Tilburg. Questo lavoro è il risultato di una ricerca comune e condivisa condotta da entrambi gli Autori. Tuttavia, nel dettaglio, Pier Giorgio Chiara è l'autore dei §§ 1, 2 e 3, mentre Isadora Neroni Rezende è l'autrice dei §§ 4, 5, 6.

Questo studio è finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea attraverso l'accordo di sovvenzione Marie Sklodowska-Curie ITN EJD "Law, Science and Technology Rights of Internet of Everything" No 814177.

[1] Dottoranda di ricerca in Diritto delle Nuove Tecnologie presso l'Università Autonoma di Barcellona | Last-JD-RIoE.

[2] Dottorando di ricerca in Diritto delle Nuove Tecnologie presso l'Università del Lussemburgo | Last-JD-RIoE.

rete di cose, che incorpora e – grazie ad Internet – connette tra loro sensori, attuatori, software di intelligenza artificiale (IA) e componenti hardware[3]. Questa enorme classe di componenti dei sistemi IoT è molto meno standardizzata della componentistica per i PC[4]. Infatti, l'IoT riunisce sotto di sé dispositivi con CPU, memoria e potenza di elaborazione limitata, come i sensori di pressione che, per essere economicamente competitivi, richiedono un hardware piccolo e a basso costo[5], e dispositivi con processori potenti e grande memoria. Ne consegue che la prima classe di dispositivi non ha la necessaria memoria e potenza di calcolo per eseguire i più aggiornati e robusti protocolli crittografici; così, la ricerca si concentra sui cd. algoritmi crittografici *lightweight*, più adatti a tali contesti "limitati".

Questi fanno sempre più affidamento su metodi crittografici per garantire i diritti fondamentali degli individui, in particolare il diritto alla *privacy* e alla protezione dei dati personali. La dottrina dedica una grande attenzione alle sfide normative (giuridiche, etiche e sociali) portate dall'IoT nei campi della *cybersicurezza*, della *privacy* e della protezione dei dati[6]. Recenti studi hanno infatti dimostrato che il paradigma dell'IoT pone seri e diversi rischi al godimento da parte degli individui dei diritti fondamentali alla *privacy* e alla protezione dei dati, indipendentemente dal fatto che siano in vigore protocolli di crittografia, siano questi "leggeri" o più tradizionalmente robusti. Queste preoccupazioni sono vieppiù amplificate nel contesto delle attività di contrasto da parte delle forze dell'ordine, poiché gli strumenti digitali forniscono alle autorità pubbliche mezzi sempre più intrusivi di monitoraggio, aventi tanto più efficacia quanto più gli ambienti in cui operano sono informatizzati. Diversamente dalle relazioni orizzontali intrattenute tra attori privati, in ambito civile, infatti, i cittadini soffrono più intensamente le asimmetrie di potere presenti nelle loro relazioni verticali con lo Stato.

[3] A. Rayes e S. Salam, *Internet of Things: from Hype to Reality*, Springer, 2019, p. 2.

[4] P. Marwedel, *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things,* Springer, 2018, p. 126.

[5] T. Stapko, *Practical Embedded security: Building Secure Resource-Constrained Systems*, Newnes, 2008, p. 85.

[6] Si veda *ex multis* U. Pagallo, M. Durante e S. Monteleone, *What is new with the Internet of Things in Privacy and Data protection? Four legal challenges on sharing and control in IoT* in R. Leenes, R. Van Brakel, S. Gutwirth e P. De Hert (a cura di) *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 2017.

L'importanza del tema è altresì evidenziata dalla recente pubblicazione, da parte del Consiglio dell'UE, di una risoluzione intitolata "Crittografia - Sicurezza attraverso la crittografia e sicurezza nonostante la crittografia". La risoluzione propone la creazione di un quadro di certezze giuridiche volto a garantire la capacità delle autorità di *intelligence* – in ambito di sorveglianza preventiva – e della giustizia penale – con particolare riguardo al campo dell'informatica forense – di accedere legalmente ai dati digitali criptati e in modo mirato. Tuttavia, nel contesto delle attività di sorveglianza preventiva e di indagine, la crittografia *end-to-end (E2E)* rende l'analisi del contenuto delle comunicazioni estremamente difficile o praticamente impossibile, senza il ricorso alla cd. "rottura" della tecnologia crittografica.

Nel contesto delineato, due diversi livelli di complessità sembrano emergere. Essi riguardano: (i) la possibilità di raggiungere un equilibrio tra i valori protetti dalla crittografia, soprattutto quella E2E, e gli obiettivi delle autorità di contrasto, con particolare riguardo al cd. *legal hacking*[7]; e, (ii) la capacità di alcuni modelli di IA di preservare i vantaggi della crittografia, permettendo di dedurre informazioni preziose dal traffico delle comunicazioni, anziché dal contenuto vero e proprio delle stesse.

Dopo aver fatto luce sui rischi paradossalmente connessi all'impiego di tecnologie crittografiche, la risposta agli interrogativi posti prenderà le mosse da una disamina tecnico-giuridica dei mezzi di IA applicati all'analisi del traffico delle comunicazioni. Nell'esporre le potenzialità offerte da tali tecniche, verranno evidenziate nuove prospettive nel concepire la distinzione tra contenuto e dati esterni alle comunicazioni (o metadati). In particolare, si sosterrà come l'analisi dei metadati offra maggiori possibilità di bilanciamento tra i diritti alla *privacy* e alla protezione dei dati, da un lato, e le esigenze di sicurezza, dall'altro. Le argomentazioni proposte saranno infine sostenute dalla più recente giurisprudenza europea in materia di sorveglianza.

[7] Si veda G. ZICCARDI, *Parlamento Europeo, captatore e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Arch. pen.*, 2017 (1).

2. I rischi della crittografia

La crittografia ricomprende sotto di sé diverse tecnologie cruciali per proteggere e promuovere diritti fondamentali come il diritto alla *privacy*, alla protezione dei dati personali e alla libertà di espressione[8]. D'altra parte, una tecnologia crittografica particolarmente "robusta" può altresì ostacolare le attività di contrasto da parte delle forze dell'ordine[9].

Diversi elementi sul piano normativo (giuridico, etico, sociale), mettono in luce il conflitto di valori sotteso alle tecniche di rottura della crittografia. Nel 2020, la cd. "crypto-guerra"[10] è stata rivitalizzata da una relazione congiunta dei cosiddetti "cinque occhi", cioè Stati Uniti, Regno Unito, Australia, Canada e Nuova Zelanda, attraverso la quale si è esplicitato che la sicurezza pubblica non possa essere protetta senza compromettere la *privacy* o la sicurezza informatica[11]. Dal canto suo, il Consiglio dell'UE ha pubblicato nel novembre 2020 una risoluzione volta a garantire la capacità delle autorità competenti nel settore della sicurezza e della giustizia penale, come le forze dell'ordine e le autorità giudiziarie, di accedere ai dati in modo legale e mirato[12].

In questo contesto, è interessante notare che il considerando 54 della proposta di revisione della direttiva sulla sicurezza delle reti e dell'informazione (di seguito, NIS 2) afferma che «l'uso della crittografia E2E dovrebbe essere "conciliato" con i poteri degli Stati membri di garantire la tutela della sicurezza pubblica e dei loro interessi essenziali in materia di sicurezza, nonché di consentire l'indagine, l'accertamento e il perseguimento di reati nel rispetto del diritto dell'Unione»[13]. La

[8] W. Wiewiórowski, *Keynote: Data protection needs encryption*, EDPS Online IPEN Workshop, 3 giugno 2020.

[9] Si veda R. Brighi, *Requisiti tecnici, potenzialità e limiti del captatore informatico. Analisi sul piano informatico-forense,* in Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie informatiche, Torino, Giappichelli, 2021, pp. 231 – 256.

[10] B. J. Koops, E. Kosta, *Looking for some light through the lens of "cryptowars" history: policy options for law enforcement authorities against "going dark"*, in *CLSR*, 2018, 34.

[11] Si veda: https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety/international-statement-end-to-end-encryption-and-public-safety-accessible-version.

[12] Consiglio dell'Unione Europea, *La sicurezza attraverso la crittografia e nonostante la crittografia,* 13084/1/20, 2020.

[13] Commissione Europea, *Proposta di direttiva del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148,* COM(2020) 823 final, considerando 54.

formulazione del considerando è piuttosto problematica perché queste "soluzioni", volte a facilitare l'accesso da parte delle forze dell'ordine, si tradurrebbero molto probabilmente in un abbassamento della sicurezza complessiva degli utenti di tali sistemi a causa di una superficie di attacco[14] più largamente estesa. A tal proposito, il Garante Europeo della Protezione dei Dati (EDPS), nel suo parere sulla proposta per la NIS 2, suggerisce di modificare il considerando 54 affinché nulla nella proposta possa essere interpretato come un'approvazione dell'indebolimento della cifratura *end-to-end* attraverso *backdoors*[15].

La dichiarazione del Garante europeo deve essere letta insieme alla suddetta risoluzione del Consiglio. Il Consiglio sottolinea la necessità di soluzioni tecniche che consentano alle autorità competenti di ottenere un accesso legittimo e mirato ai dati cifrati, nel rispetto dei principi di legalità, trasparenza, necessità e proporzionalità. Eppure, il Consiglio, nel tentativo di contemperare tutte le istanze in gioco, esclude esplicitamente qualsiasi misura che possa indebolire la crittografia, come le *backdoors*. Secondo diversi esperti di sicurezza informatica, firmatari di una lettera aperta in risposta alla risoluzione, il Consiglio andrebbe cercando una "via di mezzo" che semplicemente non esiste[16]. Allo stato dell'arte, è chimerico pensare a tecnologie informatiche ragionevolmente sicure che, da una parte, facilitino i poteri investigativi per decriptare contenuti e, dall'altra, non vedano decrescere le loro aspettative di sicurezza, garantendo pertanto i diritti fondamentali degli individui – in particolare, il diritto alla *privacy* e alla protezione dei dati personali. Una volta rotto il meccanismo crittografico, anche se solo relativamente alle forze dell'ordine o agenzie di intelligence, l'aspettativa di sicurezza per ogni utente inevitabilmente diminuisce.

Poiché l'indebolimento della crittografia E2E – tramite creazione di *backdoors* – si è rivelato non essere un'opzione, conseguenza inevitabile di quella che in dottrina è stata chiamata come "seconda cripto-

[14] Il Glossario del NIST definisce la superficie d'attacco di un sistema, un elemento del sistema o di un ambiente come l'insieme dei punti sul perimetro in cui un aggressore può cercare di entrare, causare un danno o estrarre dati da quel sistema, elemento del sistema o ambiente.

[15] EDPS, *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive*, 2021, p. 16. Il Glossario del NIST definisce la *backdoor* come un modo non documentato di accedere al sistema informatico.

[16] Si veda: https://sites.google.com/view/scientists4crypto/start.

guerra"– è stata la creazione di cornici legislative relative ai poteri di *hacking* degli Stati[17]. In questo contesto, Europol ha annunciato alla fine del 2020 una piattaforma di decrittazione innovativa, sviluppata con il Centro di Ricerca della Commissione europea, che mira ad aumentare significativamente le capacità dell'agenzia europea e delle forze dell'ordine nazionali di decrittare le informazioni legalmente ottenute nelle indagini penali[18].

Per rendere le cose più complesse, alla fine di marzo 2021, Google ha unilateralmente fermato un cyberattacco – che sfruttava vulnerabilità cd. "*zero-days*"[19]– condotto da un governo occidentale "alleato degli USA" a fini antiterroristici, sollevando inevitabilmente questioni politiche, etiche e legali intorno alle pratiche di *hacking* di Stato[20] – non per questo necessariamente lecite[21].

La crittografia non deve essere considerata una tecnologia esente da "costi": paradossalmente, tali tecnologie di sicurezza digitale generano dei rischi per i beni che si prefiggono di tutelare, ossia la sicurezza e i diritti fondamentali degli individui, in quanto i governi spesso rivendicano, in un'ottica di *trade-offs*, la supremazia della sicurezza sulle libertà.

3. L'utilizzo dell'AI nell'analisi del traffico criptato: nuove frontiere per l'analisi dei metadati

Una valida alternativa alla decriptazione dei contenuti comunicativi è l'analisi dei cd. "dati esterni al traffico" criptato, cioè l'analisi dei metadati, alimentata da algoritmi di IA. Tali tecniche preservano

[17] B. J. Koops, E. Kosta, *op. cit.*, pp. 898-899.

[18] Europol, *Europol and the European Commission inaugurate a new decryption platform to tackle the challenge of encrypted material for law enforcement investigations*, 18 dicembre 2020.

[19] Trattasi di una vulnerabilità nel sistema non ancora di dominio pubblico e di conseguenza utilizzabile senza alcun tipo di blocco da parte di chi ne è a conoscenza almeno sino a quando il produttore non introdurrà una correzione (*patch*).

[20] P. O'Neill, *Google's top security teams unilaterally shut down a counterterrorism operation,* in *MIT Technology Review*, 2021.

[21] Si veda lo scandalo "Pegasus" emerso, dal luglio 2021, grazie a diverse inchieste del *The Guardian*: https://www.theguardian.com/news/series/pegasus-project.

l'integrità della crittografia, anche della tecnologia E2E, in quanto non ricorrono alla "rottura" del meccanismo al fine di vedere il contenuto della comunicazione. In primo luogo, da un punto di vista tecnico, questa sezione mostrerà fino a che punto tali pratiche permettano di trarre inferenze di valore e quindi ottenere profili accurati degli individui. Poi, si analizzerà il quadro giuridico europeo, esistente e futuro, applicabile al trattamento dei metadati.

Mentre i dati di contenuto presentano elementi di ambiguità e interpretazione soggettiva, i metadati di contesto sono – sotto certi aspetti – più significativi e oggettivi, dal momento che riguardano l'ora, la data, la fonte, la destinazione e i campi di lunghezza della comunicazione consegnata dal dispositivo; in altre parole, «definiscono le informazioni di contesto nel quale l'oggetto informazionale si è formato, è stato condiviso, utilizzato (e.g., geolocalizzazione, *micro-tagging*)»[22]. Alcuni autori hanno però sostenuto come la tradizionale distinzione tra dati e metadati, metaforicamente rappresentata dal binomio *contenuto – busta*, non sarebbe più efficace per un duplice ordine di motivi. In primo luogo, potrebbe suggerire surrettiziamente l'ipotesi che il contenuto della comunicazione sia più sensibile dei metadati; e, in secondo luogo, i confini tra contenuto e metadati, nella comunicazione in rete, sono sempre più sfumati[23]. Un approccio relativistico per distinguere contenuto e metadati considera il contesto specifico in cui l'informazione si è formata o viene utilizzata: ad esempio, un URL è una "istruzione di consegna", cioè *metadato*, e allo stesso tempo *dato*, in quanto significa essenzialmente inviare un messaggio che dice "per favore rimandami la pagina trovata a questo URL"[24].

Dal punto di vista giuridico, con specifico riferimento alla materia della *privacy* e protezione dei dati, è pacifico che i metadati siano essenzialmente dati personali e, pertanto, che il loro trattamento non sia meno delicato dei dati di contenuto. Il cd. "test di identificabilità" stabilito dal considerando 26 del GDPR, da leggere in combinato dispo-

[22] M. Palmirani, M. Martoni, *Big data, governance dei dati e nuove vulnerabilità*, in XXXV POLITEIA, 2019, 136, p. 10.

[23] L. Mitrou, *Communications Data Retention: A Pandora's Box for Rights and Liberties?* in A. Acquisti et al. (a cura di) *Digital privacy: Theory, technologies, and practices*, Auerbach Publications, 2008, p. 422. Cfr. con Opinione dell'AG Bobek, *Rīgas satiksme*, C-13/16, §95.

[24] C. Conley, *Metadata: Piecing Together a Privacy Solution,* ACLU report, 2014, pp. 4-5.

sto con l'Art. 4 del Regolamento, stabilisce infatti che «si debba tener conto di tutti i mezzi di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare una persona fisica, direttamente o indirettamente». Inoltre, il medesimo considerando precisa che «per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici»[25]. Il test sviluppato dal considerando 26 del GDPR abbraccia essenzialmente un approccio basato sul rischio per determinare se i dati sono personali o meno[26].

Applicando tali criteri al caso dei metadati, il concetto di *fingerprinting* aiuta a fare luce, da un punto di vista tecnico, sul carattere personale nonché estremamente sensibile di tali particolari trattamenti. Osservando, attraverso i metadati, alcune proprietà dei dati criptati, è possibile creare delle sequenze di dati che attribuiscano queste proprietà ai *file* o ai siti *web* e financo dispositivi corrispondenti[27]. Mentre il *website fingerprinting* mira a identificare su quale sito *web*, o parte di esso, un utente stia navigando, analizzando il solo traffico criptato dell'utente[28], il *file fingerprinting*, attraverso l'adozione di algoritmi di *machine learning* (ad esempio, "alberi decisionali" e "random forest"), permette di rilevare dati noti, anche in tempo reale, in canali di comunicazione criptati con alta precisione[29]. Infatti, recenti studi dimostrano che l'IA, come i classificatori di apprendimento automatico e le reti neurali, migliora la precisione delle inferenze rispetto

[25] GDPR, Considerando 26.

[26] M. Finck, F. Pallas, *They who must not be identified—distinguishing personal from non-personal data under the GDPR,* in *Int. Data Priv. Law*, 2020, 10, 1, p. 15: «se ci fosse un ragionevole rischio di identificazione, i dati dovrebbero essere trattati come dati personali. D'altra parte, se il rischio fosse trascurabile, i dati potrebbero essere trattati come dati non personali, e questo anche se l'identificazione non possa essere esclusa con assoluta certezza». Tuttavia, tale lettura del Regolamento orientata al rischio ha incontrato qualche resistenza, soprattutto nel cosiddetto "approccio assolutista" del Gruppo di lavoro "Articolo 29", seguito da alcune autorità di controllo, come quella francese e irlandese.

[27] ENISA, *Encrypted traffic analysis,* 2019, p. 27.

[28] P. Sirinam et al., *Deep fingerprinting: Undermining website fingerprinting defenses with deep learning,* in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018.

[29] K. Bottinger et al., *Detecting Fingerprinted Data in TLS Traffic,* in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 2015, pp. 633-638.

all'attività e al comportamento degli utenti. Certamente, questi modelli computazionali – perfezionati da ricercatori in contesti di contrasto a nuove minacce alla *privacy* degli utenti – possono essere impiegati ai fini della prevenzione, di indagine e del perseguimento dei reati.

Nel contesto della "*IoT-surveillance*", inoltre, gli algoritmi di IA si dimostrano particolarmente efficaci nell'analisi di contenuti video criptati. Sulla base delle caratteristiche statistiche dei pacchetti di dati protetti da crittografia, un modello di *machine learning* può classificare il comportamento dell'utente alla base del traffico dati del video di sorveglianza, a condizione che gli schemi del traffico dati delle telecamere di monitoraggio differiscano significativamente quando gli utenti svolgono attività diverse nelle schermate di monitoraggio[30].

L'identificazione del dispositivo, per di più, potrebbe essere argomento ancor più pregnante circa la "sensibilità" dei metadati IoT. Chiunque, attori malintenzionati o forze dell'ordine, potrebbe osservare il volume e tasso di traffico, unitamente ai metadati di intestazione dei pacchetti del traffico di rete per dedurre dettagli sensibili sugli utenti. Il soggetto monitorante potrebbe dedurre informazioni dettagliate sugli stati, le azioni e le tipologie di dispositivi intelligenti e sensori utilizzate, così come le attività correlate degli utenti[31]. La sorveglianza passiva del traffico di rete, modalità con cui si sono sempre svolte le indagini, diventa funzionale ad alimentare algoritmi di apprendimento automatico, i quali, estrapolando da tali dati diverse caratteristiche del dispositivo (ad esempio, orari, caratteristiche dei sensori o dei dispositivi, ecc.) dal traffico criptato, consentono l'identificazione accurata delle interazioni che hanno causato il traffico di rete[32]. In altre parole, colui che monitora può venire a conoscenza delle interazioni tra un utente e un dispositivo attraverso una vasta gamma di categorie, permettendo potenzialmente il *profiling* e altre

[30] J. WANG ET AL., *User Behavior Classification in Encrypted Cloud Camera Traffic,* in *IEEE Global Communications Conference*, 2019.

[31] N. TAKBIRI ET AL., *Matching anonymized and obfuscated time series to users' profiles,* in *IEEE Trans. Inf. Theory*, 2018, 58, 2.

[32] A. ACAR ET AL., *Peek-a-boo: i see your smart home activities, even encrypted!,* in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020.

tecniche invasive della privacy[33]. Infatti, dopo l'identificazione del dispositivo, è possibile dedurre le attività dell'utente dai cambiamenti nei tassi di traffico, correlati ai cambiamenti di stato del dispositivo.

Nel contesto specifico dell'IoT, la protezione dei metadati con mezzi crittografici, che pur è stata sostenuta altrove come una possibile mitigazione contro le attività invasive nella privacy degli utenti[34], è improbabile se non impossibile. I dispositivi IoT sono per lo più limitati in termini di memoria e potenza di calcolo. Ne consegue che non sono adatti per implementare sistemi di comunicazione anonima come The Onion Router (TOR), molto esigenti in termini di capacità di elaborazione e memorizzazione.

Alla luce di ciò, è "ragionevole" attendersi che un soggetto interessato possa individuare una persona fisica mediante l'identificazione delle interazioni di un utente con un dispositivo. Pertanto, queste analisi sui metadati soddisfano la soglia stabilita dal considerando 26 del GDPR.

Il carattere personale dei metadati è ulteriormente confermato dalla normativa speciale applicabile al settore delle comunicazioni elettroniche. In forza del principio *lex generalis – lex specialis*[35], l'attuale quadro giuridico applicabile ai dati personali è in tale ambito la direttiva 2002/58/CE sulla *privacy* e le comunicazioni elettroniche (direttiva ePrivacy). La direttiva ePrivacy è stata adottata nel 2002 – poi modificata nel 2009 – e ha previsto una frammentazione terminologica dell'ampio concetto di metadati: l'articolo 2(b) stabilisce la definizione di dati sul traffico, mentre l'articolo 2(c) definisce i dati di localizzazione. Il considerando 15 specifica, inoltre, che questi dati possono riferirsi all'instradamento, alla durata, al tempo o al volume di una comunicazione, al protocollo utilizzato, all'ubicazione dell'apparecchiatura terminale del mittente o del destinatario, alla rete su cui la comunicazione ha origine o termina, all'inizio, alla fine o alla durata di una connessione.

Al fine di garantire un più elevato *standard* di protezione alla *privacy* nelle comunicazioni elettroniche, la Commissione ha proposto

[33] J. Ren et al., *Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach,* in *IMC '19: Proceedings of the Internet Measurement Conference*, 2019, pp. 276-277.

[34] W. Schulz, J. van Hoboken, *Human Rights and Encryption*, UNESCO, 2016, pp. 22-23.

[35] All'interno di una stessa materia, la normativa speciale prevale su quella di carattere generale.

nel 2017 un Regolamento ePrivacy. Senza soffermarsi troppo sul merito della Proposta nei confronti del trattamento dei metadati, è importante sottolineare che l'articolo 4(3)(a) fa perno su una più ampia definizione di "dati delle comunicazioni elettroniche" per coprire sia il contenuto delle comunicazioni elettroniche che i metadati, specificando ulteriormente questi ultimi all'articolo 4(3)(c). In tal modo, la Proposta elimina essenzialmente i termini "*dati relativi al traffico* e *dati relativi all'ubicazione"*, al fine di ottenere chiarezza giuridica e coerenza con una terminologia più "standardizzata". Tuttavia, come giustamente rilevato dall'EDPS, questa definizione, seppur ampia, non è esaustiva in quanto esclude qualsiasi metadato «che non sia richiesto ai fini della trasmissione, distribuzione o scambio di contenuti di comunicazione elettronica né trattato per la fornitura del servizio», come i dati di localizzazione in un'applicazione di messaggistica istantanea[36]. In conclusione, il futuro Regolamento ePrivacy dovrebbe fornire un quadro giuridico più chiaro e comprensivo per il trattamento di tutti i tipi di metadati.

Avendo inquadrato i termini della questione, cioè la natura altamente sensibile del metadato nel contesto di una ancor timida normativa, siamo pronti a rivolgere ora la nostra attenzione alle specifiche questioni giuridiche sollevate dal dispiegamento di modelli di IA per le attività di contrasto e la sorveglianza in ambienti intelligenti: attraverso l'impiego dei suddetti algoritmi, specialmente nell'analisi dei metadati, le forze di polizia e autorità giudiziarie eviterebbero di ricorrere a pratiche di *hacking*, non violando la crittografia.

4. Metadati e contenuto delle comunicazioni: prospettive alternative nell'ambito della giustizia penale

La panoramica fin qui offerta evidenzia in modo chiaro le potenzialità dell'IA nell'analisi dei metadati, vista come potenziale alternativa ai meccanismi di rottura della crittografia nel traffico delle comunicazioni. Tuttavia, tale osservazione di partenza non ha come necessario precipitato una visione del trattamento incrociato dei dati esterni come

[36] EDPS, *EDPS recommendations on specific aspects of the proposed ePrivacy Regulation*, 2017, p. 7.

operazione "meno invasiva" nei diritti alla *privacy* e alla protezione dei dati. È difatti un dato ormai largamente consolidato sia in giurisprudenza[37], sia in dottrina[38], che l'ingerenza nei diritti fondamentali generata da tali tecniche non sia meno significativa rispetto a quella associata alla captazione del contenuto stesso delle comunicazioni.

Cionondimeno, una prima differenza tra le due tecniche di indagine potrebbe esser apprezzata non tanto dal punto di vista del *vulnus* da esse arrecato al diritto alla *privacy*, bensì da uno "epistemologico". Pur essendo entrambi in grado di fornire informazioni dettagliate sulla sfera privata degli individui, metadati e contenuto delle comunicazioni possono non essere sempre muniti della stessa efficacia persuasiva in ordine ai fatti oggetto di interesse per le autorità di contrasto. Da un lato, a dispetto del ruolo sempre giocato dall'interpretazione, la captazione del contenuto comunicativo offre una rappresentazione diretta delle parole pronunciate, e può dunque costituire prova dichiarativa di un determinato fatto[39]. Dall'altro, lo stesso non può dirsi dell'analisi dei metadati. Nonostante la loro importanza quale fonte di informazioni per gli organi di indagine, i dati esterni non possono essere qualificati come atti comunicativi e possono dunque costituire solo fonti di *inferenza*, cioè punto di partenza per una ricostruzione a contenuto probabilistico di una determinata dinamica. In altre parole, i dati esterni non possono essere considerati prova diretta del fatto che determinate parole siano state pronunciate, o che un determinato soggetto si trovasse in un dato luogo ad un determinato momento; all'opposto, essi possono solo dimostrare – seppur con una certa pro-

[37] Cfr. Corte EDU, 13 settembre 2018, *Big Brother and Others v UK*, nn. 58170/13, 62322/14 and 24960/15), §356; CGUE, 8 aprile 2014, Digital Rights Ireland, cause riunite C-293/12 e C-594/12, §27; CGUE, 21 dicembre 2016, *Tele2 Sverige and Watson and Others*, cause riunite C-203/15 e C-698/15, §99; CGUE, 6 ottobre 2020, *La Quadrature du Net*, cause riunite C-511/18, C-512/18 e C-520/18, §117. In ambito statunitense, v. *Carpenter v. United States*, No. 16-402, 585 U.S. (2018), pp. 12-15. È doveroso notare, tuttavia, che nel panorama italiano la Suprema Corte continui a sostenere un approccio di segno opposto. Si veda, ad esempio, Cass., Sez. III, 19 aprile 2019 (dep. 23 agosto 2019), n. 36380, annotata da I. NERONI REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *Sistema Penale*, 2020, 5, pp. 183-198.

[38] V. *supra* sez. 3.

[39] Sulla distinzione tra prova dichiarativa e critico-indiziaria, v. P. FERRUA, *La prova nel processo penale*, in *Rev. Bras. de Direito Processual Penal*, 2018, 4, 1, pp. 81-128, 96-105. In particolare, si veda la descrizione del carattere complesso dell'intercettazione proposta dall'Autore.

babilità – che determinate parole siano state pronunciate, o che determinati luoghi siano stati visitati da soggetti identificati. In questo senso, i metadati possono qualificarsi come un'importante fonte di informazione per la ricostruzione delle dinamiche alla base di reti criminali, nonché servire quali fondamento di misure a carattere provvisorio o investigativo (come la disposizione di una misura cautelare o di un'intercettazione stessa). Quello che difficilmente sembrano poter fare i metadati, invece, è fondare una condanna oltre il ragionevole dubbio, se non in connessione con altri elementi probatori[40].

Un secondo, e cruciale, profilo di distinzione tra analisi dei metadati e captazione del contenuto delle comunicazioni risiede nelle diverse possibilità di bilanciamento tra diritti fondamentali ed esigenze di sicurezza prospettate da tali tecniche. Come sopra sottolineato, la rottura della crittografia implica per definizione un gioco a somma zero, dove l'accesso al contenuto della comunicazione non può che risolversi in una piena valorizzazione delle esigenze di contrasto alla criminalità a detrimento di quelle di riservatezza (e viceversa). Usando un linguaggio metaforico, per accedere al contenuto è fondamentale avere la giusta chiave per la porta: o non la si ha, e il contenuto rimane protetto dentro le mura di casa; o la si trova, e il contenuto diviene accessibile agli osservatori esterni.

A fronte di questa alternativa binaria, il trattamento dei metadati si presenta invece come un meccanismo più flessibile, in cui l'ingerenza nel diritto alla *privacy* risulta "modellabile" sia per estensione, sia per profondità. Ad esempio, come chiarito dalla stessa Corte Edu, le misure di sorveglianza di massa non configurano sempre una grave restrizione del diritto alla *privacy* e alla protezione dei dati dal punto di vista *individuale*[41]. In tali casi, difatti, l'attenzione delle autorità di contrasto o degli organi delegati è spesso "diluita" nell'ingente mole di informazioni analizzata, con conseguenze certamente più lievi per

[40] Cfr. Art. 192(2) c.p.p.

[41] Tale affermazione non deve essere letta nel senso di sminuire le crescenti preoccupazioni rispetto al concetto di *group privacy*. Se queste assumono particolare rilevanza nel mondo commerciale, consentendo pratiche quali il *targeted advertising*, nell'ambito della giustizia penale le attività delle forze dell'ordine sono (quasi) sempre votate all'identificazione del singolo, e le conseguenze più sensibili per la sfera giuridica degli interessati si realizzano solo quando l'attenzione degli organi competenti si focalizzi su individui ben identificati.

la sfera privata dei singoli interessati[42]. La quantità di dati trattati, l'arco di tempo sul quale le operazioni di trattamento si estendono, nonché il livello di invasività delle inferenze ottenute costituiscono d'altro canto valide coordinate attraverso le quali valutare la serietà dell'ingerenza nei diritti fondamentali dell'individuo[43]. L'IA come tecnologia privilegiata per l'analisi di ingenti volumi di informazioni (i cd. *big data*) sembra dunque essere, in alternativa alle tecniche di *hacking*, un valido strumento per conseguire interferenze più bilanciate nei diritti fondamentali, soddisfacendo al contempo le istanze di sicurezza collettiva.

Nel paradigma di una sempre più crescente produzione di dati nel contesto IoT, vedremo ora come anche la giurisprudenza delle due Corti sovranazionali europee sembri manifestare una maggiore consapevolezza rispetto alle potenzialità di un tale approccio diversificato.

5. Proporzionalità e analisi dei metadati nella giurisprudenza delle Corti europee

Uno sguardo complessivo alla giurisprudenza più recente della Corte Edu e della CGUE rivela una tendenza comune. Nella valutazione dei – sempre discussi – programmi di sorveglianza di massa emerge infatti una maggiore accettazione della compatibilità di tali misure con il sistema europeo multilivello di protezione dei diritti fondamentali. Un primo segno in questo senso arriva dalla Corte di Strasburgo che, nel caso *Big Brother Watch*, stima che gli Stati Parte alla Convenzione abbiano ancora un ampio margine di apprezzamento quanto alla scelta della "fisionomia" dei sistemi di sorveglianza da attuare[44]. Anche alla luce del principio di proporzionalità, dunque, le misure di monitorag-

[42] B. VAN DER SLOOT, E. KOSTA, *Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance*, in *Eur Data Prot L Rev*, 2020, 5, p. 258. Il caso di specie prende le mosse da una serie di ricorsi promossi da diverse associazioni davanti alla Corte Edu, all'indomani delle cd. rivelazioni di Edward Snowden nel 2013. Tali ricorsi, facendo leva sull'Art. 8 CEDU, censuravano i programmi di intercettazione di massa condotti dai servizi di intelligence inglesi sulla base dell'Art. 8(4) del RIPA (*Regulation of Investigatory Powers Act 2000*), nonché le iniziative di *intelligence sharing* portate avanti tra tali organi e le autorità di intelligence statunistensi.

[43] Cfr. CGUE, 2 marzo 2021, *H.K./Prokuratuur*, caso C-746/18, §37.

[44] *Big Brother Watch*, *op. cit.*, §356.

gio indiscriminate non devono essere considerate di per sé contrarie all'Art. 8 CEDU.

Tuttavia, lo scrutinio della Corte diviene necessariamente più severo sulle modalità di realizzazione dei sistemi di sorveglianza in questione. In particolare, la Grande Camera distingue in tali scenari quattro passaggi di crescente interferenza nei diritti fondamentali: la raccolta e iniziale conservazione del contenuto e dati esterni alle comunicazioni; l'applicazione di criteri-filtro prestabiliti (*selectors*) ai dati raccolti; l'esame da parte di analisti delle informazioni filtrate; la conservazione di tali dati e il loro uso per la produzione di report, anche ai fini della condivisione con altri Stati[45]. Man a mano che si procede in tali passaggi, rimarca crucialmente la Corte, maggiori garanzie devono essere apprestate nei confronti degli individui finiti sotto la lente di ingrandimento delle autorità di contrasto[46].

I giudici del Lussemburgo non hanno tardato ad allinearsi almeno in parte al dato di partenza di quest'impostazione, seppur non abbandonando *tout court* la linea costantemente adottata dal caso *Digital Rights Ireland*. Non si pretende, nei confini del presente contributo, di offrire una disanima dettagliata dell'ormai ricca giurisprudenza della CGUE sul tema. Tuttavia, due elementi devono essere posti in luce nel recente caso *La Quadrature du Net*[47]. Anzitutto, come la Corte Edu, la CGUE chiarisce che gli obiettivi di protezione della sicurezza nazionale possono legittimare programmi di sorveglianza *indiscriminati*, per il tempo necessario alla neutralizzazione di una minaccia prevedibile e concreta all'integrità dello Stato[48]. Tale scenario giusti-

[45] Corte Edu, 25 maggio 2021, *Big Brother Watch et al c. Regno Unito*, nn. 58170/13, 62322/14 e 24960/15, §325. Si deve notare che, in questa sistematizzazione delle operazioni di sorveglianza, la Corte non distingue tra programmi di trattamento dei dati esterni e vere e proprie misure di intercettazione.

[46] *Id.*, §330.

[47] Il caso in questione, sulla scia di *Tele2/Watson*, si inserisce in un contenzioso promosso davanti alle giurisdizioni francesi, belga e britanniche da alcune associazioni di attivisti per la *privacy* (tra cui, per l'appunto, la francese *Quadrature du net*). Nei ricorsi presentati, in particolare, si censurava la conformità con la Carta delle legislazioni nazionali adottate in forza dell'Art. 15(1) della direttiva e-Privacy, la quale consente ai *provider* dei servizi di telecomunicazione di procedere a una raccolta indiscriminata dei dati degli utenti ai fini della lotta alla criminalità grave e al terrorismo.

[48] *La Quadrature du Net*, *op. cit.*, §§136-137.

ficherebbe anche l'attivazione di un obbligo legislativo per i *service provider* che – dietro richiesta delle autorità di contrasto – sono tenuti ad effettuare screening indiscriminati dei metadati generati dalle attività degli abbonati, attraverso l'utilizzo di criteri prestabiliti ed in continua evoluzione[49]. Diversamente, in linea con l'approccio anteriore, la lotta alla "mera" criminalità grave giustificherebbe unicamente misure il cui ambito di applicazione sia delimitato da criteri oggettivi (e.g. geografici, soggettivi), i quali dimostrino un nesso di pertinenza tra i dati raccolti e gli obiettivi perseguiti[50].

La Corte si spinge anche oltre nell'esaminare ulteriori ipotesi di interferenza nei diritti fondamentali. Ai nostri fini, in particolare, è significativo il caso della raccolta in tempo reale di dati da parte delle autorità di contrasto. Per la gravità dell'ingerenza, che implica un accesso diretto alle informazioni da parte dell'organismo pubblico, una tale misura limitativa dei diritti dev'essere autorizzata *ex ante* da un'autorità indipendente; il principio di proporzionalità, inoltre, impone che essa sia limitata ad individui determinati, già identificati in quanto soggetti probabilmente connessi ad attività terroristiche[51]. In qualche modo, tale misura viene vista tra l'altro come un'operazione logicamente successiva rispetto alle attività di screening "allargato", volte all'individuazione di target promettenti per le autorità di contrasto.

È proprio in questa prospettiva, difatti, che si inserisce l'argomentazione al cuore di questo contributo. L'IA, quale strumento di contrasto alla criminalità, non dev'essere esclusivamente vista quale tecnologia alla base di invasive attività di monitoraggio; in diverse ipotesi, essa può anche essere parte della soluzione, ponendosi quale mezzo di delimitazione delle attività di sorveglianza più focalizzate sull'individuo, e dunque foriere delle interferenze più significative nei diritti fondamentali. Nella sfera preventiva, questa potenzialità si esprime nei suoi termini più efficaci. In un ambito in cui, a priori, è difficile determinare quali informazioni possano essere utili alla lotta alla criminalità, e a specifici atti illeciti non ancora materializzatisi, l'IA è dotata delle capacità di trattare grandi masse di dati, limitando

[49] *Id.*, §177.
[50] *Id.* §§143-144, 147-148; *Privacy International*, *op. cit.*, §75.
[51] *La Quadrature du Net*, *op. cit.*, 191.

le inferenze più significative ai *target* che sembrano rappresentare un rischio maggiore per la generalità dei consociati.

Certamente non si ignorano i pericoli connessi alle argomentazioni prospettate. La dottrina ha da tempo messo in luce le controindicazioni legate alla proliferazione di sistemi di sorveglianza di massa nelle società democratiche, anche alla luce delle recenti prese di posizione delle Corti europee appena esposte[52]. È tuttavia importante mantenere una prospettiva aperta rispetto alle potenzialità offerte da tecnologie come l'IA, soprattutto in connessione con il cambiamento di paradigma portato dall'avvento dell'IoT. È difatti la crescente complessità delle interazioni e flussi di dati negli "ambienti intelligenti" a richiedere un ripensamento delle categorie finora utilizzate per analizzare le attività di sorveglianza in campo penale, e altrove. L'aumento incontrollato della produzione di dati, nonché dei mezzi disponibili per ricavarne informazioni utili, sembra infatti portare la Corte Edu e la CGUE ad adottare un approccio meno restrittivo rispetto alle misure non chiaramente circoscritte nel loro ambito di applicazione. Per un verso, almeno in campo penale, si riconosce che il trattamento dei dati nei sistemi di sorveglianza di massa non sempre sfocia in gravi interferenze nella vita privata dei singoli; per l'altro, si limitano le misure più invasive – quali quelle che implicano un accesso diretto e in tempo reale da parte delle autorità di contrasto – a soggetti già identificati. Se questo orientamento può chiaramente sfociare in una "normalizzazione della sorveglianza di massa"[53], l'adozione di un rigoroso approccio procedurale – informato al principio di proporzionalità e implementato grazie alle tecniche di IA – sembra essere adatto ad impedire tali derive.

Per arrivare a questo punto, però, un controllo più severo si renderebbe necessario, almeno da parte della Corte Edu. Due infatti sono i fattori che indeboliscono allo stato l'orientamento sostenuto dalla Corte, con l'affioramento di seri pericoli per le garanzie individuali. Un primo problema riguarda l'adozione di un approccio "olistico"

[52] N. NI LODEAIN, *Not So Grand: The Big Brother Watch ECtHR Grand Chamber Judgement*, in *Information Law and Policy Center,* 28 maggio 2021, https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/; M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa*, in *Ejil:Talk!*, 26 maggio 2021, https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa.

[53] M. MILANOVIC, *op. cit.*, *The Grand Normalization of Mass Surveillance*.

nell'esame dei sistemi di sorveglianza censurati. Secondo una linea simile a quella già applicata nei casi incentrati su violazioni dell'Art. 6 CEDU[54], la Corte tende ad esaminare i requisiti di legittimità dei regimi di sorveglianza "nel loro complesso". Ciò significa che le lacune concernenti alcune specifiche garanzie sono suscettibili di essere "compensate" da altre previsioni del sistema[55], con conseguente "diluizione" di determinate protezioni individuali.

Una seconda debolezza riguarda invece l'approccio erroneamente diversificato per la captazione di contenuto comunicativo e metadati. A fronte di una pari invasività dal punto di vista della *privacy*, la Corte non sembra richiedere per l'analisi dei metadati lo stesso standard di garanzie rispetto alle intercettazioni, in particolare rispetto alla supervisione dei criteri di selezione delle informazioni[56]. Ciò avverrebbe anche nel caso in cui la misura di monitoraggio si focalizzi su un individuo ben identificato, ma non si "agganci" un dispositivo specifico[57]. Come sottolineato dal giudice Pinto de Albuquerque, tale rilievo non solo sembra ignorare l'equipollenza di contenuto e dato esterno in termini di potenziali lesioni della sfera privata, ma si lega ancora ad una obsoleta e sofistica tipizzazione delle misure di sorveglianza, che separa quelle riferite al *dispositivo* intercettato da quelle riferite all'*individuo*[58].

6. Conclusioni

Il presente contributo ha evidenziato l'irriducibile *trade-off* di valori che varie tecniche di "intercettazione" – tra cui, l'*hacking* di Stato – pongono in essere, presentando rischi sempre maggiori per gli individui che si muovono in ambienti "intelligenti". Nelle moderne società dell'informazione, così caratterizzate da una proliferazione del flusso

[54] V. MANES, M. CAIANIELLO, *Introduzione al Diritto Penale Europeo*, Giappichelli, Torino, pp. 217-221.

[55] *Big Brother Watch, op. cit.*, §170. Nel caso di specie, tale tecnica è servita ad evitare la censura del sistema di intelligence britannico, che mancava di una precisa tipizzazione dei "reati-presupposto" che legittimavano l'attivazione della misura.

[56] *Big Brother Watch*, *op. cit.*, §421.

[57] *Big Brother Watch*, *op. cit.*, §421.

[58] *Big Brother Watch*, *op. cit.*, Opinione in parte concorrente e in parte dissidente del Giudice Pinto de Albuquerque, §12.

di dati ed un'evoluzione delle aspettative di *privacy*, le maglie della sorveglianza digitale vengono progressivamente allargate, specialmente in senso preventivo. Se tale fenomeno può tradursi in una lesione incontrollata delle libertà fondamentali, almeno in campo penale la tendenza sembra essere quella di rafforzare le garanzie mano a mano che l'attenzione delle autorità di contrasto si focalizza sul singolo.

Anche in questo caso, tuttavia, un bilanciamento più ragionevole tra i diritti fondamentali e le esigenze di sicurezza sembra essere offerto dalle capacità di trattamento dei dati dell'IA. Diversamente dalla rottura della crittografia, che si traduce sempre un gioco a somma zero, l'analisi dei metadati permette di introdurre una pluralità di parametri nel test di proporzionalità, così ottenendo *inferenze* – e dunque, *interferenze* – più calibrate agli obiettivi di sicurezza perseguiti.

In definitiva, a dispetto delle debolezze tuttora presenti negli orientamenti delle due Corti europee, l'IA sembrerebbe ad oggi aprire strade di maggiore equilibrio rispetto alla rottura della crittografia, offrendo così adeguate possibilità di bilanciamento tra i diritti fondamentali alla *privacy* da un lato, e le istanze di protezione della collettività dall'altro.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643019
pp. 363-386 (gennaio 2022)

Fenomenologia dei *Deepfake*: aspetti teorici e operativi per la detection di volti umani "artificiali"

Luca Guarnera[1,2], Oliver Giudice[1], Sebastiano Battiato[1,2]

1. Multimedia Forensics e Deepfake

La Multimedia Forensics (MF) assume un ruolo sempre più rilevante anche grazie alla diffusione dei social network le cui stime attuali sul numero e quantità di dati multimediali (immagini, video e audio) condivisi sulle varie piattaforme hanno raggiunto livelli molto elevati. In generale, i dati multimediali contengono un'impronta digitale univoca, utile per ricostruire la storia dei dati stessi (Forensics Ballistics)[3]; per definire i modelli e le caratteristiche degli strumenti di acquisizione (scanner, fotocamera, ecc.); il social network sui quali sono stati caricati[4]; il software di editing multimediale (es. PhotoShop, GIMP, ecc.) utilizzato per la manipolazione (spesso per scopi dannosi) e molto altro.

L'emergere del fenomeno dei Deepfake ha aperto un nuovo fronte nel settore specifico della creazione di contenuti manipolati. Immagini, video e audio creati con questa nuova potente tecnologia, chiamati anche *media sintetici*, sono generati utilizzando algoritmi di intelligenza

[1] IPLAB – Università di Catania, Catania, Italia.
[2] iCTLab s.r.l. – Spinoff dell'Università di Catania, Catania, Italia.

[3] S. Battiato, O. Giudice, and A. Paratore, *Multimedia Forensics: discovering the history of multimedia contents*. Proceedings of the 17th International Conference on Computer Systems and Technologies, pp. 5–16, 2016.

[4] O. Giudice, et al. *A classification engine for image ballistics of social data.* International Conference on Image Analysis and Processing. Springer, Cham, pp. 625–636, 2017.

artificiale basati su framework chiamati Autoencoder[5] e Generative Adversarial Networks (GAN)[6].

Gli algoritmi per la generazione di Deepfake sono in grado di risolvere compiti come: *image-to-image translation* (ad esempio trasformare un cavallo in una zebra, o trasformare una scena con sfumature invernali in sfumature estive), *sketch-to-image translation* (ad esempio, uno schizzo di una borsa in bianco e nero può essere trasformato in una borsa colorata e reale) e molto altro ancora. Queste tecniche si sono fortemente evolute negli ultimi anni e attualmente esistono algoritmi in grado di cambiare gli attributi dei volti delle persone come il colore dei capelli, il sesso o persino generare in maniera pseudocasuale il volto di una persona. La Figura 1 mostra una panoramica dei principali approcci Deepfake proposti in letteratura.

Molte industrie cinematografiche utilizzano già questi algoritmi per creare doppiaggi video di attori di altissima qualità. Sfortunatamente però, molti sono gli utilizzi per così dire malevoli che generano dei fenomeni deprecabili. Il primo utilizzo inappropriato di questa potente tecnologia si è palesato al grande pubblico nel 2017, dove un utente di Reddit ha sviluppato un algoritmo di Deep Learning in grado di trasferire volti di celebrità in video porno.

I tradizionali algoritmi di Multimedia Forensics presenti in letteratura riguardanti il rilevamento di *forgery* non sono in grado di distinguere i Deepfake dai contenuti multimediali reali con risultati di classificazione elevati. Per questo motivo è emersa la necessità di creare nuovi algoritmi di rilevamento dei Deepfake che fossero in grado di contrastare l'uso malevolo di queste nuove tecnologie.

Come già accennato, tutti i contenuti multimediali contengono un'impronta digitale univoca che può essere estratta per definire, ad esempio, il modello di telecamera utilizzato durante l'acquisizione. È stato possibile dimostrare che anche i Deepfake contengono una traccia unica lasciata dai modelli generativi che può essere utilizzata non solo per risolvere task del tipo *Real Vs. Deepfake* ma anche per definire quale algoritmo di Deep Learning è stato utilizzato per generare i corrispondenti dati sintetici.

[5] D.P. Kingma, M. Welling. *Auto-Encoding Variational Bayes*. arXiv preprint arXiv:1312.6114, 2013.

[6] I. Goodfellow et al., *Generative Adversarial Nets*. Advances in Neural Information Processing Systems, pp. 2672–2680, 2014 (27).

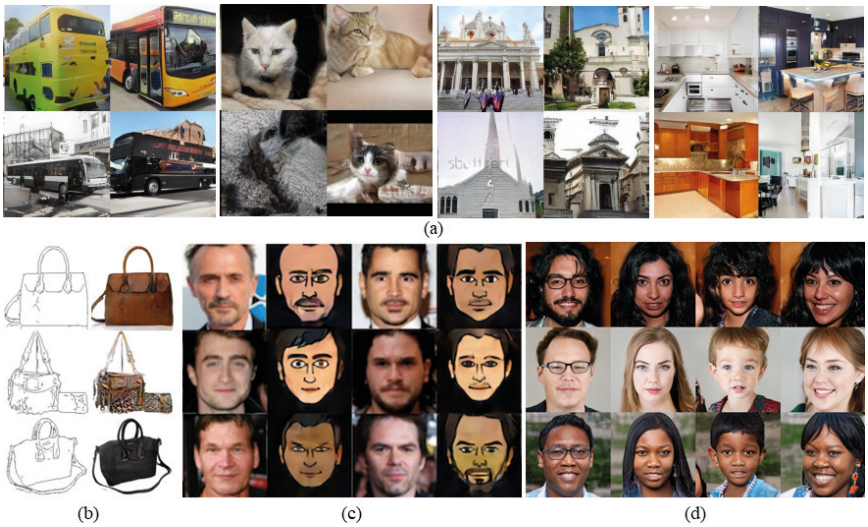


Figura 1. Esempi di immagini Deepfake generate da (a) architettura ProGAN[7]; (b) traduzione "sketch-to-image"[8]; (c) traduzione "Photos-to-Emojis"[9]; (b) architettura StyleGAN[10] che genera il cosiddetto "this person does not exist"[11].

2. Fenomenologia dei Deepfake

Un contenuto multimediale digitale può essere manipolato con molti strumenti e software. Chiunque abbia un pò di esperienza nell'uso di Photoshop o GIMP può "attaccare" le immagini per modificarne il contenuto, la semantica e, stravolgerne il messaggio in esso contenuto. Tuttavia, questo tipo di contraffazione è stato ampiamente studiato negli ultimi anni e sono disponibili anche strumenti commerciali con la capacità di rilevarli e descriverli[12,13].

[7] T. Karras et al., *Progressive Growing of GANs for Improved Quality, Stability, and Variation.* arXiv preprint arXiv:1710.10196, 2017.

[8] P. Isola et al., *Image-to-Image Translation with Conditional Adversarial Networks*. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1125-1134, 2017.

[9] Y. Taigman, A. Polyak, and L. Wolf, *Unsupervised Cross-Domain Image Generation.* arXiv preprint arXiv:1611.02200, 2016.

[10] T. Karras, S. Laine, and T. Aila, *A Style-Based Generator Architecture for Generative Adversarial Networks.* Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4401-4410, 2019.

[11] https://thispersondoesnotexist.com/.

[12] L. Verdoliva, *Media Forensics and Deepfakes: an overview*. IEEE Journal of Selected Topics in Signal Processing 14.5 (2020): 910-932.

[13] A. Piva, *An Overview on Image Forensics*. International Scholarly Research Notices, pp. 1-22, 2013.

I progressi nel campo dell'intelligenza artificiale e nell'elaborazione delle immagini stanno cambiando il modo in cui le persone interagiscono con immagini e video digitali. Nello specifico, l'avvento degli Autoencoder e delle Generative Adversarial Networks (GAN), ha permesso la creazione e la diffusione di tecniche estremamente raffinate in grado di *attaccare* i dati digitali, *alterarli* o *crearne i contenuti da zero*. Questi strumenti sono in grado di ottenere risultati sorprendentemente realistici portando alla nascita del fenomeno *Deepfake*.

Per Deepfake si intendono tutti quei contenuti multimediali sinteticamente alterati o creati sfruttando i *modelli generativi* nel settore del Deep Learning. In generale, un modello generativo è un algoritmo che tecnicamente si occupa di "imparare" la distribuzione dei dati di addestramento al fine di generare nuovi dati con caratteristiche simili rispetto al set di dati originale. In altre parole, nel caso in cui volessimo creare oggetti della categoria "automobili", allora dovremmo creare un algoritmo che sia in grado di "inferire" la distribuzione di dati che caratterizza varie tipologie di automobili, ovvero catturare gli elementi essenziali (come i colori, le forme, ecc.) che definiscono l'oggetto in questione al fine di riprodurlo nel miglior modo possibile. Non è possibile ottenere esattamente la stessa distribuzione dei dati di input, ma in generale si riesce a definire un modello che si avvicina il più possibile alla vera distribuzione dei dati di training. Per raggiungere questo obiettivo, negli ultimi anni i ricercatori hanno utilizzato la potenza delle *Deep Neural Networks* (*Reti Neurali Profonde)* per apprendere una funzione che può approssimare la distribuzione del modello di dati di addestramento.

Questi metodi generativi si sono evoluti molto rapidamente dando luogo a dati multimediali sintetici estremamente sorprendenti, soprattutto per quanto riguarda l'elevata qualità dei dettagli dei contenuti Deepfake creati.

Diversi utilizzi di tale tecnologia sono stati già sviluppati ed applicati in vari contesti come, ad esempio, il *Salvador Dalì Museum* in Florida (Figura 2(a)) che ha dato la possibilità ai visitatori del museo di interagire con l'artista[14]; l'applicazione che presenta il calciatore David Beckham[15] che parla nove lingue diverse (Figura 2(b)) per una campagna contro la *malaria*; approcci in grado di descrivere un dipinto o un paesaggio ai non vedenti rendendoli capaci di connettersi con l'ambiente circostante.

[14] https://www.youtube.com/watch?v=mPtcU9VmIIE.
[15] https://www.youtube.com/watch?v=QiiSAvKJIHo.

(a) (b)

Figura 2(a). Esempi di immagini di Salvador Dalì (b) Esempi di immagini di David Beckham in cui parla 3 di 9 lingue diverse.

Recentemente, volti di veline, politici, attori, presentatori televisivi e molti altri sono stati oggetto principale di attacchi mediante Deepfake: uno dei primi esempi è il famoso scambio di volti di Jim Carrey sul corpo di Alison Brie[16] (Figura 3(a)), o Mr. Bean è Charlize Theron nella versione Deepfake dello spot di J'adore[17] (Figura 3(b)), e ancora Jim Carrey invece di Jack Nicholson in Shining[18] (Figura 3(c)), o Tom Cruise che sostituisce Robert Downey Jr. in Iron Man[19] (Figura 3(d)). La tecnologia Deepfake è stata utilizzata anche nel mondo della politica, ad esempio quando il volto del presidente argentino Mauricio Macri è stato sostituito da quello di A. Hitler o il volto del cancelliere Angela Merkel sostituito dal volto di Donald Trump. Quest'ultimo nel 2019 è stato oggetto di un Deepfake in cui veniva deriso per il suo aspetto e il colore della pelle. Nel 2018, invece, è stato creato un Deepfake dal regista Jordan Peele utilizzando l'immagine di Barack Obama in cui pronunciava parole mai dette, ma il messaggio era semplice: mettere in guardia sul pericolo dell'uso illecito di questa potente tecnologia.

[16] https://www.youtube.com/watch?v=SEar_6UtX9U.
[17] https://www.youtube.com/watch?v=tDAToEnJEY8.
[18] https://www.youtube.com/watch?v=JbzVhzNaTdI.
[19] https://www.youtube.com/watch?v=iDM69UEyM3w.

Figura 3. Esempi di Deepfake: (a) il volto di Jim Carrey è stato trasferito sul corpo di Alison Brie, (b) Mr. Bean è Charlize Theron in una versione Deepfake dello spot di J'adore, (c) Jim Carrey invece di Jack Nicholson in Shining e (d) Tom Cruise sostituisce Robert Downey Jr. in Iron Man.

Le manipolazioni sui volti delle persone riguardano quattro modalità principali:

- *intera sintesi del volto* (*entire face synthesis):* crea intere immagini di volti inesistenti[10,20,21]. Questa manipolazione potrebbe essere utilizzata ad esempio nel campo dei videogiochi per creare nuovi protagonisti, ma potrebbe anche essere utilizzata per generare disinformazione (es. creazione di profili falsi nei social network);
- *manipolazione degli attributi (attribute manipulation):* modifica gli attributi del viso come il colore dei capelli, il sesso, l'età, ecc. Questo tipo di manipolazione è noto anche come *modifica del viso* o *ritocco del viso*. Attualmente, diverse tecnologie

[20] T. Karras et al. *Analyzing and Improving the Image Quality of StyleGAN*. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 8110-8119, 2020.

[21] T. Karras et al. *Training Generative Adversarial Networks with Limited Data*. arXiv preprint arXiv:2006.06676, 2020.

hanno realizzato questo tipo di manipolazione, come l'applicazione mobile chiamata FaceApp[31] o i potenti motori GAN come StarGAN[22], StarGAN-v2[23];

- *scambio di identità (identity swap):* sostituisce il volto di una persona in un video con il volto di un'altra persona. Questo tipo di manipolazione può essere ottenuto considerando tecniche di Deep Learning (come Deepfakes[24]) e approcci di computer grafica (come FaceSwap[25]). Come riportato in precedenza, queste manipolazioni possono essere sfruttate per scopi industriali (come all'interno dell'industria cinematografica) ma anche per scopi dannosi come nella creazione di video pornografici;
- *scambio di espressioni (expression swap)*: modifica l'espressione facciale della persona. Questo tipo di manipolazione è anche conosciuto come *reenactment del volto*. Face2Face[26] e NeuralTexture[27] sono esempi di questa tecnologia ed è possibile usarli per diffondere informazioni false come il video di Obama[28], creato da Buzzfeed in collaborazione con Monkeypaw Studios, o il video in cui Mark Zuckerberg[29] realizza una serie di affermazioni sulla capacità della piattaforma di rubare i dati dei suoi utenti.

La Figura 4 mostra esempi di queste tipologie di manipolazioni di volti di persone.

[22] Y. Choi et al. *StarGAN: Unified Generative Adversarial Networks for Multi-Domain Image-to-Image Translation*. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 8789-8797, 2018.

[23] CHOI, Yunjey, et al. *StarGAN v2: Diverse Image Synthesis for Multiple Domains.* Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 8188-8197, 2020.

[24] https://github.com/deepfakes/faceswap.

[25] https://github.com/MarekKowalski/FaceSwap.

[26] J. THIES et al., *Face2face: Real-Time Face Capture and Reenactment of RGB Videos*. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2387-2395, 2016.

[27] J. THIES et al, *Deferred Neural Rendering: Image Synthesis Using Neural Textures.* ACM Transactions on Graphics (TOG) 38.4 (2019): 1-12.

[28] https://www.youtube.com/watch?v=cQ54GDm1eL0.

[29] https://www.youtube.com/watch?v=NbedWhzx1rs.

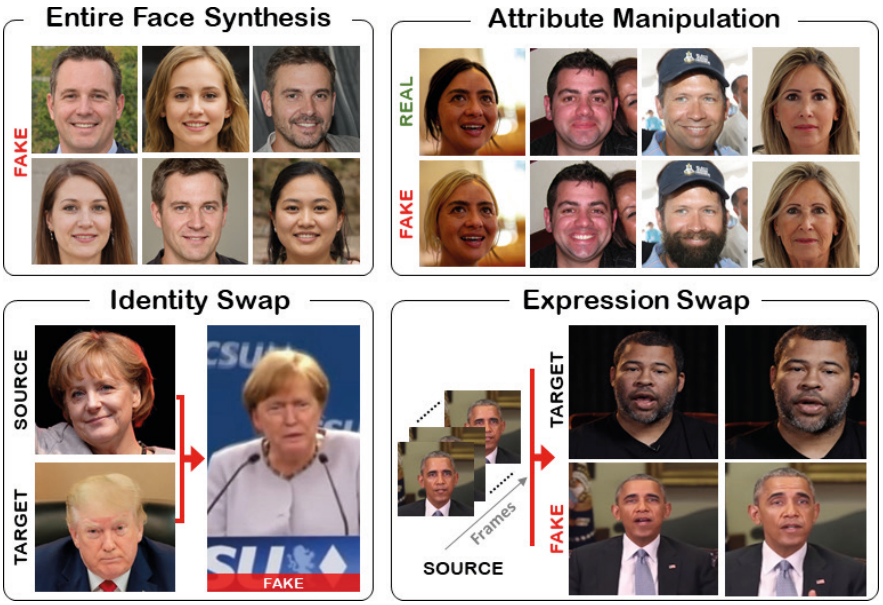


Figura 4. Manipolazioni sui volti delle persone. *Intera sintesi del volto*: immagine generata dalle architetture StyleGAN[10] e StyleGAN2[21]. *Manipolazione degli attributi*: esempi di immagini generate dal motore StarGAN[23]. *Scambio di identità*: il volto della cancelliera Angela Merkel sostituito dal volto di Donald Trump. *Scambio di espressioni*: esempi di fotogrammi video del Deepfake di Barack Obama.

Le architetture Deepfake si sono evolute considerevolmente negli ultimi anni, ottenendo contenuti multimediali sintetici con una risoluzione sempre più elevata, una qualità dei dettagli sempre più accurata e una quasi completa assenza di anomalie (Figura 5).

La manipolazione dei volti umani è nata ancor prima dell'avvento dei Deepfake. Ciò che oggi chiamiamo "reenactment del volto" si può in qualche modo risalire a una prima applicazione di un progetto accademico del 1997, con uno strumento chiamato *Video Rewrite* proposto da Bregler et al.[30] che consentiva la creazione automatica di un nuovo video di una persona in grado di mimare una sequenza di parole (data come traccia audio di riferimento) mai dette dal protagonista del video originale. Queste tecnologie si sono sorprendentemente evolute negli anni, raggiungendo risultati sempre più sofisticati, come il lavoro proposto da Thies et al.[27] con il framework chiamato *Face2Face* in cui

[30] C. Bregler, M. Covell, and M. Slaney. *Video Rewrite: Driving Visual Speech with Audio*. Proceedings of the 24th Annual Conference on Computer Graphics and Interactive Techniques, pp. 353-360, 1997.

l'obiettivo di animare in tempo reale le espressioni facciali di un video di destinazione dalle espressioni facciali di una persona catturate da una fotocamera (webcam).

Figura 5. L'evoluzione dei modelli generativi (ad esempio tramite architetture GAN) per la creazione di contenuti multimediali sintetici (da Goodfellow et al.[6] (2014) a Karras et al.[10] (2018)).

La tecnologia Deepfake non è solo coinvolta in attività relative alla manipolazione di volti di persone, ma potrebbe essere utilizzata per scambiare o generare luoghi, animali, oggetti, ecc. in maniera sorprendentemente realistica. In effetti, questo potrebbe portare un'innovazione dirompente in molti ambiti lavorativi, come nell'industria automobilistica o in architettura, poiché è possibile generare un'auto o un appartamento attraverso *GAN* dedicati o nell'industria cinematografica dove è possibile, quando necessario, sostituire il volto di uno *stuntman* con un attore. Inoltre, la creazione di Deepfake sta diventando estremamente facile: applicazioni come FaceApp[31], sono in grado di produrre trasformazioni sui volti umani come il cambio di genere, l'invecchiamento, e tanto altro ancora. I risultati sono sorprendentemente realistici ed estremamente facili da produrre anche per utenti non esperti con pochi tocchi sul proprio smartphone. Sfortunatamente diversi video di Deepfake collegati alla pornografia sono stati utilizzati per screditare attrici famose come Emma Watson o Angelina Jolie, o in altri contesti sono stati utilizzati per diffondere disinformazione e fake news.

[31] https://www.faceapp.com/.

Risulta quindi assolutamente necessario creare nuove tecniche in grado di rilevare e contrastare questo nuovo potente fenomeno[12,32].

Sebbene il rilevamento di un Deepfake sia difficile per gli umani, lavori recenti hanno dimostrato che potrebbero essere rilevati in modo sorprendentemente semplice utilizzando le *Reti Neurali Convoluzionali* (CNN)[33,34,35,36,37] specificamente addestrate al compito. Tuttavia, le soluzioni basate su CNN presentate fino ad oggi, mancano di robustezza, capacità di generalizzazione e spiegabilità poiché risultano essere estremamente specifici per il contesto in cui sono stati formati e, inoltre, essendo molto profonde, le architetture neurali tendono ad estrarre la semantica sottostante dalle immagini senza dedurre alcuna impronta digitale univoca.

Diverse grandi aziende, da Facebook a Microsoft, hanno deciso di agire contro questo fenomeno. Rossler et al. hanno creato un database di video Deepfake[38], mentre Facebook e Microsoft hanno lanciato l'iniziativa *Deepfake Detection Challenge*[39] invitando i ricercatori di tutto il mondo a creare nuovi strumenti per rilevare Deepfake e media multimediali manipolati.

Al fine di ottenere soluzioni in grado di definire se un contenuto multimediale è un Deepfake, occorre comprendere come questi dati vengono creati in modo da identificare quelle tracce univoche lasciate dai vari processi generativi. Nella sezione successiva verranno descritte le principali tecnologie utilizzate per la creazione dei Deepfake.

[32] L. Guarnera et al., *Preliminary Forensics Analysis of Deepfake Image*s, 2020 AEIT International Annual Conference (AEIT). IEEE, pp. 1-6, 2020.

[33] X. Xuan et al., *On the Generalization of GAN Image Forensics*. Chinese Conference on Biometric Recognition. Springer, Cham, pp. 134-141, 2019.

[34] H. Chih-Chung, Y. Zhuang, and C. Lee, *Deep Fake Image Detection Based on Pairwise Learning*. Applied Sciences 10.1, 2020: 370.

[35] A. Gandhi and J. Shomik, *Adversarial Perturbations Fool Deepfake Detectors.* 2020 International Joint Conference on Neural Networks (IJCNN). IEEE, pp. 1-8, 2020.

[36] L. Li et al., *Face X-ray for More General Face Forgery Detection.* Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 5001-5010, 2020.

[37] SY. Wang et al. *CNN-generated images are surprisingly easy to spot... for now*. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 8695-8704, 2020.

[38] A. Rossler et al. *Faceforensics++: Learning to Detect Manipulated Facial Images*. Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 1-11, 2019.

[39] https://deepfakedetectionchallenge.ai.

2.1. *Metodi di creazione di Deepfake*

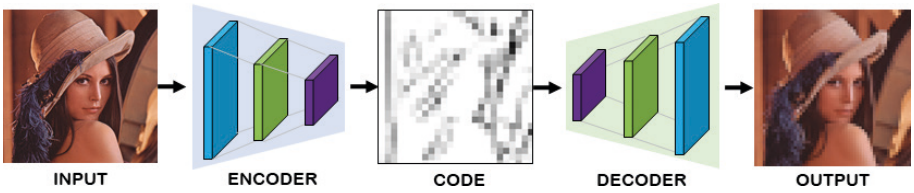


Figura 6. Flusso di lavoro del motore AE. Data un'immagine come input al codificatore (encoder), genererà una rappresentazione latente (code) che verrà utilizzata dal decodificatore (decoder) per generare la stessa immagine come output.

Una delle prime tecniche di Deep Learning utilizzate per creare Deepfake sono stati gli Autoencoder (AE)[40.]. In generale, un'architettura Autoencoder è composta da tre componenti: *codificatore (encoder), rappresentazione latente (code)* e *decodificatore (decoder)*.

La Figura 6 mostra uno schema generico di un'architettura AE. Il codificatore prende un'immagine come input e genera un *code* o la cosiddetta *rappresentazione latente* che è una rappresentazione intermedia di dimensione inferiore dei dati di input. L'obiettivo del decoder è ricostruire un dato multimediale con le stesse caratteristiche (dimensioni, ecc.) dell'input a partire dalla *rappresentazione latente*. Notare che il decoder non conosce i dati di input all'encoder. Nello specifico, il decoder sarà in grado di ricostruire un'immagine tanto più simile a quella in input all'encoder quando l'encoder genererà la migliore rappresentazione latente dell'input. Per fare ciò, l'architettura sarà addestrata in modo da minimizzare l'errore tra la differenza della struttura dei dati di input rispetto ai dati ricostruiti dal decoder. Questo processo termina quando la perdita di ricostruzione è ridotta al minimo, risultando in un output molto simile all'input.

[40] Una rete neurale di apprendimento auto-supervisionata progettata per ricostruire il suo input da una rappresentazione dimensionale inferiore.

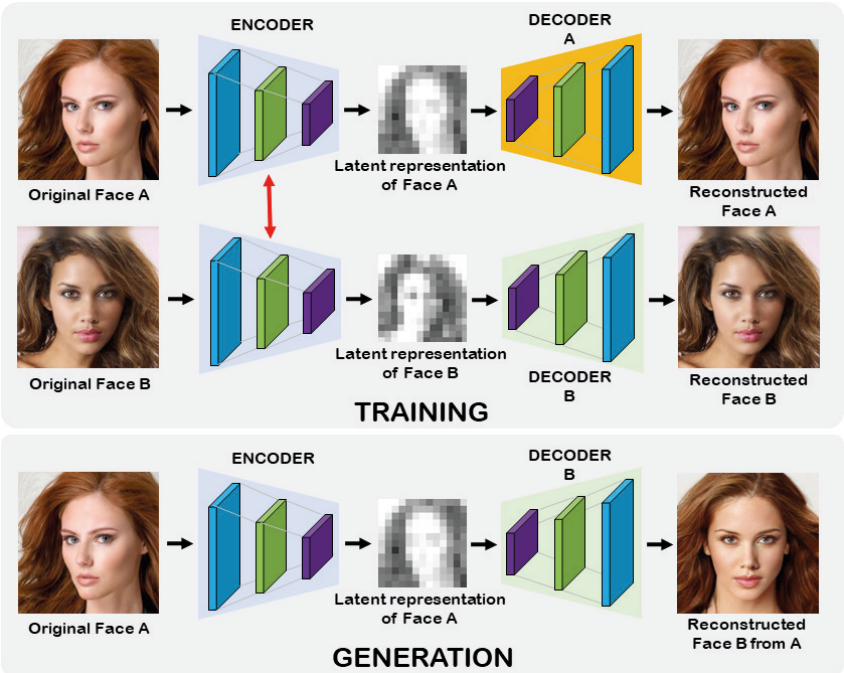


Figura 7. Scambio di volti utilizzando due coppie di codificatori e decodificatori. Questo approccio viene utilizzato per apprendere le caratteristiche latenti dei volti nella fase di allenamento. Successivamente, la coppia di decodificatori viene scambiata per generare la Faccia A con le caratteristiche della Faccia B.

Un'architettura basata su AE per la creazione di Deepfake è costituita dai cosiddetti *Deep Autoencoder*[41]. Come descritto in precedenza, l'obiettivo del decodificatore è provare a ricostruire l'immagine di input al codificatore. Consideriamo il caso in cui il compito di un framework Deepfake è lo scambio di volti tra due persone. Questo può essere fatto considerando due coppie encoder-decoder. Ogni coppia verrà addestrata su una serie di immagini, come due architetture standard. La caratteristica principale di questo framework è che i parametri dei due encoder sono condivisi al fine di trovare e apprendere la somiglianza tra due insiemi di immagini del viso (posizioni degli occhi, posizioni della bocca, ecc.). In altre parole, i due encoder vengono considerati come "gemelli" poiché condividono gli stessi parametri di rete

[41] P. Vincent et al., *Extracting and Composing Robust Features with Denoising Autoencoders.* Proceedings of the 25th International Conference on Machine learning, pp. 1096-1103, 2008.

neurale. In particolare, una volta completato l'addestramento delle due coppie di codificatore e decodificatore, i due decodificatori vengono scambiati al fine di utilizzare il codificatore dell'immagine sorgente e il decodificatore dell'immagine bersaglio per generare l'immagine bersaglio con le caratteristiche dell'immagine sorgente. FakeApp[42], ZAO[43], FaceSwap[44] e REFACE[45] sono alcune delle prime applicazioni sviluppate per la creazione di Deepfake considerando questo approccio. Un esempio di manipolazione del face-swap che sfrutta questo principio è mostrato nella Figura 7 in cui l'encoder allenato con *Face A* è connesso al decoder di *Face B* per ricostruire la *Face B* dalla *Face A* originale.

Risultati sorprendentemente realistici sono ottenuti attraverso framework chiamati *Generative Adversarial Networks* (GAN) introdotte per la prima volta da Goodfellow et al.[6]. Gli autori hanno proposto un nuovo approccio in cui due modelli si addestrano contemporaneamente: un modello generativo *G*, che impara la distribuzione dei dati di input, e un modello discriminativo *D*, che stima la probabilità che un campione arrivi dai dati di addestramento anziché da *G*. La procedura di allenamento per *G* consiste nel massimizzare la probabilità che *D* commetta un errore, risultando così in una partita a due giocatori di tipo "min-max". Matematicamente, il generatore accetta un input casuale z (il quale potrebbe essere un numero, una sequenza di numeri ecc.) con densità di probabilità p_z e restituisce un output $x = G(z, \theta_g)$ secondo una certa distribuzione di probabilità p_g (θ_g rappresenta i parametri del modello generativo). Il discriminatore, $D(x, \theta_d)$ calcola la probabilità che x provenga dalla distribuzione dei dati di training p_{data} (θ_d rappresenta i parametri del modello discriminativo). L'obiettivo è ottenere un generatore che sia un buon stimatore di p_{data}. Quando ciò accade, il discriminatore verrà "ingannato" e non sarà più in grado di distinguere immagini provenienti da p_{data} e p_g; quindi p_g seguirà la distribuzione di probabilità mirata, ovvero p_{data}.

In sintesi, il discriminatore viene addestrato in modo da massimizzare la probabilità di assegnare l'etichetta corretta sia agli esempi di addestramento che ai campioni di *G*. Simultaneamente, il generatore viene addestrato in modo da minimizzare la distanza tra le due distribuzioni.

[42] https://faceswap.dev/.
[43] https://apps.apple.com/cn/app/zao/id1465199127.
[44] https://www.malavida.com/en/soft/fakeapp/.
[45] https://reface.app/.

La Figura 8 mostra una struttura semplificata di un framework GAN. *G* può essere pensato come una squadra di falsari che cercano di produrre valuta falsa, mentre *D* può essere associato alla polizia, cercando di rilevare l'attività dannosa.

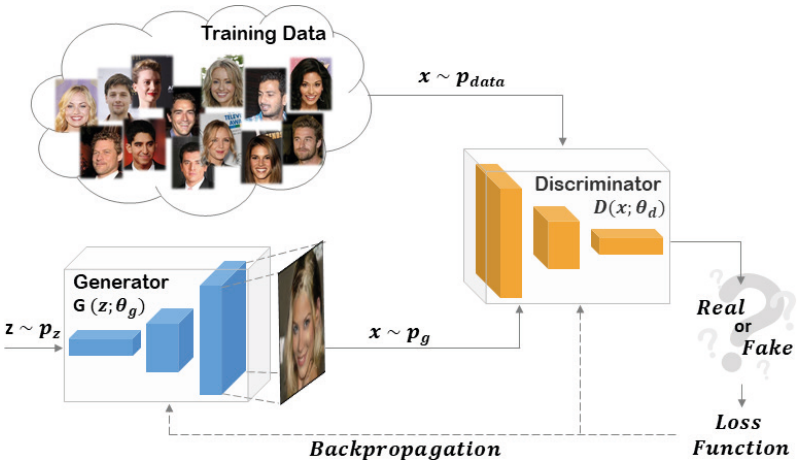


Figura 8. Schema generico di un framework GAN.

I progressi nelle architetture GAN portano a diversi lavori basati sulla manipolazione di volti umani. Come descritto precedentemente, le principali tecniche per manipolare i volti delle persone sono lo scambio di volti, la rievocazione del volto, la manipolazione degli attributi e la sintesi dell'intera faccia.

In generale, i metodi tradizionali basati sullo scambio di volti[46],[47] consistono nel:

- rilevamento del volto nelle immagini di origine e selezione di un'immagine del volto candidato nel set di dati di addestramento con caratteristiche simili all'input;
- sostituzione dei componenti del viso (come occhi, naso e bocca), regolazione della struttura dell'immagine (illuminazione, colori, ecc.) e fusione dei due volti;

[46] D. Bitouk et al., *Face Swapping: Automatically Replacing Faces in Photographs*. ACM SIGGRAPH 2008 papers. 2008, pp.1-8.

[47] B.M. Smith and Z. Li, *Joint Face Alignment with Non-parametric Shape Models*. European Conference on Computer Vision. Springer, Berlin, Heidelberg, pp. 43-56, 2012.

– classificare l'output calcolando una distanza sulla regione di sovrapposizione.

Con l'evoluzione dei metodi basati sul Deep Learning i principali limiti di queste tecniche (quali la perdita di espressione dell'immagine del volto in ingresso; la presenza di artefatti, posizioni innaturali del volto finale, ecc.) sono stati quasi completamente risolti ottenendo risultati più sofisticati e realistici.

In passato queste manipolazioni venivano eseguite con tecniche di Computer Grafica, ricostruendo il volto a partire da un modello 3D[48]. Queste tecniche si sono evolute con il sorprendente sviluppo dei modelli basati su GAN (ad esempio Nirkin et al.[49]).

Approcci recenti come quello proposto da Korshunova et al.[50] sono in grado di trasferire il contenuto semantico (ad esempio, postura facciale, espressione facciale e condizioni di illuminazione) dell'immagine di input nell'immagine di output.

Natsume et al.[51] hanno proposto l'implementazione di *RSGAN* tramite due Autoencoder per codificare rispettivamente la rappresentazione latente delle regioni del viso e dei capelli. Un limite di questo metodo è che non gestisce bene le occlusioni facciali (occhiali, viso parzialmente coperto da oggetti, ecc.) ottenendo immagini con artefatti. Questo problema è stato affrontato da Li et al.[52] con il framework chiamato *FaceShifter* ottenendo ottimi risultati nel task di face-swap.

Un'altra categoria di manipolazione di volti di persone riguarda la classe di algoritmi inerenti al *reenactment*, i quali consentono di manipolare le espressioni facciali di una persona (trasferimento di gesti facciali, movimenti oculari, ecc.). In generale, questa tecnica viene applicata ai video multimediali. Il lavoro di Thies et al.[53] è stato tra i primi a

[48] Y. Nirkin et al., *On Face Segmentation, Face Swapping, and Face Perception.* 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018). IEEE, pp. 98-105, 2018.

[49] Y. Nirkin et al., *FSGAN: Subject Agnostic Face Swapping and Reenactment.* Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 7184-7193, 2019.

[50] I. Korshunova et al., *Fast Face-swap Using Convolutional Neural Networks.* Proceedings of the IEEE International Conference on Computer Vision, pp. 3677-3685, 2017.

[51] R. Natsume, et al., *RSGAN: Face Swapping and Editing using Face and Hair Representation in Latent Spaces.* arXiv preprint arXiv:1804.03447, 2018.

[52] L. Li et al., *Faceshifter: Towards High Fidelity and Occlusion Aware Face Swapping*. arXiv preprint arXiv:1912.13457, 2019.

[53] J. Thies et al., *Real-time Expression Transfer for Facial Reenactment.* ACM Trans. Graph. 34.6, 2015, 183-1.

proporre tecniche di ricostruzione del volto sfruttando un sensore RGB-D per tracciare e ricostruire il modello 3D di un attore sorgente e target. Uno dei metodi più potenti basati su approcci matematici per il Face-Reenactment è il lavoro proposto da Thies et al.[27] con l'architettura chiamata *Face2Face*. Questo metodo è in grado di alterare i movimenti facciali dei flussi video RGB in tempo reale, utilizzando una webcam standard per catturare i movimenti da alterare nella sorgente.

Le tecniche di ricostruzione del volto si sono evolute molto negli ultimi anni portando non solo a modificare l'espressione facciale ma anche a rianimare i video di ritratto cambiando ad esempio la posa della testa, lo sguardo degli occhi e molto altro. Nel lavoro di Kim et al.[54], viene inizialmente calcolata una rappresentazione parametrica del volto per produrre un rendering sintetico dell'identità del bersaglio. Una rete di traduzione render-to-video basata su GAN condizionali (cGAN) elabora questa rappresentazione per generare un rendering sintetico in fotogrammi video fotorealistici. In generale, queste tecniche richiedono una grande quantità di dati di addestramento. Questa limitazione è stata recentemente superata proponendo approcci di rievocazione facciale "one-shot" utilizzando una o un numero limitato di immagini di origine[55].

Infine, le ultime due categorie che possiamo considerare per la manipolazione del viso riguardano la sintesi dell'intero volto e la manipolazione degli attributi di volti umani.

In generale, la manipolazione degli attributi del viso utilizza tecniche di *image-to-image translation* per affrontare la diversità di stile[56,57,58]. Il principale limite di questi metodi è la mappatura tra due domini che non li rende scalabili al numero crescente di domini. In altre parole, è possibile addestrare un modello per cambiare, ad esempio, solo il colore dei capelli, cambiare solo l'espressione facciale. Matematicamente, se considerassimo N domini, questi metodi richiederebbero

[54] K. Hyeongwoo et al., *Deep Video Portraits.* ACM Transactions on Graphics (TOG) 37.4. 2018, 1-14.

[55] O. Wiles et al., *X2Face: A Network for Controlling Face Generation using Images, Audio, and Pose Codes*. Proceedings of the European Conference on Computer Vision (ECCV), pp. 670-686, 2018.

[56] A. Almahairi et al., *Augmented CycleGAN: Learning Many-to-Many Mappings from Unpaired Data.* International Conference on Machine Learning. PMLR, pp. 195-204, 2018.

[57] X. Huang et al., *Multimodal Unsupervised Image-to-Image Translation*. Proceedings of the European conference on computer vision (ECCV), pp. 172-189, 2018.

[58] Q. Mao et al., *Mode Seeking Generative Adversarial Networks for Diverse Image Synthesis.* Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 1429-1437, 2019.

un addestramento di *N* x *(N-1)* generatori per gestire le *traduzioni* di ogni dominio. Questi approcci sembrano alquanto limitati sotto questo aspetto. Per cercare di creare un modello unico per risolvere il compito di *image-to-image translation* su più domini, diversi studi in letteratura sono stati proposti.

StarGAN[23] è un'architettura in grado di eseguire compiti di *image-to-image translation* su più domini utilizzando un unico modello. Data un'etichetta casuale come input, come il colore dei capelli, l'espressione facciale, ecc., il framework è in grado di eseguire un'operazione di *image-to-image translation*. I risultati hanno dimostrato come *StarGAN* riesce a generare immagini di qualità visiva superiore rispetto ai metodi esistenti in letteratura. Questa è una delle prime migliori soluzioni in questa categoria di manipolazione, ma *StarGAN* ha una limitazione importante: non cattura la natura multimodale della distribuzione dei dati. In altre parole, questa architettura apprende una mappatura deterministica di ciascun dominio, ovvero data un'immagine e un'etichetta fissa come input, il generatore produrrà lo stesso output per ciascun dominio. Ciò dipende principalmente dal fatto che ogni dominio è definito da un'etichetta predeterminata. Questa limitazione è stata risolta con la seconda versione di StarGAN chiamata *StarGAN-v2*[24].

He et al.[59], hanno proposto una nuova tecnica chiamata *AttGAN* in cui viene applicato un vincolo di classificazione degli attributi all'immagine generata, al fine di garantire solo le corrette modifiche degli attributi desiderati. I risultati ottenuti hanno mostrato come *AttGAN* supera lo stato dell'arte sulla modifica realistica degli attributi facciali.

Infine, le migliori tecniche di sintesi dell'intero volto sono StyleGAN[10] e StyleGAN2[21] con esempi disponibili nella pagina web *this person does not exist*[11]. Gli autori di StyleGAN hanno proposto un generatore diverso rispetto agli standard motori GAN mediante la mappatura di punti nello spazio latente ad uno spazio latente intermedio che controlla l'output di stile in ogni punto del processo di creazione. Pertanto, StyleGAN è in grado non solo di generare foto di volti incredibilmente realistiche e di alta qualità, ma offre anche parametri di controllo in termini di stile complessivo dell'immagine generata a diversi livelli di dettaglio. Piccole anomalie potrebbero rivelare la falsità delle immagini generate. Per correggere quelle imperfezioni, Karras et al.

[59] Z. He et al., *AttGAN: Facial Attribute Editing by Only Changing What you Want.* IEEE Transactions on Image Processing 28.11 (2019): 5464-5478.

hanno apportato alcuni miglioramenti al generatore di StyleGAN proponendo StyleGAN2[21].

2.2. *Metodi di Detection di Deepfake*

I metodi esistenti di rilevamento di Deepfake risolvono un compito di classificazione binaria, ovvero stabiliscono solo se un contenuto multimediale è *Reale* oppure *Deepfake*.

Le immagini generate dalle architetture GAN risultano essere molto complicate da classificare, poiché questi framework riescono a produrre immagini sintetiche molto realistiche e di alta qualità. Esistono diversi algoritmi di rilevamento dei Deepfake in letteratura. Tuttavia, la maggior parte dei lavori sono considerati privi di generalizzazione poiché funzionano molto bene solo con dati con cui sono stati allenati. Questa caratteristica risulta essere un limite cruciale di queste tecniche a causa dello sviluppo sempre più rapido di nuove architetture generative.

In generale, per le immagini sintetiche, le attuali tecniche di rilevamento mirano a identificare quelle anomalie introdotte nel processo generativo che sono spesso presenti sullo sfondo[60,61]. Altri metodi invece cercano di estrarre l'impronta lasciata dal modello generativo[62,63,64,65].

Per i video sintetici, invece, vengono analizzati anche i cosiddetti artefatti temporali. Ad esempio, le tecniche di rievocazione del volto potrebbero portare ad anomalie nella sincronizzazione dei fotogrammi video[66,67]non presenti comunemente in dati multimediali reali.

[60] S. McCloskey and M. Albright, *Detecting GAN-generated Imagery Using Color Cues*. arXiv preprint arXiv:1812.08247, 2018.

[61] X. Li et al., *Fighting Against Deepfake: Patch&Pair Convolutional Neural Networks* (PPCNN). Companion Proceedings of the Web Conference, pp. 88-89, 2020.

[62] N. Yu et al., *Attributing Fake Images to GANs: Learning and Analyzing GAN Fingerprints.* Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 7556-7566, 2019.

[63] L. Guarnera, O. Giudice, S. Battiato, *Deepfake Detection by Analyzing Convolutional Traces.* Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, pp. 666-667, 2020.

[64] L. Guarnera, O. Giudice, S. Battiato, *Fighting Deepfake by Exposing the Convolutional Traces on Images*. IEEE Access 8 (2020): 165085-165098.

[65] O. Giudice, L. Guarnera, S. Battiato, *Fighting Deepfakes by Detecting GAN DCT Anomalies.* J. Imaging 2021, 7, 128. https://doi.org/10.3390/jimaging7080128.

[66] D. Güera, et al., *We Need No Pixels: Video Manipulation Detection Using Stream Descriptors*. arXiv preprint arXiv:1906.08743, 2019.

[67] I. Amerini et al., *Deepfake Video Detection through Optical Flow Based CNN*. Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops. 2019.

Diversi metodi allo stato dell'arte utilizzano approcci basati sul Deep Learning per cercare di distinguere i dati sintetici dai dati reali.

Li et al.[68] hanno ottenuto buoni risultati di classificazione utilizzando diverse architetture neurali profonde addestrate tramite particolari punti di riferimento facciali estratti con DLIB[69]. Una tecnica molto interessante è stata proposta da Li et al.[70] in cui hanno utilizzato un'architettura di Deep Learning per analizzare la mancanza di battiti di ciglia nei fotogrammi video dei volti sintetizzati. Un limite di questa tecnica è che non riesce a rilevare i volti manipolati con gli occhi chiusi. Le tecniche di creazione di Deepfake si stanno evolvendo molto rapidamente creando video sintetici con battito di ciglia simili ai video reali. In quest'ultimo scenario, quest'ultimo metodo non sarà più in grado di distinguere i video reali dai Deepfake.

Approcci di Deep Learning sono stati impiegati per classificare le immagini Deepfake.

Un lavoro interessante è stato proposto da Agarwal et al.[71] in cui cercano di identificare le manipolazioni di scambio di volti tramite un framework in grado di calcolare due caratteristiche biometriche: la biometria facciale (estratta tramite l'architettura di deep learning) e la biometria comportamentale (estratta tramite una rete di codificatori-decodifica). La combinazione di queste caratteristiche ha permesso l'identificazione di manipolazioni di scambio di volti.

Ottimi risultati sono stati ottenuti da quelle tecniche in grado di estrarre informazioni riguardanti segnali biologici come nel lavoro proposto da Fernandes et al.[72] in cui è stata calcolata la frequenza cardiaca combinando la variazione del colore della pelle, l'intensità ottica media e l'ingrandimento euleriano del video. Gli autori hanno addestrato un modello di equazioni differenziali ordinarie neurali con questa funzione per il compito di classificazione Deepfake.

[68] Y. Li, S. Lyu, *Exposing Deepfake Videos by Detecting Face Warping Artifacts.* arXiv preprint arXiv:1811.00656, 2018.

[69] D.E. King, *Dlib-ml: A Machine Learning Toolkit.* The Journal of Machine Learning Research 10, 2009, pp.1755-1758.

[70] Y. Li, et al., *In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking*. 2018 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2018.

[71] S. Agarwal et al., *Detecting Deep-Fake Videos from Appearance and Behavior*. 2020 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2020.

[72] S. Fernandes et al., *Predicting Heart Rate Variations of Deepfake Videos Using Neural ODE.* Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops. 2019.

Alcuni modelli generativi non sono in grado di creare tutti gli elementi essenziali per ottenere immagini sintetiche che risultino autentiche all'occhio umano. Spesso, infatti, mancano i riflessi; sono presenti diversi colori degli occhi; sono presenti artefatti nei denti; orecchie di forma diversa e altro ancora. Sfruttando queste informazioni, Matern et al.[73] hanno addestrato due classificatori estraendo caratteristiche in grado di descrivere queste anomalie. Un limite di questa tecnica è che funziona solo nel caso in cui si considerino volti sintetici con occhi aperti o denti visibili.

Alcune tecniche di rilevamento di Deepfake utilizzano approcci "artigianali/tradizionali" per il task di classificazione, ovvero approcci non basati su architetture come le Reti Neurali. Ad esempio, nel lavoro proposto da Guarnera et al.[68,69], è stato dimostrato che la correlazione dei pixel nelle immagini Deepfake risulta essere differente rispetto a immagini reali acquisite da comuni dispositivi. Questa caratteristica ha consentito la creazione di un classificatore robusto in grado di distinguere immagini reali da immagini Deepfake con un alto livello di classificazione. Il metodo riesce anche a identificare le immagini manipolate con FaceApp[31] come Deepfake.

Le immagini Deepfake contengono delle statistiche frequenziali differenti rispetto a immagini reali[33]. Queste possono essere estratte e considerate come impronte digitali uniche lasciate dai singoli motori GAN. Recentemente, Giudice et al.[70] hanno proposto una nuova pipeline in grado di rilevare le cosiddette *GAN Specific Frequencies* (GSF), ovvero quelle frequenze che caratterizzando le immagini Deepfake le quali definiscono un'impronta digitale unica di diverse architetture generative. Utilizzando la Trasformata Discreta del Coseno (DCT – *Discrete Cosine Transform*), sono state rilevate queste frequenze anomale. Le statistiche desunte dalla distribuzione dei coefficienti estratti dalla DCT sono risultate essere fondamentali per riconoscere i dati generati dal motore GAN. I test di robustezza effettuati attaccando le immagini tramite operazioni di compressione, mirroring, rotazione, ridimensionamento e aggiunta di rettangoli di dimensioni e colori casuali hanno ulteriormente dimostrato l'efficacia del metodo proposto dagli autori.

[73] F. Matern, C. Riess, M. Stamminger, *Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations*. 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW). IEEE, 2019.

Inoltre, non solo sono stati ottenuti dei risultati di classificazione superiori rispetto quanto presente nella letteratura, ma il metodo fornisce anche molti spunti in termini di spiegabilità.

Jain et al.[74] hanno proposto un lavoro noto come DAD-HCNN, basato su una pipeline di classificazione gerarchica composta da tre livelli per distinguere rispettivamente immagini reali Vs alterate tramite tool di editing (primo livello), alterate Vs immagini generate da GAN (secondo livello) e, infine, definire l'architettura GAN specifica (terzo livello). Il framework è in grado di rilevare ritocchi e immagini generate da GAN con elevata precisione.

Un set di dati di riferimento è stato introdotto da Rossler et al.[39] come punto di riferimento per il rilevamento di Deepfake. Si chiama FaceForensics++ e si basa principalmente su quattro metodi di manipolazione: due metodi basati sulla grafica computerizzata (Face2Face[27], FaceSwap[26]) e due approcci basati sul Deep Learning (DeepFakes[25], NeuralTextures[28]).
Considerando approssimativamente la letteratura sul campo, sembra che il rilevamento di Deepfake sia un compito facile, già risolto. Tuttavia, le tecniche analitiche basate sul dominio della frequenza mancano ancora di accuratezza e gli algoritmi basati su reti neurali riescono ad ottenere buoni risultati di classificazione ma tendono a discriminare la semantica più delle tracce specifiche delle varie GAN. Inoltre, queste tecniche sono computazionalmente onerose e difficili da comprendere o controllare[14].

3. Discussione e conclusione

La rapida diffusione e la facilità di utilizzo degli strumenti di editing dei media digitali hanno introdotto metodologie per alterare i file multimediali con tecniche sempre più complesse. D'altra parte, la comunità scientifica si è attrezzata di conseguenza sviluppando algoritmi e tecniche altrettanto efficaci in grado di produrre evidenze forensi della eventuale manipolazione. I rapidi progressi nel settore dell'Intelligenza Artificiale tramite l'utilizzo di tecniche di Deep Learning e del loro paradigma generativo hanno innalzato il livello dello scontro con l'introduzione dei cosiddetti Deepfake.

[74] A. Jain et al., *Detecting GANs and Retouching based Digital Alterations via DAD-HCNN*. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. 2020.

I principali motori utilizzati per la creazione di contenuti multimediali sintetici sono gli Autoencoder e Generative Adversarial Network. Queste tecnologie consentono di manipolare volti di persone modificando il colore dei capelli, il genere o persino creare una persona che non esiste nel mondo reale.

Gli attacchi Deepfake di tipo *Spear Phishing*, *CEO Fraud* e *Phishing* possono riguardare anche piccole e grandi realtà aziendali. Rispetto alle tradizionali tecniche di manipolazioni di immagini, un attaccante, attraverso le piattaforme oggi disponibili per la creazione di Deepfake è in grado di creare contenuti multimediali estremamente realistici al fine di perfezionare i tradizionali attacchi informatici come frodi ed estorsioni online, rubare l'identità digitale delle persone e tanto altro ancora. I Deepfake sono in grado di aggirare sistemi di intelligenza artificiale, come quelli di autenticazione: basti pensare ad esempio ad un sistema di autenticazione basato sul riconoscimento del volto che viene attaccato mostrando un'immagine generata tramite GAN per poter accedere in un'area riservata di un'azienda (es. per azioni tipiche di spionaggio industriale). Altre tipologie di attacchi effettuati tramite questa nuova potente tecnologia sono stati di tipo *Spear Phishing* e di *Whaling*. In particolare, in questo contesto, alcuni attaccanti hanno utilizzato immagini Deepfake per creare due profili falsi della stessa persona su due social network differenti quali *Twitter* e *LinkedIn* di una "presunta" giornalista del quotidiano *Bloomberg* chiamata *Maisy Kinsley*[75]. L'obiettivo dell'attacco era quello di realizzare un'azione di spionaggio industriale tramite l'acquisizione di informazioni riservate, entrando in contatto con 195 venditori della società Tesla. Fortunatamente, in questo caso la testata giornalistica stessa ha confermato su richiesta esplicita della controparte, che non esisteva nel suo team una giornalista di nome Maisy Kinsley rendendo di fatto nullo l'attacco. Un esempio invece in cui l'attacco è stato effettuato con successo riguarda una società inglese, in cui è stato autorizzato un bonifico bancario della cifra pari a 200.000 sterline verso un conto corrente ungherese. In quest'ultimo caso la tecnica Deepfake è stata utilizzata per manipolare in real-time il contenuto audio di una telefonata.

[75] https://www.theregister.com/2019/06/17/roundup_ai/.

Altre potenziali abusi riguardano gli aspetti geo-politici; si pensi ad esempio ad una possibile campagna elettorale, in cui dei contenuti video real-time o meno, anche su una testata giornalistica autorevole, potrebbero veicolare il risultato di un Deepfake.

Il settore di maggiore diffusione riguarda senza timore di smentita il mondo della pornografia. Si parla in questo caso di *DeepNude*, *DeepPorn* o *Porno Deepfake*. In questo contesto, il volto della vittima viene sostituito al volto di un attore in un video porno al fine di divulgare contenuti pornografici mai avvenuti. Sotto questo aspetto alcune applicazioni disponibili nei vari *store* sono state ritirate, poiché consentivano di denudare "virtualmente" l'immagine di una persona sotto attacco. In questi contesti si realizzano dei veri e propri attacchi di tipo *Revenge Porn* anche a partire da una quantità limitata di dati della vittima: basta anche una semplice foto del profilo scaricata dai vari social della vittima.

Giuridicamente risulta essere complicato definire e classificare i reati basati su tecnologie Deepfake. Nel dicembre del 2020 i Deepfake sono stati definiti, in un documento pubblicato dal *Garante privacy*[76], come una forma particolare di furto di identità. L'uso illecito di questa tecnologia può essere ricondotto a due tipi di reati: *frode informatica* e *sostituzione della persona*. Nel contesto del *Revenge Porn*, giuridicamente esistono leggi che puniscono coloro che hanno divulgato immagini e video di natura pornografica senza il consenso della persona protagonista.

È sempre più pressante quindi la necessità di creare soluzioni informatiche sempre più sofisticate al fine di contrastare l'uso illecito di questa potente tecnologia.

La maggior parte degli algoritmi di rilevamento di *forgery* classici, non sono in grado di distinguere i Deepfake dai contenuti reali. Come riportato in letteratura, i dati multimediali contengono un'impronta digitale univoca in grado di identificare il modello del dispositivo utilizzato durante la fase di acquisizione (come smartphone e scanner), il social network su cui sono stati caricati i dati e ricostruire la storia dei dati stessi. Recenti studi hanno dimostrato che anche i contenuti Deepfake hanno un'impronta digitale unica lasciata dai modelli generativi. I ricercatori hanno dimostrato di essere in grado di estrarre questa traccia ottenendo

[76] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9512226#:~:text=I%20deepfake%20sono%20foto%2C%20video,imitare%20fedelmente%20una%20determinata%20voce.

buoni risultati di classificazione nel task *Real Vs Deepfake* e individuando anche l'algoritmo di Deep Learning utilizzato per generarli.

I vari motori GAN disponibili in letteratura utilizzano diverse architetture di generatori e discriminatori (implementati tramite Convolution Neural Network (CNN)) per risolvere diversi compiti (cambiare il colore dei capelli, creare volti di persone che non esistono). Le CNN sono composte da strati convoluzionali e i loro parametri (come la dimensione del kernel e molti altri) caratterizzano i contenuti multimediali sintetici. Risultano essere proprio i layer convoluzionali che lasciano una traccia, la quale può essere rilevata analizzando la correlazione dei pixel dell'immagine[68,69].

Nella continua lotta tra *Forensics* e *anti-Forensics*, con l'avvento delle tecnologie di Intelligenza Artificiale, assistiamo al momento ad uno scontro in cui a modelli generativi sempre più performanti e disruptive, in grado di ingannare l'occhio umano e non solo, si contrappongono tecniche e modelli che ne individuano le tracce nascoste. È chiaro che le competenze e l'esperienza di dominio necessaria per affrontare la sfida deve essere di prim'ordine ma a nostro parere il bravo investigatore digitale può a buon ragione ritenersi ancora ottimista e utilizzare strumenti anch'essi complessi di estrazione, acquisizione e analisi anche nel contesto dei Deepfake.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643020
pp. 387-409 (gennaio 2022)

La nuova Proposta di Regolamento europeo sull'Intelligenza artificiale: questioni giuridiche e approcci regolatori

Giuseppe Contissa[1], Federico Galli[1],
Francesco Godano[1], Galileo Sartor[1]

1. Introduzione

Il presente contributo esamina la recente Proposta di Regolamento sull'Intelligenza artificiale, presentata dalla Commissione europea nell'aprile 2021. La Proposta mira a costruire un quadro normativo dell'Intelligenza artificiale (IA) compatibile con i valori europei e con la tutela dei diritti umani: fornisce una definizione e classificazione dei sistemi di IA, stabilisce una serie di requisiti per la loro realizzazione, commercializzazione e utilizzo, e delinea una serie di strumenti di controllo e sanzione. In questa sede descriveremo i tratti salienti della Proposta, vagliandone gli aspetti innovativi, gli elementi problematici ed i possibili interventi di modifica.

Negli ultimi anni il campo dell'IA ha conosciuto un rapido sviluppo in settori sempre più ampi della vita sociale. Le tecnologie dell'informazione e l'IA stanno trovando crescente applicazione non solo nei distretti ad alta specializzazione tecnologica, ma anche nell'alveo di prodotti e servizi di uso comune, coinvolgendo ampie fasce della popolazione. A fronte degli enormi benefici, molti sono i rischi che tali tecnologie comportano nei confronti di diritti e libertà fondamentali. Si è quindi posta all'attenzione delle istituzioni europee la necessità di fornire una base normativa comune che consideri le implicazioni umane, etiche e socio-economiche dell'IA nel rispetto dei valori europei. Negli ultimi anni è stata avviata una serie di iniziative per elaborare i

[1] CIRSFID – Alma Human Artificial Intelligence, Università di Bologna.

contenuti di tale legislazione, nel contesto di un più generale programma che coinvolge la regolazione della gestione dei dati, del mercato digitale e della robotica[2].

I primi documenti in cui si solleva la necessità di intraprendere questo percorso risalgono al 2017[3]. Nell'aprile del 2018, la Commissione ha presentato una "strategia europea" in tema di IA, orientata su tre direttrici: (1) la promozione della ricerca, dello sviluppo tecnologico e delle applicazioni industriali legate all'IA; (2) il sostegno all'apparato socio-economico interessato da tali sviluppi tecnologici; (3) infine, la definizione di "un quadro etico e giuridico adeguato, basato sui valori dell'Unione e coerente con la Carta dei diritti fondamentali dell'UE"[4].

Parallelamente, la Commissione ha istituito un "Gruppo di esperti ad alto livello" sull'IA, il quale ha pubblicato, nell'aprile 2019, gli *Orientamenti etici per un'Intelligenza artificiale affidabile*[5]. Il documento individua tre principi fondamentali per un'IA che possa considerarsi "degna di fiducia" (*trustworthy*): legalità, eticità, robustezza tecnica e sociale. Su queste basi, il Gruppo di esperti ha individuato i requisiti che un sistema di IA dovrebbe presentare[6]: (1) intervento e sorveglianza umani; (2) robustezza tecnica e sicurezza; (3) riservatezza e

[2] Di recente emanazione sono: Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), 15 dicembre 2020, COM(2020) 842 final (Digital Markets Act); Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, 15 dicembre 2020, COM(2020) 825 final (Digital Services Act); Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati), 25 novembre 2020, COM(2020) 767 final (Data Governance Act).

[3] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, 2015/2103(INL).

[4] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale Europeo e al Comitato delle regioni. L'Intelligenza artificiale per l'Europa, 25 aprile 2018, COM(2018) 237 final, pp. 3-4. Oltre alla Carta dei diritti, la Commissione si riferisce all'articolo 2 del TUE per la definizione dei valori fondamentali dell'Unione.

[5] Gruppo di esperti ad alto livello sull'Intelligenza artificiale, Orientamenti etici per un'IA affidabile, 8 aprile 2019.

[6] Le linee guida contengono inoltre una "lista di controllo" per la valutazione dell'operatività di tali requisiti da parte delle aziende. Durante la seconda metà del 2019, oltre 350 organizzazioni hanno sottoposto i propri prodotti e servizi di IA al vaglio di questa lista: sulla base dei riscontri ricevuti è emerso che, mentre un certo numero di requisiti si riflette già nei regimi normativi esistenti, quelli riguardanti la trasparenza, la tracciabilità e la supervisione umana non sono specificamente coperti dalla legislazione vigente in molti settori economici.

governance dei dati; (4) trasparenza; (5) diversità, non discriminazione ed equità; (6) benessere sociale e ambientale; (7) accountability.

Sulla scorta di tali indicazioni, nel febbraio 2020 la Commissione europea ha pubblicato il *Libro bianco sull'Intelligenza artificiale*[7]. Il documento articola in modo dettagliato le opzioni strategiche definite nel 2018, affiancando all'obiettivo di una tecnologia "degna di fiducia" la promozione della "eccellenza" europea nel settore della ricerca e dell'industria. Per quanto riguarda l'ambito giuridico, il Libro bianco definisce come prioritari gli interventi in tema di diritti fondamentali e governance dei dati, di sicurezza e responsabilità, di armonizzazione ed effettività della legislazione.

Dal canto suo, il Parlamento europeo ha anch'esso affrontato alcune questioni inerenti alla regolazione dell'IA. In particolare, la Risoluzione sulla responsabilità[8] è rilevante per la definizione di IA e per l'adozione di un approccio normativo basato sul rischio.

Il percorso, qui rapidamente sintetizzato, è culminato nella Proposta di emanazione di un Regolamento Europeo, noto come AI Act[9], che predispone un quadro legislativo organico per lo sviluppo e l'utilizzo dell'IA.

2. La Proposta di Regolamento: caratteri essenziali e ambito di applicazione

Andiamo ora ad esaminare la struttura e gli elementi principali della Proposta. Il documento è articolato in 12 titoli comprensivi di 85 articoli, ed è corredato da 9 allegati tecnici.

La prima parte della Proposta è contenuta nel titolo I, che definisce l'oggetto e il campo di applicazione del Regolamento. Le nuove norme sono dirette: (1) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA all'interno dell'Unione; (2) agli utenti di sistemi di IA situati nell'Unione; (3) ad utenti e fornitori di sistemi situati in un

[7] Commissione Europea, Libro Bianco sull'Intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia, 19 febbraio 2020, COM/2020/65 final.

[8] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 2020/2014(INL).

[9] Commissione Europea, Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (AI Act), 21 aprile 2021, COM/2021/206 final.

paese terzo, quando "l'output prodotto dal sistema sia utilizzato nell'Unione" (art. 2).

L'art. 3 contiene le definizioni dei termini usati nel documento. Di primaria importanza è la definizione di "sistema di intelligenza artificiale", di cui si discuterà più avanti (sezione 3). In tema, è opportuno però sin da subito segnalare l'utilizzo da parte della Proposta del termine "utente". Con questa dizione, ci si riferisce a "qualsiasi persona fisica o giuridica […] che utilizza un sistema di IA sotto la sua autorità": la nozione differisce dunque da quella comune di "utilizzatore finale" del sistema (v. sezione 6).

La seconda parte della Proposta (titoli II-IV) contiene la disciplina delle diverse categorie di sistemi di IA individuate dal legislatore europeo. La classificazione prescelta segue un approccio cd. *risk-based*, fondato sul livello di rischio che i caratteri o l'uso di tali tecnologie comportano. Si individuano in tal modo i sistemi che comportano (i) un rischio inaccettabile, (ii) un rischio alto, e (iii) un rischio medio o basso.

Nel titolo II sono disciplinate le "pratiche" – ossia gli utilizzi o gli effetti dell'IA – considerate proibite nell'ordinamento comunitario, in ragione del loro patente contrasto con i valori o i diritti fondamentali dell'Unione (art. 5). Il divieto riguarda le pratiche di manipolazione, *social scoring* e identificazione biometrica. Ci soffermeremo su ognuna di queste pratiche nella sezione 4.

Il titolo III contiene la regolamentazione dei sistemi di IA che creano un rischio elevato per la salute e la sicurezza o i diritti fondamentali delle persone. Questi sistemi, di cui parleremo nella sezione 5, sono ammessi nell'ordinamento dell'Unione nella misura in cui soddisfino determinati requisiti e siano sottoposti ad una valutazione di conformità preliminare alla loro immissione sul mercato o messa in servizio (di quest'ultima tratteremo nella sezione 7).

Il titolo IV della Proposta dispone alcuni obblighi di trasparenza – ulteriori rispetto a quelli previsti per i sistemi ad alto rischio – in capo a determinati sistemi di IA che presentano specifici rischi legati all'interazione fra uomo e macchina, e che sono generalmente (ma non necessariamente) riconducibili alla categoria dei sistemi "a medio rischio". In tali casi, si prevede che chi utilizza il sistema debba essere informato del fatto che sta interagendo con un'IA. Ne discuteremo nella sezione 6.

La terza parte della Proposta (titoli V-XII) contiene la normativa sulla governance e sul controllo dei sistemi di IA, insieme alle regole sull'ese-

cuzione del Regolamento. Di questa parte ci occuperemo, più sinteticamente, nella sezione 7.

Con l'obiettivo di creare un quadro giuridico favorevole all'innovazione, il titolo V promuove la creazione di "ambienti normativi controllati" (*normative sandboxes*) per la sperimentazione tecnologica. Il titolo VI disciplina gli organismi di governo del sistema-mercato di IA a livello dell'Unione e degli Stati membri. Il titolo VII mira ad agevolare le funzioni di governance attraverso la creazione di una banca dati europea per i sistemi di IA ad alto rischio. Vengono poi disciplinati (titolo VII) il monitoraggio dei sistemi successivo all'immissione sul mercato, gli obblighi informativi e la vigilanza del mercato. Nel titolo IX si fornisce una serie di regole relative alla creazione di codici di condotta per i fornitori di sistemi di IA non ad alto rischio.

Gli ultimi titoli contengono norme di carattere generale relative all'esecuzione del futuro Regolamento: l'obbligo di riservatezza nella gestione delle informazioni, disposto in capo alle autorità pubbliche (titolo X); le norme relative al potere di adottare atti delegati (titolo XI); gli obblighi per la Commissione di valutare regolarmente la necessità di aggiornamenti e di preparare relazioni periodiche sulla valutazione e la revisione del Regolamento (titolo XII). Entriamo ora nel dettaglio delle norme.

3. Definizione di Intelligenza artificiale

La definizione di Intelligenza artificiale inclusa nella Proposta all'art. 3, n. 1 è composta da due parti. La prima, funzionale, intende essere più ampia possibile ed include il software che "può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono".

La seconda è costituita da un elenco nell'Allegato I di tecniche utilizzate in sistemi di IA: apprendimento automatico (supervisionato e non, per rinforzo), approcci basati su logica e conoscenza (come i sistemi esperti), e approcci statistici (stima bayesiana, ricerca e ottimizzazione)[10].

[10] Nell'articolo 4 della Proposta si stabilisce l'uso di atti delegati per modificare l'elenco delle tecniche e degli approcci definiti nell'allegato I per mantenere l'elenco aggiornato agli sviluppi futuri del mercato e delle tecnologie.

Le due definizioni tendono evidentemente in direzioni diverse. La prima, più in linea con il modello *risk-based*, è neutrale rispetto alla tecnologia e guarda alla possibile influenza del sistema sul mondo. Al contrario, l'elenco dell'Allegato I mira a restringere il cerchio di applicazione a tecnologie specifiche, per dare maggiore certezza ai produttori e utilizzatori di sistemi di IA.

Il riferimento ai tre approcci di IA potrebbe condurre a una interpretazione molto ampia, tale da coprire tecnologie che normalmente non sono considerate di IA. In particolare, il riferimento a modelli logici e statistici rischia di estendere molto il campo di applicazione del Regolamento, che classificherebbe (erroneamente) come sistemi di IA la grande maggioranza di software esistenti[11]. Non è chiaro se le considerazioni del Regolamento si possano applicare allo stesso modo a un programma basato su regole risalente a quindici anni fa e a un complesso sistema di apprendimento automatico sviluppato oggi[12]. Verrebbe da chiedersi come mai non focalizzare la Proposta sulle decisioni algoritmiche – l'oggetto che si intende regolare – con un approccio *risk-based*, e tecnologicamente neutrale. Il rischio è quello di generare grande incertezza, anche tra gli operatori del mercato, al momento di determinare se un certo sistema di IA adotti o meno le tecniche definite nell'Allegato I.

D'altro canto, se interpretata in senso stretto, la definizione di IA potrebbe finire per escludere alcune applicazioni di sistemi automatizzati che, sebbene sviluppati attraverso metodi tradizionali (come la programmazione procedurale) e completamente deterministici, presentano un alto grado di rischio, specialmente quando progettati per essere indipendenti dall'intervento/supervisione umana. In questa categoria *extra* potremmo includere sistemi come Frank[13], che assegnava le prenotazioni ai *rider* di Deliveroo, e il sistema Parcoursup

[11] P. GLAUNER, *An Assessment of the AI Regulation Proposed by the European Commission*, arXiv preprint:2105.15133, 2021; V. DIGNUM, *Responsible artificial intelligence: how to develop and use AI in a responsible way*, Springer Nature, 2019.

[12] La circostanza è stata rilevata anche da Barry O´Sullivan, membro del Gruppo di esperti ad alto livello sull'Intelligenza artificiale. Si veda il suo intervento accessibile online: https://www.youtube.com/watch?v=X9h8MZIuvKg.

[13] F. GALLI, F. GODANO, *Il rapporto di lavoro dei riders e la natura discriminatoria delle condizioni di accesso al lavoro dell'algoritmo frank*, Diritto di Internet, III, 2021, pp. 275–288.

per l'iscrizione all'università usato in Francia[14][15]. Entrambi questi sistemi si basavano su complesse forme di automazione, non riconducibili alle tecniche di IA previste dalla Proposta.

Vale la pena ricordare che nella già citata risoluzione del Parlamento europeo sulla responsabilità civile per l'IA è stata adottata una definizione molto più generica e astratta, ovvero "un sistema che è basato su software o incorporato in dispositivi hardware, e che mostra un comportamento che simula l'intelligenza, tra l'altro, raccogliendo ed elaborando dati, analizzando e interpretando il suo ambiente, e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici".

4. Le pratiche proibite

Il Titolo II, contenente il solo art. 5, stabilisce quattro pratiche proibite che costituiscono il più elevato livello di rischio connesso a sistemi di IA. Per queste pratiche, la Proposta pone un divieto generalizzato, salvo ammettere eccezioni in casi specifici.

4.1. *Manipolazione*

L'art. 5 (1), lett. a, riguarda le pratiche manipolative svolte attraverso sistemi di IA. In particolare, esso proibisce "l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico".

La formulazione del divieto lascia aperte alcune importanti questioni. Il significato dell'espressione "tecniche subliminali" non è chiaro, né appare comprensibile il significato di "consapevolezza" in

[14] A. Bibal, M. Lognoul, A. De Streel, B. Frénay, *Legal requirements on explainability in machine learning*, Artificial Intelligence and Law, 29 (2021), pp. 149–169.

[15] Si è discusso come il sistema abbia avuto un profondo impatto sulla vita degli studenti, determinando quali posti di laurea sarebbero disponibili per loro dopo la scuola superiore. Il funzionamento del sistema non è mai stato reso pubblico, ma sembra che non siano state utilizzate né tecniche statistiche, né di apprendimento automatico, né basate sulla conoscenza, bensì una combinazione di più metodi.

relazione alle pratiche che opererebbero "senza" di essa. La versione del testo in inglese utilizza il termine "consciousness", che sembra conferire al divieto un significato metagiuridico. Ci si potrebbe chiedere se, alla luce di questa vaga terminologia, possano essere ricomprese tecniche quali l'utilizzo delle architetture digitali per indurre certi comportamenti nocivi negli utenti (*dark pattern*)[16], o le raccomandazioni personalizzate e adattive che possono condurre l'individuo a scelte irrazionali ed impulsive (c.d. *hypernudging*)[17].

Relativamente al risultato della manipolazione, le tipologie di danno riferite nel divieto non sono chiare. Mentre il danno fisico in teoria è facile da identificare, appare più difficile immaginare casi in cui il danno fisico sia provocato da sistemi di IA usati in senso manipolativo[18]. Viceversa, gli scenari in cui potrebbero verificarsi danni psicologici appaiono più verosimili considerato il crescente utilizzo di sistemi intelligenti capaci di riconoscere gli stati emotivi degli individui[19] e la capacità di influire su di essi[20]. Tuttavia, in assenza di chiari indici di misurazione, risulta difficile identificare il danno psicologico, vista la sua intrinseca soggettività. Occorre, infine, segnalare l'esclusione dei danni economici e dei pregiudizi di carattere sociale, scelta che escluderebbe molte pratiche di IA ritenute rischiose (ad es., sistemi per la pubblicità mirata o sistemi di raccomandazione)[21].

Il rischio è che, sebbene lodevole nel suo obiettivo, il divieto di manipolazione rimanga una dichiarazione di intenti. Ci si augura che il

[16] LUGURI, L. STRAHILEVITZ, *Shining a light on dark patterns*, University of Chicago, Public Law Working Paper, 2019.

[17] K. YEUNG, *'Hypernudge': Big Data as a mode of regulation by design*, Information, Communication &; Society, 20, 2017, pp. 118-136.

[18] La Commissione ha presentato solo un esempio piuttosto inverosimile: "[un] suono impercettibile [riprodotto] nelle cabine dei camionisti per spingerli a guidare più a lungo di quanto sia sano e sicuro [dove] l'IA è usata per trovare la frequenza che massimizza questo effetto sui conducenti". Vedi, Gabriele Mazzini (DG CONNECT), 'A European Strategy for Artificial Intelligence' (2nd ELLIS Workshop in Human-Centric Machine Learning (YouTube recording), 10 Maggio 2021) https://youtu.be/OZtuVKW qhl0?t=10346.

[19] C. BURR, N. CRISTIANINI, *Can Machines Read our Minds?*, Minds and Machines, (2019), pp. 1-34.

[20] S. C. MATZ, M. KOSINSKI, G. NAVE, D. J. STILLWELL, *Psychological targeting as an effective approach to digital mass persuasion*, Proceedings of the National Academy of Sciences, 114, 2017, pp. 12714-12719.

[21] Ci sembra importante menzionare che, in caso di danno economico, si applica comunque la Direttiva 2005/29/CE sulle pratiche commerciali scorrette.

legislatore specifichi quali pratiche o tecniche siano da considerare effettivamente pericolose per l'autonomia degli individui. Per esempio, ci si potrebbe aspettare un divieto dell'utilizzo di certe tecniche di apprendimento automatico (come il *reinforcement learning*) in contesti di più facile dipendenza come i videogames o i social network; oppure, si potrebbe vietare l'uso di alcune categorie di dati sensibili in grado di influenzare i comportamenti (ad es. dati biometrici in contesti di marketing, informazioni sulle opinioni politiche nei social network).

4.2. *Sfruttamento di vulnerabilità*

La seconda pratica proibita consiste nell'uso di un sistema «che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico» (art. 5, lett. b).

Pur essendo apprezzabile l'attenzione ai gruppi più deboli, non è chiaro quale sia l'effettivo valore aggiunto di questa disposizione rispetto alla precedente. In particolare, non viene dato alcun indizio sul significato di "sfruttamento". Si potrebbe pensare che esso sia diverso dalla manipolazione, e che l'uso delle informazioni possa qualificare alcune persone fisiche come vulnerabili: per esempio, un sistema che utilizza le informazioni sull'età di una persona al fine di promuovere l'acquisto di articoli per bambini sembra essere coperto dalla disposizione.

Il legislatore comunitario adotta un approccio tradizionale al concetto di vulnerabilità, ricomprendendo caratteri come l'età e la disabilità fisica o mentale. Non è chiaro perché altri tipi di vulnerabilità non siano presi in considerazione nella Proposta (ad es. vulnerabilità di tipo finanziario). Peraltro, le vulnerabilità possono dipendere non solamente dalle caratteristiche degli individui, ma anche da fattori esterni e transitori. Una tale accezione della vulnerabilità sarebbe giustificata nei contesti di IA basata sui dati (ad es., nel marketing), dove gli individui sono raggruppati in tempo reale sulla base dei loro comportamenti e stati emotivi[22].

[22] Su una nozione più elastica di vulnerabilità digitale, si veda BEUC, *EU Consumer protection 2.0. Structural asymmetries in digital consumer market*, Report, March 2021.

4.3. *Social scoring*

Il terzo divieto riguarda i sistemi di IA finalizzati al cd. *social scoring,* ossia la valutazione e la classificazione dell'affidabilità delle persone fisiche sulla base del loro comportamento in determinati contesti sociali o di altre caratteristiche personali. La norma (art. 5, lett. c) proibisce la vendita di tali sistemi e il loro utilizzo *da parte dell'autorità pubblica* (o di altri soggetti per conto di essa), quando tale "punteggio sociale" comporti un trattamento pregiudizievole o sfavorevole per individui o gruppi di persone fisiche, in due casi: 1) l'effetto dannoso si verifica in contesti sociali diversi da quelli in cui i dati utilizzati dal sistema sono stati originariamente generati o raccolti; oppure 2) il danno è ingiustificato o sproporzionato rispetto al comportamento sociale o alla sua gravità.

La proibizione appare chiaramente ispirata all'intento di opporsi ai sistemi di *social scoring* diffusi in varia misura nei paesi asiatici tecnologicamente avanzati, ed in particolare in Cina[23]. Il timore della deriva cinese sembra però aver distolto l'attenzione del legislatore dall'utilizzo di tali sistemi *da parte dei privati*, che in Europa risulta peraltro più frequente. Questa lacuna è problematica considerato che anche lo *scoring* privato può avere un impatto significativo sui diritti fondamentali e i principi democratici di base: si pensi all'accesso a servizi essenziali come la fornitura di gas e acqua, oppure ai servizi di credito o assicurativi.

Occorre inoltre segnalare la dubbia opportunità dei due requisiti, e cioè quello di integrità contestuale dei dati e della proporzionalità del pregiudizio. Il primo ammette che l'impiego del *social score* sia sempre legittimo se i dati utilizzati dal sistema sono raccolti in un contesto collegato al punteggio sociale. Il secondo, invece, sembra lasciar aperto un ampio margine di discrezionalità nel definire quando il danno è proporzionale rispetto al comportamento sociale.

[23] Com'è noto buona parte della vita sociale in Cina è regolata da questo sistema. Si pensi ai meccanismi di valutazione e sanzione sociale delle infrazioni stradali.

4.4. *Identificazione biometrica a distanza e in tempo reale*

L'ultima pratica vietata (art. 5(1) lett. d, (2), (3), e (4)) riguarda l'immissione sul mercato, la messa in servizio e l'uso di "sistemi di identificazione biometrica a distanza in tempo reale in spazi accessibili al pubblico a fini di contrasto"[24]. Come regola generale, questi sistemi sono vietati. Tuttavia, sono previste molteplici eccezioni, tra cui l'uso per (i) la ricerca mirata di specifiche vittime potenziali di reato, compresi i bambini scomparsi; (ii) la prevenzione di una minaccia specifica, sostanziale e imminente alla vita o all'incolumità delle persone fisiche o di un attentato terroristico; (iii) l'individuazione, la localizzazione, l'identificazione o il perseguimento dell'autore o del sospettato di una serie di reati specifici[25].

Nei casi menzionati sopra, l'adozione di sistemi di identificazione biometrica a distanza in tempo reale richiede il rispetto di alcune garanzie procedurali. Queste consistono, da un lato, nella valutazione dei presupposti per l'uso di tali tecnologie, e delle potenziali conseguenze per i diritti e per le libertà; dall'altro, nelle limitazioni temporali, geografiche e personali. In ogni caso, si richiede un'autorizzazione preventiva dell'autorità giudiziaria o di un'autorità amministrativa indipendente dello Stato membro. Tale autorizzazione, tuttavia, "in una situazione di urgenza debitamente giustificata" può essere richiesta anche durante o dopo l'uso. L'autorità può concedere l'autorizzazione solo se, sulla base di prove oggettive o di chiare indicazioni, l'uso del sistema in questione è necessario e proporzionato al raggiungimento di uno degli obiettivi consentiti dalla Proposta[26]. Infine, gli Stati membri restano liberi di prevedere la possibilità di autorizzare in via generale l'identificazione biometrica, sempre nei limiti e alle condizioni di cui ai paragrafi 1, lett. d), 2 e 3.

[24] Tali sistemi sono definiti al punto 37 dell'articolo 3 come sistemi «in cui la cattura dei dati biometrici, il confronto e l'identificazione avvengono senza un ritardo significativo». La definizione è intesa a coprire non solo l'identificazione istantanea, ma anche quella effettuata a breve distanza di tempo; altri tipi di identificazione biometrica sono considerati come "sistema di identificazione biometrica a distanza".

[25] Si fa riferimento ai reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio e punibile nello Stato membro interessato con una pena o una misura di sicurezza privative della libertà della durata massima di almeno tre anni, come stabilito dal diritto di tale Stato membro.

[26] Il paragrafo 4 impone agli Stati membri di stabilire nel diritto nazionale norme dettagliate per la richiesta, il rilascio e l'esercizio, nonché il controllo relativo alle autorizzazioni di tali usi.

Considerato il rischio elevato che questa tecnologia comporta per gli individui, la regolamentazione dettagliata dei sistemi di identificazione biometrica è da accogliere con favore. Tuttavia, la portata della disposizione appare troppo ristretta, e le sue eccezioni troppo vaghe.

La proibizione dei sistemi biometrici si applica solo alla "identificazione" delle persone fisiche. Il termine non è sempre efficace per descrivere i caratteri di tali tecnologie: molti dei sistemi che utilizzano dati biometrici (ad es., il movimento degli occhi e delle labbra, la frequenza cardiaca, la conduttanza cutanea, ecc.) non sono finalizzati all'identificazione dell'individuo, ma alla categorizzazione secondo classi o metriche predefinite e per valutare il loro comportamento, che può essere considerato pericoloso o indesiderabile.

Inoltre, il perimetro delle eccezioni al divieto di utilizzo di sistemi biometrici dovrebbe essere oggetto di una ponderata riflessione nel percorso di approvazione del Regolamento. La formulazione attuale è molto ampia, e con ogni probabilità causerà grossi dubbi interpretativi e problemi pratici nei tribunali prima di arrivare ad un accettabile grado di chiarezza.

5. Sistemi IA ad alto rischio: metodologia e obblighi

5.1. *Metodologia per definire i sistemi di IA ad alto rischio*

I sistemi ad alto rischio sono definiti nella Proposta di Regolamento come sistemi che «creano un rischio elevato per la salute e la sicurezza o i diritti fondamentali delle persone fisiche». Il loro uso è regolato da una serie di requisiti e una valutazione di conformità *ex ante*. La definizione può comprendere categorie di IA presenti anche nelle pratiche proibite, a seconda dell'uso.

Come per la definizione di IA, la determinazione dell'alto rischio si compone di due parti. Prima di tutto, un sistema è considerato ad alto rischio se costituisce un componente di sicurezza di un prodotto regolato da una delle normative di armonizzazione dell'Unione Europea (New Legislative Framework, NFL): le normative sono elencate nell'allegato II, e comprendono tra gli altri la direttiva 2009/48/CE sulla sicurezza dei giocattoli e il Regolamento (UE) 2017/745 sui dispositivi medici. Il Regolamento non si applicherebbe invece alle normative del così detto "vecchio approccio", ossia non ricomprese nel NLF: tuttavia

i requisiti per i sistemi di IA ad alto rischio dovranno essere presi in considerazione al momento dell'adozione di nuove norme in materia. Di questa ultima categoria fanno parte il Regolamento (UE) 2018/858 sull'aviazione civile e il Regolamento (UE) n. 168/2013 sui veicoli a motore.

A questa definizione si aggiunge un elenco contenuto nell'Allegato III, che include otto macro-aree in cui i sistemi di IA utilizzati si presumono di alto rischio. Tra queste troviamo l'identificazione biometrica, l'accesso a servizi pubblici e privati, attività di contrasto e amministrazione della giustizia.

Di particolare interesse nell'ambito della giustizia penale sono i sistemi descritti nella categoria *attività di contrasto* (Allegato III, n. 6, let. d): «sistemi di IA destinati a essere utilizzati dalle autorità di contrasto [...] per la valutazione dell'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati», «per individuare i deep-fake», «per la profilazione delle persone fisiche», e «per l'analisi criminale riguardo alle persone fisiche, che consentono alle autorità di contrasto di eseguire ricerche in set di dati complessi, correlati e non correlati, resi disponibili da fonti di dati diverse o in formati diversi, al fine di individuare modelli sconosciuti o scoprire relazioni nascoste nei dati».

Con questa definizione, la Proposta di Regolamento non sembra seguire un approccio *risk-based*: seleziona invece aree di mercato nelle quali l'uso di sistemi di IA implica presumibilmente un alto livello di rischio per i diritti e le libertà fondamentali degli individui. Ci si sarebbe invece aspettati un modello più simile all'istituto della valutazione di impatto sulla protezione dei dati contenuta nel GDPR, che include l'analisi di trattamenti valutativi o di scoring, di monitoraggio sistematico, combinazione di dati derivanti da trattamenti con finalità diverse, e così via[27].

[27] Gruppo Art. 29, *Guidelines on Data Protection Impact Assessment (DPI A) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 (As last Revised and Adopted on 4 October 2017),* European Commission, 2017.

5.2. *Governance dei dati*

La Proposta di Regolamento delinea poi i requisiti essenziali (Capo 2) che si ricollegano agli obblighi dei soggetti previsti nel capo successivo. La grande maggioranza degli obblighi ricade sul "fornitore", il soggetto che sviluppa un sistema IA al fine di immetterlo sul mercato o di metterlo in servizio con il proprio nome o marchio, a titolo oneroso o gratuito (art. 3, n. 3). Tra questi requisiti figurano: un'appropriata governance dei dati (art. 10); la conservazione delle registrazioni (art. 12); la trasparenza e fornitura di informazioni agli utenti (art. 13).

Secondo l'art. 10, i sistemi di IA ad alto rischio basati su tecniche di apprendimento dai dati devono soddisfare criteri di qualità per quanto riguarda l'uso dei dati per l'addestramento (*training set*), per la convalida (*validation set*) e per la prova (*test set*). I dati devono essere pertinenti e rappresentativi, e devono tenere conto delle proprietà specifiche dell'area geografica di applicazione. In modo piuttosto ambizioso, il legislatore UE richiede che i dati siano "esenti da errore" e "completi"; un livello di qualità che potrebbe essere difficile da definire a livello tecnico, vista l'eterogeneità dei sistemi.

Un'ulteriore pratica adeguata di governance dei dati consiste nel monitoraggio, il rilevamento e la correzione delle distorsioni (*bias*). È ormai noto, infatti, come l'utilizzo di sistemi di IA basati sull'apprendimento automatico aumenti il rischio di casi di discriminazione indiretta, anche non intenzionale. Ciò può accadere in molti modi, a seconda di come vengono selezionate le variabili target del modello, le caratteristiche del modello di apprendimento e gli elementi sostitutivi (*proxy*)[28]. Al fine di minimizzare il rischio di esiti discriminatori, la Proposta prevede che un eventuale trattamento di categorie speciali di dati di cui all'art. 9 GDPR possa avvenire in modo legittimo, fatte salve le tutele necessarie per i diritti e le libertà fondamentali delle persone fisiche.

Infine, l'ultimo comma dell'art. 10 richiede l'implementazione di pratiche adeguate di governance dei dati anche per i sistemi di IA ad alto rischio che non si basano sull'addestramento automatico. Quest'ultimo aspetto è apprezzabile, considerato che anche altre tecniche di IA, come ad esempio sistemi esperti, possono condurre a effetti pregiudizievoli per i diritti e le libertà fondamentali.

[28] Barocas, A. D. Selbst, *Big data's disparate impact*, Calif. L. Rev., 104, 2016, p. 671.

5.3. *Trasparenza e spiegabilità*

I sistemi di IA ad alto rischio devono essere progettati in maniera da rendere comprensibile il loro funzionamento a utenti[29] e fornitori, che devono avere chiare istruzioni sul funzionamento e la finalità del sistema[30] (art 13).

Questo uso del termine *trasparenza* differisce dal tipo di trasparenza previsto nel Titolo IV, rivolto agli utilizzatori finali, di cui si parlerà nella sezione 6.

Il requisito si giustifica con l'ampio numero di sistemi di IA, e la relativa facilità con cui un attore nuovo può entrare nel mercato, potendo quindi non possedere conoscenze tecniche adeguate per comprendere appieno queste informazioni. L'art. 13 si concentra sull'interpretabilità dei sistemi di IA da parte dei suoi utenti[31] [32].

Nelle linee guida etiche del Gruppo di esperti sull'Intelligenza artificiale[33] si parlava espressamente del pubblico, e dei requisiti di trasparenza e spiegabilità, a cui si fa cenno nei considerando 69 e 70. Si tratta di elementi fondamentali affinché i cittadini possano capire la motivazione di una decisione algoritmica[34]. Questo approccio è stato perso nella Proposta di Regolamento, e si è prediletto un approccio incentrato sulla trasparenza verso i produttori e fornitori.

5.4. *Supervisione umana*

La Proposta stabilisce che i sistemi ad alto rischio siano sviluppati «con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche» (art. 14).

[29] Si ricorda che gli utenti non sono gli utilizzatori finali, ma coloro che operano il sistema sotto la propria autorità (vedi sezione 2).

[30] R. Chatila, V. Dignum, M. Fisher, F. Giannotti, K. Morik, S. Russell, K. Yeung, *Trustworthy AI*, in *Reflections on Artificial Intelligence for Humanity*, Springer, 2021, pp. 13–39.

[31] G. Sartor, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Study PE 641.530, European Parliamentary Research Service, 2020.

[32] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, D. Pedreschi, *A survey of methods for explaining black box models*, ACM Computing Surveys (CSUR), 51, 2018, pp. 1–42.

[33] Gruppo di esperti ad alto livello sull'Intelligenza artificiale, Orientamenti etici, cit..

[34] M. Brkan, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, International Journal of Law and Information Technology, 27, 2019, pp. 91–121.

La sorveglianza, che mira a prevenire o minimizzare i rischi per la salute, la sicurezza, o i diritti fondamentali (art 14 (2)), deve essere garantita mediante misure individuate dal fornitore, integrate nel sistema, o implementate dall'utente. Tali misure mirano a supportare le azioni indicate al paragrafo 4 dell'art. 14: a) comprendere appieno le capacità e i limiti del sistema di IA ed essere in grado di monitorarne il funzionamento; b) mantenere un atteggiamento consapevole rispetto al rischio di *bias*; c) essere in grado di interpretare correttamente l'output del sistema; d) essere in grado di decidere di non usare il sistema o di ignorare, annullare, o ribaltare il suo output; e) essere in grado di intervenire sul funzionamento del sistema o di interromperlo. Inoltre, l'art. 29 della Proposta, riferito a sistemi di IA ad alto rischio, aggiunge l'obbligo di usare (art. 29 (1)) e monitorare il funzionamento (art. 29 (3)) del sistema, coerentemente con le istruzioni per l'uso.

Queste norme appaiono in linea con i precedenti documenti a livello europeo, come gli Orientamenti etici per un'Intelligenza artificiale affidabile, che promuovono il requisito della sorveglianza umana[35]. Tuttavia, risulta difficile comprendere come il supervisore possa, per tutti i tipi e le applicazioni di IA, esercitare effettivamente le azioni descritte nel paragrafo 4 dell'art. 14, operando una sintesi tra esigenze di tutela tanto ampie e diverse quali sicurezza, salute, diritti umani (che potrebbero richiedere anche una difficile operazione di bilanciamento). In realtà, la possibilità per l'umano di comprendere appieno le capacità e i limiti di sistemi così complessi è ad oggi assai limitata per molte tipologie di IA, e porterebbe di conseguenza, secondo alcuni esperti, a un divieto indiretto di tali sistemi[36].

Come sottolineato da Selbst, l'Intelligenza artificiale (in particolare quella basata su sistemi di apprendimento automatico) è fondamentalmente aliena per un essere umano. Lo scopo stesso di tali sistemi è compiere operazioni secondo modalità in larga parte precluse agli esseri umani[37]. I sistemi di IA spesso, per i compiti che sono loro assegnati,

[35] Gruppo di esperti ad alto livello sull'Intelligenza artificiale, Orientamenti etici, cit. p. 17.

[36] M. Ebers, V. R. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, J, 4, 2021, pp. 589-603.

[37] A. D. Selbst, *Negligence and AI's human users*, BUL Rev., 100, 2020, p. 1315.

sorpassano le capacità degli umani, eccedendone limiti cognitivi e temporali nell'accesso ed elaborazione di informazioni[38].

Questo porta a uno sfasamento tra competenze e responsabilità: i sistemi di IA, adottati per le loro capacità di decisione e previsione superiori rispetto agli esseri umani, sono posti sotto la supervisione degli stessi esseri umani, creando un "compito impossibile"[39].

Il supervisore umano tenderà a fare affidamento sulle decisioni di un sistema di IA[40], tanto più se questo è stato certificato, a meno che non abbia motivi specifici per ritenere che esso sia malfunzionante, o che non sia in grado di incorporare nella sua valutazione ulteriori elementi, esterni al sistema stesso[41].

6. Obblighi di trasparenza per determinati sistemi: i cd. "sistemi di medio rischio"

Il titolo IV comprende il solo articolo 52 e affronta tre specifici sistemi di IA per cui sono previsti alcuni obblighi di trasparenza, con l'obiettivo di contrastare il loro potenziale manipolativo.

In proposito, occorre effettuare qualche precisazione. Innanzitutto, la trasparenza richiesta per questi tipi di IA non coincide con la trasparenza intesa come "spiegabilità" richiesta dall'art. 13 per i sistemi ad alto rischio, di cui si è detto più sopra (sezione 5.3). Ciò che si richiede qui è di rendere noto all'utilizzatore finale che questi sta interagendo con un sistema di IA. Difatti, i beneficiari dell'art. 52 non sono gli "utenti" nel senso utilizzato dalla Proposta, ma tutte le "persone fisiche" che con il sistema interagiscono, e specialmente gli "utilizzatori finali" (v. sezione 0). Infine, quando i sistemi soggetti all'art. 52 rientrino nella categoria ad alto rischio, a tali obblighi si aggiungono i requisiti previsti dal titolo III (inclusa la spiegabilità).

[38] C. Deskus, *Fifth Amendment Limitations on Criminal Algorithmic Decision-Making*, NYUJ Legis. & Pub. Policy, 21, 2018, p. 237.

[39] L. Bainbridge, *Ironies of automation, in Analysis, design and evaluation of man–machine systems*, Elsevier, 1983, pp. 129–135.

[40] J. Millar, I. Kerr, *Delegation, relinquishment, and responsibility. The prospect of expert robots*, in Robot Law, Edward Elgar Publishing, 2016

[41] F. Lagioia, G. Contissa, *The Strange Case of Dr. Watson: Liability Implications of AI Evidence-Based Decision Support Systems in Health Care*, Eur. J. Legal Stud., 12, 2020, p. 281.

Il primo gruppo descritto nell'art. 52 si riferisce genericamente a sistemi "destinati a interagire con le persone fisiche". Sebbene la definizione appaia piuttosto ambigua, la disposizione è stata pensata per affrontare il problema dei chatbot[42]. In questo caso, il fornitore del sistema deve garantire che le persone (utenti e "utilizzatori finali") siano consapevoli di interagire con un'IA. L'obbligo non si applica quando l'interazione "è evidente dalle circostanze e dal contesto di utilizzo".

Il secondo gruppo ricomprende i sistemi di riconoscimento delle emozioni e di categorizzazione biometrica. Questi sistemi interpretano i dati biometrici e fanno valutazioni sugli individui ma, a differenza dei sistemi di cui all'art. 5 lett. d) e all'Allegato III, n. 1, non sono finalizzati all'identificazione della persona fisica. Alla prima categoria possono essere ricondotti, ad esempio, i sistemi di IA che applicano tecniche di analisi del sentimento o di profilazione psicografica. Alla seconda categoria possono essere ricollegati invece alcuni *wearable* come Apple Watch o FitBit, che utilizzano dati biometrici per effettuare valutazioni sullo stato di salute degli utenti, ma anche sistemi di riconoscimento vocale (come Siri o Alexa) o facciale. Per quanto certamente utile, si può dubitare che siffatto requisito di trasparenza possa diminuire in modo significativo la pericolosità di questi sistemi rispetto a diritti e libertà fondamentali.

Infine, il terzo gruppo di sistemi inclusi nell'articolo 52 si riferisce alla pratica dei "deep fakes". Tale pratica è definita come l'uso del sistema di IA per generare o manipolare un contenuto (immagine, audio o video) in modo tale da creare una somiglianza pressoché perfetta con persone, luoghi o oggetti effettivamente esistenti e indurre così l'utente a considerarlo autentico.

Per tutte le tipologie di sistemi qui descritte è prevista un'eccezione all'obbligo di trasparenza nel caso in cui i sistemi siano utilizzati a fini di indagine e accertamento di reati.

[42] I chatbot possono essere definiti come sistemi software che utilizzano tecniche di elaborazione (NLP) e generazione (NLG) del linguaggio naturale per simulare una conversazione con un essere umano.

7. Valutazione di conformità, sistema di monitoraggio e governance

Per completare il quadro della Proposta, occorre infine soffermarci sulle forme di controllo preventivo dei sistemi di IA e di monitoraggio successivo alla loro immissione nel mercato, nel quadro più generale dei sistemi di governance previsti dal legislatore europeo.

Le nuove norme prevedono che, prima della loro immissione sul mercato, i sistemi di IA ad alto rischio siano sottoposti ad una preliminare valutazione di conformità ai requisiti del Regolamento. Come regola generale, l'art. 43(2) stabilisce che la valutazione di conformità si basa sul controllo interno del fornitore (disciplinato dall'Allegato VI). Ciò significa che i fornitori valutano autonomamente che il loro sistema di gestione della qualità e la documentazione tecnica specifica siano aderenti ai requisiti normativi. A questo fine, i fornitori possono adeguarsi agli standard esistenti[43] oppure possono implementare a livello tecnico i requisiti essenziali del Regolamento in modo autonomo.

In determinati casi è invece previsto l'intervento di soggetti terzi. Per i sistemi di categorizzazione biometrica delle persone fisiche (art. 43(1)), l'autovalutazione richiede l'approvazione di un "organismo notificato" (art. 33) indipendente e accreditato presso le autorità di sorveglianza prevista dal Regolamento. I sistemi che costituiscono componenti di sicurezza di prodotti già regolati dal New Legislative Framework (NLF) seguono la procedura di valutazione di cui alla relativa normativa, al fine di evitare duplicazioni procedurali (art. 43(3)).

Per molti dei sistemi di IA ad alto rischio i fornitori potranno invece apporre il marchio di conformità UE sulla base della sola autovalutazione. Questa scelta solleva non poche perplessità, nella misura in cui si esclude qualsiasi supervisione preventiva relativamente a tecnologie considerate molto rischiose per le persone[44].

La Proposta di Regolamento stabilisce un sistema di governance dell'ordinamento sia a livello UE che a livello nazionale. A livello dell'UE, la Proposta istituisce una nuova autorità, il Comitato europeo

[43] Su delega della Commissione europea, gli organismi di standardizzazione (come il CEN o il CENELEC) possono prevedere degli standard tecnici relativi ai requisiti essenziali dei sistemi di IA ad alto rischio.

[44] Per un'analisi della valutazione di conformità v. J. Mökander, M. Axente, F. Casolari, and L. Floridi, *Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI Regulation*, Minds and Machines, 2021, pp. 1–28.

per l'Intelligenza artificiale, con compiti di coordinamento della governance (titolo VI, capo 1). Il Comitato garantisce l'efficace cooperazione tra le autorità nazionali (anche attraverso la condivisione di *best practices*), e sostiene l'attività della Commissione formulando pareri e linee guida.

Gli Stati membri, dal canto loro, dovranno designare una o più autorità nazionali competenti, per sorvegliare sull'applicazione e il rispetto del Regolamento (capo 2). Le autorità potranno chiedere ai fornitori informazioni e accedere alla documentazione, sollecitare l'adozione di misure correttive e il ritiro del sistema dal mercato.

Per quanto riguarda gli ulteriori strumenti di governo del sistema, il titolo VII della Proposta dispone l'istituzione, presso la Commissione europea, di una banca dati per i sistemi di IA indipendenti ad alto rischio. La banca dati raccoglierà informazioni importanti sulle caratteristiche e le finalità dei sistemi, sulle certificazioni pertinenti e sull'identità del fornitore[45]. Si prevede poi, al titolo IX, che la Commissione e gli Stati membri promuovano l'adozione di codici di condotta per i sistemi di IA diversi da quelli ad alto rischio. Tali codici dovrebbero adeguarsi ai requisiti previsti per i sistemi ad alto rischio, in modo che anche i sistemi non ad alto rischio rispettino gli stessi standard.

Per quanto riguarda le sanzioni, la Proposta sembra seguire l'approccio già adottato dal GDPR. Al titolo X sono previste sanzioni amministrative in caso di violazione o mancato rispetto delle norme contenute nel Regolamento. In caso di violazione dei divieti di cui all'articolo 5 o della non conformità del sistema di IA ai requisiti dell'articolo 10, le sanzioni possono arrivare fino a trenta milioni di euro o, se l'autore del reato è una società, fino al 6% del fatturato annuo globale. In caso di altre violazioni, le sanzioni sono ridotte ad un massimo di venti milioni di euro o del 4% del fatturato della società (art. 71).

Nonostante la rilevanza delle misure sanzionatorie e la possibilità per le autorità di richiedere il ritiro dal mercato o il richiamo dei prodotti, la disciplina complessiva non appare del tutto sufficiente a garantire un'applicazione efficace. L'esperienza del GDPR mostra che un eccessivo affidamento sull'*enforcement* delle autorità nazionali si espone al rischio di difformità applicative, a causa delle notevoli divergenze di risorse e prassi di intervento nei diversi Stati membri. Com'è usuale in campo tecnologico, poi, si pone il problema di possibili

[45] L'elenco completo delle informazioni è contenuto nell'Allegato VII.

difformità nei criteri di valutazione degli standard tecnici, che sarà tanto più pregnante in un settore, quello dell'IA, caratterizzato da un elevato numero di attori e di standard diversi.

Infine, occorre segnalare che la Proposta non contiene meccanismi di azione per gli individui o gruppi danneggiati, nemmeno nella forma di reclamo (ad es. all'autorità di sorveglianza del mercato). L'assenza di tali previsioni, che avrebbero compensato i limiti dell'*enforcement* pubblico, risulta certamente criticabile, avendo come effetto anche il ridimensionamento del ruolo della società civile nello sviluppo affidabile dell'IA.

8. Conclusioni

Sulla base di questa breve rassegna, possiamo formulare qualche osservazione conclusiva.

La Proposta costituisce, come si è visto, il frutto di un processo condiviso nell'alveo delle istituzioni europee, ed ha il merito di riunire i diversi aspetti tecnologici, socio-economici e regolativi sottesi allo sviluppo e alla diffusione dell'IA in Europa. Elabora una definizione e una classificazione dei diversi sistemi, fornisce un insieme di requisiti e di incombenze per quei sistemi che mettono a rischio i diritti e i valori europei, stabilisce un'architettura di governance e monitoraggio delle tecnologie. Tuttavia, diversi sono i punti deboli di questa legislazione.

Si sono notate le carenze relative ai diversi aspetti della normativa: le incertezze nella definizione e classificazione dei sistemi (si pensi alla genericità del requisito dei "metodi statistici"), le ambiguità nelle proibizioni (come il *social scoring* pubblico) e nei requisiti dei sistemi ad alto rischio (ad es. la sorveglianza umana), le insufficienze nei meccanismi di controllo (si pensi al cd. controllo interno). A nostro parere, tutti questi aspetti sottendono due elementi di carattere generale che rivelano la prospettiva complessiva del legislatore europeo, da un lato volta alla protezione dei diritti e delle libertà fondamentali, ma dall'altro largamente influenzata dal modello di legislazione industriale orientata al mercato.

Il primo elemento è costituito dall'approccio *top-down* del Regolamento[46]. Il legislatore identifica le tecnologie dell'AI, predetermina le pratiche proibite e rischiose e identifica *ex ante* il livello di rischio, facendone derivare le regole applicabili. Tuttavia, lo studio dell'automazione suggerisce come sia più adeguato, per la regolazione di tali tecnologie, un approccio *bottom-up*, basato sull'identificazione delle caratteristiche della tecnologia e dei processi nei quali essa viene utilizzata (e ciò soprattutto se si opera in un contesto basato sul rischio). In caso contrario, come si è visto nel presente commento, si corre il pericolo di creare categorie normative astratte che non rappresentano in modo adeguato caratteri e rischi effettivi delle singole soluzioni tecnologiche.

In secondo luogo, l'impianto complessivo della Proposta rivela una contraddizione di fondo fra il piano pubblicistico e quello dei diritti individuali. Le norme intendono regolare il rischio che l'IA crea per i valori e i diritti umani tutelati dall'Unione. E tuttavia: dove si trova l'essere umano in queste norme? La Proposta è incentrata su obblighi e prerogative del fornitore, dell'utente e del supervisore: definisce i requisiti di sviluppo dei sistemi, le modalità di utilizzo e certificazione, i meccanismi di controllo. Dei soggetti su cui ricadono le conseguenze dell'utilizzo del sistema non v'è quasi traccia: a chi subisce l'operato del sistema (ad esempio chi si ritrova sorvegliato, indagato, accusato da un'IA) non si conferiscono diritti né strumenti di azione. Il Regolamento proclama di volere difendere i valori europei e i diritti fondamentali dai rischi dell'IA. Tuttavia, per perseguire questo lodevole obiettivo, nessuno strumento specifico di difesa in più viene fornito ai titolari dei diritti coinvolti.

Perché non mettere nero su bianco nella Proposta, ad esempio, il diritto ad ottenere una spiegazione da parte del sistema AI? O il diritto a non essere soggetti a decisioni discriminatorie? Per entrambi gli aspetti, il legislatore avrebbe potuto fornire linee guida di sviluppo tecnico e certificazione. Si tratta di due aspetti, peraltro su cui il GDPR non aveva fatto chiarezza, e questa poteva certamente essere l'occasione per rimediare[47].

[46] L. Floridi, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, Philosophy & Technology, 34, 2021, pp. 215–222.

[47] S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*; M. Brkan, *op. cit.*, pp. 100-101.

L'attenzione all'impatto dell'IA sulle persone, del resto, sarebbe forse stata agevolata da un approccio *bottom-up*. Si sarebbe potuto, ad esempio, partire dalla Carta dei diritti fondamentali dell'Unione europea, stabilendo per ciascun diritto i parametri di misura del rischio legato alla sua violazione (tenendo conto del "peso" di ogni diritto, e del grado di rischio). Sulla base di questi parametri, si sarebbe potuto determinare, di volta in volta, il livello di rischio dello specifico sistema di IA (evitando così il "*cherry-picking*" di cui si è detto), nonché le misure di protezione individuali. In questo modo, sarebbe stato possibile fornire una sorta di diritti "accessori" che rendessero "azionabili" i diritti umani messi in pericolo.

Si può insomma concludere che Proposta di Regolamento, tentando di coniugare i diritti individuali con le esigenze di mercato relative all'IA, fatichi a trovare un bilanciamento soddisfacente e soluzioni applicative adeguate. Ci si può certamente augurare che il prosieguo del percorso legislativo conduca ad un maggiore equilibrio.

PARTE IV

MODELLI IBRIDI DI COOPERAZIONE GIUDIZIARIA

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643021
pp. 413-430 (gennaio 2022)

Aspetti di Informatica forense nel Regolamento della Procura europea

ANTONIO GAMMAROTA[1]

1. Premessa e delimitazione dell'ambito di indagine

Il Regolamento (UE) 2017/1939 del Consiglio del 12 ottobre 2017 che riguarda l'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea ("EPPO")[2] – d'ora in poi anche solo "Regolamento" – istituisce il nuovo organo inquirente indipendente incaricato di individuare, perseguire e portare in giudizio gli autori dei reati che ledono gli interessi finanziari dell'Unione previsti dalla direttiva (UE) 2017/1371 e stabiliti dal regolamento[3].

Il Regolamento attua l'art. 86 del Trattato sul funzionamento dell'Unione europea (TFUE) introdotto dal Trattato di Lisbona e disciplina molti aspetti del nuovo organo inquirente europeo tra loro eterogenei, prevedendo norme sulla costituzione, composizione, organizzazione, procedura, bilancio interno, attuazione e coordinamento. Nella loro diversità, non sempre in linea con l'elevata qualità della tecnica legislativa dell'Unione, le norme del Regolamento compongono in un

[1] Ph.D, Professore a contratto di Informatica forense, Dipartimento di Scienze Giuridiche, CIRSFID - Alma Human Artificial Intelligence, Università di Bologna; Avvocato in Bologna, Cassazionista.

[2] EPPO è l'acronimo di European Public Prosecutor Office, Ufficio del istituito con Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), in https://eur-lex.europa.eu/eli/reg/2017/1939/oj; per la presente analisi verrà utilizzato il testo ufficiale pubblicato in italiano come REGOLAMENTO (UE) 2017/1939 DEL CONSIGLIO del 12 ottobre 2017 relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea (EPPO), in GUUE L283 31 ottobre 2017.

[3] Cfr. D. CAVALLINI, *Analisi della disciplina e prime riflessioni sui profili ordinamentali della procura europea, alla luce del d.lgs. n. 9 del 2021 di adeguamento della normativa nazionale al regolamento europeo*, maggio 2021, in https://dirittodidifesa.eu/; A. DAVOLI, *Cooperazione giudiziaria in materia penale*, https://www.europarl.europa.eu/ftu/pdf/it/FTU_4.2.6.pdf.

quadro unitario l'articolata fisionomia strutturale e funzionale del nuovo organo inquirente[4].

Il presente contributo verterà sull'analisi di alcune norme del Regolamento EPPO che rientrano nello spettro di interesse dell'Informatica forense[5], con l'intento di individuare eventuali intersezioni con i principi e la disciplina interna in tema di indagini informatiche, mezzi di prova digitale e mezzi per la loro ricerca. Non potranno invece essere affrontati, per economia espositiva, i temi collaterali riguardanti la gestione dei flussi documentali digitali effettuati dall'EPPO, in quanto rientranti nell'ambito dell'informatica giudiziaria, branca dell'informatica giuridica che studia le norme e le tecniche per la gestione automatizzata dei flussi documentali del processo, materia regolata dagli artt. 43-46 del Regolamento, né le problematiche attinenti al rapporto tra attività dell'EPPO e la protezione dei dati personali *tout court*[6], né le norme sul trattamento dei c.d. dati personali operativi di cui al Capo VIII del Regolamento[7].

[4] Non è ancora possibile vagliare casi affrontati dall'EPPO; tuttavia, il primo banco di prova per l'operatività dell'organo sarà probabilmente costituito dai casi che seguiranno alle notizie di reato relative ai finanziamenti a sostegno dell'azione per la ripresa economica e sociale europea intrapresa con il piano Next Generation EU.

[5] Disciplina che studia le norme giuridiche e le regole tecniche per il trattamento dei dati digitali ad uso forense; tale definizione costituisce l'affinamento della prima versione esposta nel corso della presentazione sul tema "Dalla Computer Forensics all'Informatica forense" svolta a maggio 2003 nell'ambito della II edizione del Master in Diritto delle nuove tecnologie, Centro Studi di Informatica Giuridica di Bari, come riportato da P. GALEOTTI, Master-*Post eventum* 12.05.03, in http://www.avvocatiacquavivacassano.it; sulle origini, oggetto e metodo dell'Informatica forense, sia consentito rinviare a A. GAMMAROTA, *Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali*, 2016, in https://amsdottorato.unibo.it.

[6] A quest'ultimo proposito, va notato come il Considerando 95 ("*Le disposizioni del presente regolamento in materia di protezione dei dati non pregiudicano le norme applicabili relativamente all'ammissibilità dei dati personali come prova nei procedimenti penali.*"), riaffermi il principio di autonomia e prevalenza del trattamento dei dati personali per fini giudiziari e di prova, in base al quale nessuna facoltà ad essa relativa può essere in alcun modo compressa dalle norme sulla protezione dei dati personali, nemmeno ove previste dallo stesso Regolamento.

[7] La disciplina di cui al capo VIII, artt. 47-89, dedicata alla Protezione dei dati personali definiti "operativi" sembra approntata per l'EPPO nella sua posizione soggettiva di titolare del trattamento.

2. I principi fondamentali del Regolamento EPPO

L'EPPO svolge indagini, esercita l'azione penale ed esplica le funzioni di pubblico ministero dinanzi agli organi giurisdizionali competenti degli Stati membri fino alla pronuncia del provvedimento definitivo (cfr. art. 4, Reg.) e svolge la propria attività cooperando e avvalendosi del sostegno di Eurojust, in conformità dell'articolo 100 del Regolamento (cfr. art. 3, Reg.)[8].

Per quanto riguarda la sua articolazione, il nuovo organo inquirente dell'Unione è indivisibile e opera come un ufficio unico con struttura decentrata ed organizzata a livello centrale e a livello decentrato.

Il livello centrale è costituito da un ufficio nella sede dell'EPPO ed è composto dal collegio, dalle camere permanenti, dal procuratore capo europeo, dai sostituti del procuratore capo europeo, dai procuratori europei e dal direttore amministrativo[9].

Il livello decentrato dell'EPPO, invece, è composto dai procuratori europei delegati (PED) aventi sede negli Stati membri. L'ufficio centrale e i procuratori europei delegati sono assistiti dal personale dell'EPPO nell'esercizio delle funzioni ad essi assegnate dal presente regolamento (art. 8 Reg.).

Tra i principi informatori delle attività svolte dall'EPPO e previsti dall'art. 5 Reg., vanno annoverati l'obbligo di rispetto dei diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea (co. 1), lo svolgimento delle attività nel rispetto dei principi dello stato di diritto e della proporzionalità (co. 2), le norme sul diritto applicabile (co. 3), l'obbligo di indagare in maniera imparziale e di raccogliere tutte le prove pertinenti, sia a carico che a discarico (co. 4), l'avvio e la conduzione delle indagini senza indebito ritardo (co. 5), l'obbligo per le autorità nazionali competenti di assistere attivamente e prestare sostegno alle indagini e alle azioni penali dell'EPPO, informandosi al principio di sincera cooperazione (co. 6).

[8] Sui rapporti tra EPPO ed Eurojust, v. A. CLUNY, *In principio era la Procura europea*, in Questione Giustizia, 2/2021, in https://www.questionegiustizia.it.

[9] Sulla struttura e funzioni dell'EPPO, v. F. FALATO, *L'azione penale verso le nuove misure d'indagine europee (Metodo e contenuti di una categoria dommatica rivisitata alla luce della entrata in funzionamento della Procura europea tra fisiologie regolamentari e difetti della legge delega)*, 2020, in https://archiviopenale.it.

Oltre a istituire e regolamentare il funzionamento del nuovo organo inquirente europeo, il Regolamento prevede anche alcune norme di natura processuale e organizzative per le attività di investigazione e indagine su reati di specifica competenza.

3. Le competenze dell'EPPO

La competenza per materia dell'EPPO, regolata dall'art. 22 del Regolamento, è limitata ai reati di cui all'articolo 3, paragrafo 2, lettera d), della direttiva (UE) 2017/1371[10], ovvero ai casi di "Frode che lede gli interessi finanziari dell'Unione", quale attuata dalla legislazione nazionale, allorquando le azioni od omissioni di carattere intenzionale definite in detta disposizione siano connesse al territorio di due o più Stati membri e comportino un danno complessivo pari ad almeno 10 milioni di EUR.

Quindi, si tratta di una competenza *ratione materiae* riservata ai casi più gravi di frode e ripartita territorialmente con la competenza nazionale, alle quali residuano i casi di rilevanza economica inferiore alla già menzionata soglia.

In secondo luogo, va ricordato come il fine perseguito dall'Unione con il Regolamento non sia solo quello di dare corpo, voce e azione all'organo deputato alla persecuzione delle violazioni delle norme finanziarie europee, funzione tipica autonomamente svolta anche dagli organi di accusa degli ordinamenti statali europei, quanto quello di costruire un'autonoma operatività del nuovo ufficio armonizzata con i principi e le autorità giurisdizionali dei paesi membri[11].

Difatti, nonostante la sua immediata efficacia, il Regolamento richiede agli stati membri il varo di ulteriori atti normativi nazionali per integrare e adattare le norme interne alle previsioni europee e rendere operativo il nuovo organo[12].

[10] DIRETTIVA (UE) 2017/1371 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 5 luglio 2017 relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale, c.d. direttiva PIF su Protezione Interessi Finanziari, reati di riciclaggio e frodi transfrontaliere in materia di IVA.

[11] Cfr. F. Falato, cit.

[12] L'Italia ha avviato tale attività integratrice nel 2019 con la legge delega n. 117 mediante la quale sono stati definiti anche i principi e i criteri direttivi per l'attuazione della direttiva PIF. Sono poi seguiti due decreti attuativi: il d.lgs. 14 luglio 2020, n. 75 che attua la direttiva PIF e il d.lgs. 2 febbraio 2021, n. 9 relativa ai caratteri della nuova figura dei pubblici ministeri europei; sull'at-

L'armonizzazione dell'azione costituisce il nucleo del principio fondamentale disciplinato dall'art. 5, co. 3, in tema di rapporti con gli ordinamenti statali, il quale prevede che: «3. Le indagini e le azioni penali a nome dell'EPPO sono disciplinate dal presente regolamento. Il diritto nazionale si applica agli aspetti non disciplinati dal presente regolamento. Salvo disposizione contraria del presente regolamento, il diritto nazionale applicabile è il diritto dello Stato membro il cui procuratore europeo delegato è incaricato del caso ai sensi dell'articolo 13, paragrafo 1. Qualora un aspetto sia disciplinato sia dal diritto nazionale che dal presente regolamento, prevale quest'ultimo».

Detta norma fissa i principi che regolano il diritto applicabile alle indagini e alle azioni penali aventi ad oggetto i reati di competenza dell'EPPO e graduando la prevalenza delle discipline giuridiche concorrenti nei seguenti termini:

1) alle indagini e azioni penali dell'EPPO si applicano le norme del Regolamento, secondo un principio che potremmo definire di "esclusività";
2) agli aspetti non disciplinati dal Regolamento si applicano le norme nazionali, secondo un principio di "residualità";
3) salvo disposizione contraria dello stesso Regolamento, il diritto nazionale applicabile ai casi residuali è il diritto dello Stato membro il cui procuratore europeo delegato è incaricato del caso ai sensi dell'articolo 13, paragrafo 1, secondo un principio di residualità giuridica di quest'ultimo;
4) nel caso in cui l'aspetto sia disciplinato sia dal diritto nazionale che dal Regolamento, prevale quest'ultimo, in base al principio di "prevalenza dell'EPPO".

tività di adeguamento dell'Italia, v. L. SALAZAR, *L'adeguamento interno da parte italiana al regolamento EPPO alla vigilia dell'avvio delle prime indagini*, in Sistema penale, 4/2021, https://www.sistemapenale.it; G. GUAGLIARDI, *Procura Europea. Siamo davvero pronti in assenza di un codice di procedura penale europeo? Una nuova sfida per l'avvocatura e la magistratura,* Giurisprudenza Penale Web*,* 2021/2, in https://www.giurisprudenzapenale.com.

4. Le norme del Regolamento EPPO rilevanti per l'Informatica forense

I dati digitali apportano un indubbio contributo informativo alla ricostruzione processuale dei fatti, negli ultimi anni essi hanno assunto una progressiva rilevanza in ogni tipologia di processo, ed in particolare nelle investigazioni informatiche e telematiche in ambito penale[13]. La centralità assunta dai dati digitali per le investigazioni e indagini penali è un fenomeno riscontrabile sia nel panorama nazionale che transnazionale quale effetto comune del processo di globalizzazione e capillarizzazione della tecnologia digitale[14].

Tuttavia, se da un lato le informazioni di interesse processuale tratte dai dati digitali ormai prevalgono sugli altri elementi di prova, è altrettanto vero che domina una scarsa attenzione per l'applicazione di norme giuridiche e regole tecniche idonee a garantire una sufficiente qualità dei dati digitali dai quali vengono tratte tali informazioni.

Tra le norme del Regolamento EPPO più tipicamente procedurali è possibile individuare una serie di norme che prevedono diversi strumenti investigativi e di indagine rivolte alla ricerca e acquisizione di dati e documenti digitali a fini di prova.

Tali norme, però, pur riguardando il trattamento di dati digitali a fini investigativi e probatori, non comprendono alcuna previsione relativa alle procedure tecniche necessarie a garantire agli stessi un sufficiente livello di qualità[15], a differenza delle analoghe o ulteriori misure investigative e di indagine già presenti nei singoli ordinamenti statali pur richiamate in via residuale o sussidiaria.

[13] C. Maioli, *Dar voce alle* prove: elementi di informatica forense, in *Crimine virtuale, minaccia reale*, Franco Angeli, Milano, 2004.

[14] Per le problematiche relative allo scambio della prova v. M.A. Biasiotti, *Presente e futuro dello scambio della prova elettronica in Europa,* in M.A. Biasiotti, M. Epifani, F. Turchi (a cura di), *Trattamento e scambio della prova digitale in Europa,* in *Informatica e Diritto,* 1-2/2015, ESI, Napoli, 2016; per le questioni relative alla circolazione delle notizie di reato, A. Gammarota, *Lo scambio transnazionale di notizie di reati informatici: questioni di legittimità e di effettività dei diritti di difesa dell'indagato-imputato, ibidem*, pp. 391 e ss.

[15] Sulle problematiche relative al trattamento dei dati digitali ad uso probatorio, v. A. Gammarota, *La tecno-regolazione del trattamento dei dati digitali nel processo penale,* in R. Brighi, M. Palmirani, M.E. Sánchez Jordán (a cura di), *Informatica giuridica e informatica forense al servizio della società della conoscenza. Scritti in onore di Cesare Maioli,* Aracne editrice, 2018, pp. 255-282.

Tale lacuna non mancherà di creare situazioni ambigue nelle quali la mancanza di coordinamento tra le norme ad analogo contenuto faranno propendere per opzioni che privilegeranno le misure meno garantite.

5. I principi sulle misure investigative

La Sezione 2 del Regolamento riguarda le *Norme relative alle misure investigative e ad altre misure* che costituiscono il fulcro della disciplina degli strumenti investigativi forniti all'EPPO, inclusa una serie di previsioni operative per la raccolta, assicurazione e trattamento degli elementi di prova relativi ai fatti oggetto di indagine.

La sezione è aperta dall'articolo 30 sulle "Misure investigative e altre misure" ed esordisce attribuendo ai PED gli strumenti ivi elencati prevedendo che: «1. Almeno nei casi in cui il reato oggetto dell'indagine è punibile con una pena massima di almeno quattro anni di reclusione, gli Stati membri assicurano che i procuratori europei delegati siano autorizzati a disporre o a chiedere le misure investigative seguenti».

Poiché si tratta di una serie di misure costituenti una base minima comune agli inquirenti europei, va in primo luogo annotata la parte finale della norma che impone agli Stati membri di prevedere nei rispettivi ordinamenti interni misure che, in relazione ai casi oggetto di indagine rientranti nell'ambito della competenza per materia fissata dal Regolamento e costituenti reato per i quali siano previsti limiti edittali nel massimo di almeno quattro anni, riconoscano agli inquirenti delegati[16] il potere di disporre degli strumenti investigativi introdotti dal Regolamento, direttamente o a richiesta, evidentemente rivolta all'organo giurisdizionale competente ad autorizzarla[17].

La sussunzione nell'ordinamento statale delle misure investigative previste dal Regolamento apre la questione riguardante le modalità con le quali si procederà all'integrazione e coordinamento del Regolamento con l'analoga disciplina interna dei paesi membri. L'adeguamento imporrà la scelta di tecnica legislativa tra l'interpolazione delle norme esi-

[16] Per le norme sulla composizione dell'ufficio dell'EPPO e sulla funzione dei procuratori europei e delegati, si vedano artt. 8 e ss. del Regolamento.

[17] A tal proposito sarà interessante osservare l'esito che avranno le risultanze di attività investigative disposte sulla base di un giudizio che successivamente possa rivelarsi privo dei requisiti di ammissibilità dello strumento investigativo richiesto, e quale tipo di invalidità, e di che natura, o di inutilizzabilità, assoluta o relativa, delle risultanze investigative si affermerà.

stenti e l'adozione di un autonomo strumento normativo dedicato alle nuove misure. Per quanto riguarda il nostro ordinamento, sulla base delle esperienze analoghe del passato, può preconizzarsi come altamente probabile che si proceda con l'ennesimo intervento integratore del codice di procedura penale, con l'effetto di appesantire ulteriormente l'ordito codicistico[18].

Ove l'attività adeguatrice tardasse o mancasse, il nuovo organo non rimarrebbe comunque privo di poteri e inane. Infatti, l'immediata efficacia e vincolatività che caratterizza un Regolamento dell'Unione, il portato letterale delle misure ivi previste sufficientemente completo e dettagliato, in alcuni casi più specifico rispetto alle analoghe ma meno aggiornate norme statali, la previsione comune a tutti i paesi membri, costituiscono sufficiente garanzia di immediata efficacia dell'azione dell'EPPO.

Ove invece le misure previste dal Regolamento siano già previste anche dai singoli ordinamenti dei paesi membri, sorge la questione della concorrenza di tali strumenti. A tal proposito sovvengono gli ulteriori principi del Regolamento cui si è già fatto riferimento in precedenza, finalizzati a risolvere questioni riguardanti il diritto applicabile alle indagini.

Secondo il principio di esclusività di cui all'art. 5, co. 3, gli strumenti di indagine dell'EPPO prevalgono rispetto alle analoghe previsioni dei singoli ordinamenti nazionali. Tuttavia, poiché molte misure in tema di trattamento di dati digitali e telematici a fini forensi analoghe a quelle previste dal Regolamento sono già presenti nel nostro codice di rito e con un maggior dettaglio in conseguenza delle modifiche introdotte dalla L. 48/2008[19] di ratifica della Convenzione di Budapest[20], sarà interessante osservare quale spazio verrà riconosciuto al principio di re-

[18] È quanto, ad esempio, indicato dal DECRETO LEGISLATIVO 2 febbraio 2021, n. 9 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea «EPPO». (21G00012) (GU n.30 del 5-2-2021).

[19] Legge 18 marzo 2008, n. 48, Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno, in G. U. n. 80 del 4 aprile 2008 S.O. n. 79; sulla Legge 48/2008, v. L. Luparia (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest*, Giuffrè, Milano, 2009; P. Perri, voce *Computer forensics (indagini informatiche)*, in Digesto delle discipline penalistiche, Utet, Torino, 2011; sulla cooperazione giudiziaria in materia di criminalità informatica, v. M.A. Biasiotti, M. Epifani, F. Turchi, (a cura di), cit.

[20] *Convention on Cybercrime*, Budapest, 23, IX, 2001 in https://www.coe.int; v. G. Ilarda, G. Marullo, (a cura di), Cybercrime: conferenza internazionale – *La Convenzione del Consiglio d'Europa sulla Criminalità Informatica*, Giuffrè, Milano, 2004.

sidualità secondo il quale, in caso di aspetti non disciplinati dal Regolamento, si applicano le norme nazionali.

6. Le norme relative alle misure investigative

L'art. 30, co. 1, del Regolamento individua concretamente le misure investigative previste che verranno di seguito ripercorsi[21].

La lettera a) prevede l'attività di «a) perquisizione di locali, terreni, mezzi di trasporto, abitazioni private, indumenti o altro bene personale e sistemi informatici, nonché qualsiasi misura cautelare necessaria a preservarne l'integrità o a evitare la perdita o l'inquinamento di prove». Si tratta della perquisizione locale che, ai nostri fini, può essere effettuata anche su "sistemi informatici".

Circa il portato dell'espressione "sistemi informatici" va innanzitutto rilevato come la lacuna sul piano definitorio non consenta di delimitarne l'estensione sul piano oggettivo. Con tutti i limiti della specialità della norma che impedisce applicazioni analogiche, non si potrà non far riferimento all'analoga previsione extra ordinamentale dell'Unione, per quanto riconducibile alla medesima matrice europea, di cui all'art. 1 della Convenzione di Budapest[22] secondo la quale per sistema informatico ("computer system") si « [...] (indica) qualsiasi dispositivo o gruppo di dispositivi interconnessi o correlati, uno o più dei quali, in base a un programma, esegue l'elaborazione automatica dei dati».

Quanto alla tipologia della "perquisizione informatica", la norma non specifica se la misura si riferisca alla perquisizione "in locale" effettuata intervenendo fisicamente sul dispositivo per accedere ai dati digitali in modo diretto, o se sia ammissibile qualche forma di perquisizione telematica o da remoto o on line, attività resa possibile sia da comuni programmi di gestione a distanza di sistemi informatici, sia da strumenti specificamente dedicati alle investigazioni digitali tra i quali, ad esempio, alcuni tipi di captatore informatico[23].

[21] Le misure a disposizione dei PED vengono chiamate investigative ma non vanno confuse con quelle che, con analoga espressione nel sistema processuale penale italiano vengono indicate come attività di Polizia Giudiziaria.

[22] «*(means) any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*».

[23] Sulle potenzialità tecniche del captatore in riferimento all'attività di perquisizione informatica da remoto, R. Brighi, *Funzionamento e potenzialità investigative del malware*, in G. Giostra, R. Orlandi, (a cura di), *Nuove norme in tema di intercettazioni*, Giappichelli, 2018. pp.

In relazione ai criteri tecnici da seguire per la corretta effettuazione della "perquisizione informatica", la norma in esame non prevede l'adozione di alcuna precauzione espressamente volta alla protezione dell'integrità e affidabilità dei dati digitali e, di converso, del loro patrimonio informativo, come invece imporrebbero la natura fisica dei dati digitali e dei sistemi informatici. Si tratta di quelle misure adeguate descritte, ad esempio, nell'art. 19 della Convenzione di Budapest in tema di ricerca e sequestro di dati archiviati in computer[24] e che ormai costituiscono il paradigma tipizzato e ricorrente del trattamento dei dati digitali affinché siano ritenuti idonei a svolgere in ambito forense una funzione rappresentativa dei fatti minimamente affidabile.

In Italia, ad esempio, tali cautele sono state trasfuse in molteplici previsioni della Legge 48/2008 e, tra le altre, nell'analoga norma di cui all'art. 247, co. 1-bis, c.p.p. in tema di sequestro di dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che si trovino in un sistema informatico o telematico.

È evidente come la previsione della perquisizione informatica europea rievochi tutte le questioni riguardanti il diritto all'autodeterminazione informativa della persona, per la tutela del quale bisognerà trovare il punto di equilibrio tra esigenze investigative e protezione dei diritti fondamentali della persona[25].

La seconda parte della norma sulla perquisizione, evidenzia la necessità di misure che siano dirette a *preservarne l'integrità o a evitare la perdita o l'inquinamento di* prove, e quindi specificamente finalizzate a proteggere il risultato della perquisizione. Tale previsione richiama non tanto le specifiche misure tecniche cui si è appena fatto riferimento,

211-236; M. Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali,* Giuffrè, 2017; sull'utilizzabilità per intercettazioni da remoto senza necessità di rogatoria internazionale, v. Cass. Sez II., 22 ottobre 2020 (ud. 22 luglio 2020), n. 29362, con nota di F. Demartis, *La Cassazione rifiuta la rogatoria per le intercettazioni all'estero con captatore informatico*, in Diritto Penale e Processo, 10/2021, p. 1352 e ss.

[24] V. l'articolo 19 della Convenzione di Budapest in tema di ricerca e sequestro di dati.

[25] Sul diritto all'autodeterminazione informativa quale diritto individuale comprimibile dalla perquisizione on line dei dispositivi informatici solo a determinate condizioni si è pronunciata la Corte costituzionale tedesca in *Bundersverfassungsgericht*, 27 febbraio 2008, in Riv. trim. dir. pen. econ., 3, 2009, p. 679, con nota di R. Flor *Brevi riflessioni a margine della sentenza del Bundersverfassungsgerich sulla c.d. on line durchsuchung;* in particolare, sulla perquisizione da remoto mediante captatore, v. L. Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni,* in *Diritto Penale Contemporaneo*, 1/2018, p. 64 e ss.

quanto piuttosto le previsioni di cui norme del codice di procedura penale italiano in tema di sequestro probatorio (art. 253 e ss. c.p.p.) e di custodia delle cose sequestrate (art. 259 c.p.p.), norme queste ultime che invece prevedono le particolari cautele tecniche riconducibili al paradigma informatico-forense[26].

La lettera b) dell'art. 30 del Regolamento prevede poi la «b) produzione di qualsiasi oggetto o documento pertinente in originale o in altra forma specificata». Tale previsione non brilla per chiarezza, atteso che l'affiancamento del "documento" a "qualsiasi oggetto" sottenderebbe un'unica categoria omnicomprensiva basata sull'elemento della "materialità" che, unitamente alla specificazione "pertinente in originale", sembrerebbe limitare la previsione normativa ai soli documenti analogici[27]. Con uno sforzo esegetico non del tutto convincente si potrebbe ritenere che la successiva espressione «o in altra forma specificata», analogamente alla clausola residuale di atipicità della forma prevista dall'art. 234 c.p.p. in tema di prova documentale, consentirebbe di recuperare alla categoria dei documenti la ben più ampia tipologia dei documenti digitali. Va altresì notato come la lettera della norma in esame soffrirebbe di qualche incertezza nel punto in cui, riferendosi al *documento pertinente in originale o in altra forma specificata*, non consenta di distinguere i documenti digitali tra documenti originali e documenti originari a seconda del rapporto di anteriorità cronologica che può sussistere tra le due tipologie e dal quale dipendono notevoli ripercussioni sul piano ontologico, pratico e giuridico[28].

[26] Con l'espressione "Paradigma di Budapest" indico il modello di procedura introdotto dall'art. 19 della Convenzione di Budapest in tema di perquisizione e sequestro di dati archiviati e che caratterizza ogni procedura di trattamento dei dati digitali a fini processuali: «[…] *a seize or similarly secure a computer system or part of it or a computer-data storage medium;b) make and retain a copy of those computer data;* c) *maintain the integrity of the relevant stored computer data; d) render inaccessible or remove those computer data in the accessed computer system* […]».

Trasfuso dalla L. 48/2008 in varie norme del codice di procedura quali gli artt. 244, 247, 254-bis, il Paradigma è compiutamente riprodotto nell'art. 260 c.p.p.: «Sigillo elettronico o informatico e copia di dati - Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

[27] Per un inquadramento della prova documentale anche in relazione alla natura analogica o digitale, v. P. TONINI, C. CONTI, *Il diritto delle prove penali,* Giuffrè, 2014, pp. 383 e ss.

[28] La distinzione tra documento digitale originale e documento digitale originario costituisce una delle categorie classificatorie più rilevanti nell'ambito dell'informatica forense, sul quale sia consentito rinviare ancora ad A. GAMMAROTA, 2016, cit., p.112 e ss.

Infine, la propensione a ritenere la norma in esame relativa ai soli documenti, siano essi analogici o digitali, verrebbe agevolata dal contenuto delle lettere a) e c) del medesimo art. 30 che invece prevedono misure specifiche proprie per i dati informatici che, a buon motivo, vengono ritenuti entità concettualmente e giuridicamente diverse.

Infatti, fermo quanto già evidenziato per la lettera a) dell'art. 30, la lettera c) prevede la misura volta ad «(c) ottenere la produzione di dati informatici archiviati, cifrati o decifrati, in originale o in altra forma specificata, inclusi i dati relativi al conto bancario e i dati relativi al traffico, ad eccezione dei dati specificamente conservati conformemente al diritto nazionale ai sensi dell'articolo 15, paragrafo 1, seconda frase, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio»[29].

Tale norma contempla la misura volta a prevedere la produzione di dati informatici accomunati dalla loro natura tecnica, sia in chiaro che cifrati, a prescindere dal loro contenuto.

Da tale misura sono espressamente esclusi i dati oggetto degli obblighi di conservazione dei dati di traffico telefonico e telematico di cui alla direttiva 2002/58/CE relativa al trattamento dei dati personali ed alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Per il resto, la norma prevede una misura volta ad ottenere la produzione di dati digitali dalla più disparata natura e che, essendo accomunati unicamente dalla loro rappresentazione binaria, richiederà un'attività di coordinamento con categorie e discipline specifiche relative ad altre tipologie di dati digitali.

Sarà interessante osservare come tale misura verrà coordinata con le norme del rito italiano nel quale tali dati non rilevano tanto per la loro natura digitale, quanto per la natura dei documenti che li veicolano o mediante i quali sono rappresentati quali, ad esempio, i documenti informatici *tout court*, la corrispondenza telematica, i dati bancari, ecc., assecondate dalla tendenza della giurisprudenza di legittimità a classificare nella categoria residuale del documento ogni elemento di prova digitale che non trovi *aliunde* altra più idonea classificazione.

La lettera d) dell'art. 30 prevede il «d) congelamento degli strumenti o dei proventi di reato, compresi i beni, di cui si prevede la confisca da

[29] Si tratta della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali ed alla tutela della vita privata nel settore delle comunicazioni elettroniche.

parte del giudice competente, ove vi sia motivo di ritenere che il proprietario o chi possiede o ha il controllo di detti proventi o strumenti di reato si adopererà per vanificare il provvedimento di confisca».

Per quanto l'espressione "congelamento"[30] non trovi corrispondenza nelle norme del nostro codice di procedura penale, è probabile che con tale espressione debba intendersi il sequestro conservativo. Ove così fosse, la previsione rileverebbe ai fini dell'informatica forense nei casi in cui fosse necessario sottoporre a misura conservativa in vista della confisca quegli strumenti, proventi e beni caratterizzati dalla loro natura digitale. Si pensi, ad esempio, ai reati commessi mediante l'uso di dispositivi informatici o telematici, ovvero a proventi di reato realizzati o convertiti in criptovalute, situazioni ricorrenti con frequenza sempre maggiore.

Ebbene, anche in tali casi, oltre alle norme procedurali, sarà opportuno fare riferimento anche alle regole tecniche relative al corretto trattamento dei dati digitali ampiamente trattate nell'ambito dell'Informatica forense.

Alla lettera e) dell'art. 30 del Regolamento, si prevede la misura dell'*intercettazione delle comunicazioni elettroniche di cui l'indagato o l'imputato è destinatario o mittente, su ogni mezzo di comunicazione elettronica utilizzato dall'indagato o dall'imputato*. La norma prevede la misura delle intercettazioni delle comunicazioni elettroniche il cui ambito, anche ad una interpretazione di stretta lettera, non è chiaramente delimitato e suscita diversi dubbi sulla sua portata. Infatti, non è chiaro se l'espressione "comunicazione elettronica" sia di formulazione volutamente vaga e ampia tale da poter includere ogni forma di comunicazione sia verbale, sia scritta, sia multimediale, purché elaborata da sistemi elettronici, al fine di ricomprendere non solo i dispositivi che si basino sull'elaborazione e trasmissione di dati codificati in digitale ma anche, e soprattutto, i dispositivi elettronici portatili per le comunicazioni elettroniche in senso stretto, quali ad esempio i telefoni cellulari, gli smartphone e i tablet.

La norma in esame sembra aver ricompreso in un'unica previsione ogni tipologia di comunicazione, a differenza, ad esempio, di quanto previsto nell'ordinamento italiano ove, per effetto dell'interpolazione adeguatrice ai progressi tecnologici susseguitasi negli ultimi trent'anni, l'ampia categoria della captazione delle comunicazioni risulta articolata in intercettazione di comunicazioni telefoniche personali e locali

[30] Nella versione italiana dell'art. 30 lett. d) del Regolamento, i termini "freeze" della versione inglese e "gel" della versione francese sono stati tradotti con il termine "congelamento".

(art. 266, commi 1 e 2, c.p.p.), peraltro recentemente novellata dalle previsioni relative all'utilizzo del captatore[31], e in intercettazioni di comunicazioni informatiche o telematiche (art. 266 bis c.p.p.)[32].

È evidente come alle problematiche giuridiche e tecniche che caratterizzano la disciplina nazionale già ampiamente rimarcate dalla dottrina, si sommino anche le questioni sulla gestione transnazionale di tale misura e sulla sua compatibilità con le garanzie relative alla libertà di comunicazione quale diritto fondamentale della persona e al trattamento dei dati personali.

Infine, il primo paragrafo dell'art. 30 chiude con la previsione relativa al «f) tracciamento e rintracciamento di un oggetto mediante mezzi tecnici, comprese le consegne controllate di merci».

La norma attiene all'utilizzo investigativo dei dati generati dalle tecnologie digitali che registrano i movimenti e i trasferimenti di oggetti e beni. La categoria nella quale rientrano tali tipi di dati è in realtà molto più ampia e ricomprende soprattutto, ma non solo, quelli relativi allo stoccaggio, trasporto, movimentazione e consegna di oggetti e merci.

Infatti, la norma è formulata con termini talmente ampi da consentire un uso della misura anche oltre le strette finalità che la previsione apparentemente delimiterebbe, atteso che, controllando il movimento degli oggetti e merci si può attuare il pedinamento digitale delle persone (e anche degli animali) e quindi realizzare il loro controllo a distanza. Si pensi ad esempio al tracciamento di un dispositivo digitale indossabile o dell'etichetta di un indumento che contenga un chip di tracciamento, o di un dispositivo per la geolocalizzazione di un animale domestico o selvatico, o di un qualunque altro dispositivo personale che emetta segnali che consentono di tracciarne il movimento o di geolocalizzarlo. Ebbene, in tali casi, il tracciamento del movimento del bene portato dalla persona può coincidere con il controllo del movimento e del comportamento della persona, modalità che mette in grave pericolo le libertà fondamentali e la dignità della persona.

Il paragrafo 2 dell'art. 30, prevede che «2. Fatto salvo l'articolo 29, le misure investigative di cui al paragrafo 1 del presente articolo possono essere soggette a condizioni conformemente al diritto nazionale

[31] Sugli aspetti giuridici e tecnici relativi al captatore, cfr. R. BRIGHI, cit.

[32] Va rilevato che la previsione delle intercettazioni di flussi telematici era stata trasfusa nell'art. 266-bis c.p.p. sin dal 1993 a seguito della L. 547/93. Per tale motivo, nessuna modifica era stata introdotta dalla L. 48/2008 di ratifica della Convenzione di Budapest, che ha previsto le intercettazioni di flussi telematici come strumento comune ai paesi aderenti all'azione di contrasto del cibercrimine promossa dal Consiglio d'Europa.

applicabile se il diritto nazionale contiene restrizioni specifiche che si applicano con riguardo a categorie specifiche di persone o di professionisti giuridicamente vincolati a un obbligo di riservatezza». Orbene, la norma prevede che, salvi i casi di richiesta di revoca dei privilegi e immunità previsti dal diritto nazionale (art. 29, co.1) o dell'Unione (art. 29 co. 2), le misure appena rassegnate possano essere condizionate da restrizioni e limitazioni previste dagli ordinamenti dei paesi aderenti che prevedano particolari forme di riservatezza cui sono obbligate determinate categorie di persone e professionisti.

A tal proposito, proprio il nostro codice di rito penale prevede diverse norme che potrebbero costituire attuazione della previsione in commento, in quanto dettate in materia di segreto che alcuni soggetti hanno il diritto di opporre all'ordine di esibizione di dati informatici.

È il caso ad esempio dell'artt. 256, 2 co., c.p.p. che, a fronte dell'ordine di consegnare «dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto» rivolto a chi è soggetto a segreto professionale (art. 200 c.p.p.), o di ufficio (art. 201 c.p.p.), o di stato (art. 202 c.p.p.), consente al destinatario dell'ordine di esentarsi eccependo il segreto, salva la successiva attività inquirente per la verifica della sua effettiva sussistenza.

È evidente che condizioni e prescrizioni come quelle appena esaminate prevalgano sulla misura del Regolamento, per quanto solo la loro applicazione consentirà di verificare quali modalità di coordinamento tra dette norme prevarranno.

Il paragrafo 3 dell'art. 30 del Regolamento prevede che «3. Le misure investigative di cui al paragrafo 1, lettere c), e) e f), del presente articolo possono essere soggette a ulteriori condizioni, comprese limitazioni, previste dal diritto nazionale applicabile. In particolare, gli Stati membri possono limitare l'applicazione del paragrafo 1, lettere e) ed f), del presente articolo a specifici reati gravi. Lo Stato membro che intende avvalersi di tale limitazione notifica all'EPPO il pertinente elenco di specifici reati gravi in conformità dell'articolo 117».

La norma prevede che le misure investigative relative alla produzione di dati digitali (lett. c), alle intercettazioni di comunicazioni elettroniche (lett. e) e al tracciamento e rintracciamento di oggetti (lett. f) possano essere soggette a ulteriori condizioni e limitazioni previste dal diritto nazionale e, in particolare, che le ultime due misure menzionate in merito alle intercettazioni e al tracciamento siano limitate a ben precise figure di reato individuate in base alla loro gravità. È evidente come

il ricorso a misure particolarmente intrusive e pericolose per le libertà fondamentali (comunicazioni, movimento, autonomia informativa) possa trovare giustificazione e trovare il punto di equilibrio solo in relazione all'esigenza di investigare specifici reati gravi. Da un lato, la norma sgombera il campo dal rischio che le misure siano utilizzate non ai soli fini di indagine a seguito di *notitiae criminis* già acquisite e iscritte, quanto per ricercare notizie di reato[33].

Dall'altro, la previsione in esame, se da un lato consentirà di elevare la tutela prevista dal Regolamento al livello dei singoli ordinamenti, dall'altro lato non mancherà di creare ingiustificate disparità di trattamento derivante dai diversi livelli di gravità e di garanzia riconosciuti dai diversi ordinamenti. Pertanto, sarà interessante verificare in quale misura i diversi stati attueranno tale previsione o se non si renderà necessario uniformare lo statuto "degli specifici reati gravi" e soprattutto delle garanzie individuali secondo il principio di uguaglianza, attestando queste ultime ai livelli più elevati tra quelli previsti dai sistemi dei paesi membri.

Di particolare interesse ai fini della presente disamina, è il paragrafo 4 dell'art. 30 del Regolamento in quanto, prevedendo che «4. I procuratori europei delegati sono autorizzati a chiedere o a disporre, oltre alle misure di cui al paragrafo 1, qualsiasi altra misura del loro Stato membro che il diritto nazionale mette a disposizione dei procuratori in casi nazionali analoghi». La norma, introducendo una forma di sussidiarietà delle misure previste dai singoli ordinamenti, apre all'applicabilità delle ulteriori previsioni previste dai singoli ordinamenti nazionali. La norma completa la già nutrita faretra delle misure e strumenti di indagine informatica a disposizione degli inquirenti senza tuttavia prevedere appropriate e specifiche forme di garanzia e controllo sulla portata e l'uso di tali strumenti, essendo assolutamente insufficienti le garanzie procedurali previste dall'art. 41 del Regolamento. Anche a tal proposito sarà interessante osservare come verranno applicate le norme che, nell'ambito dei singoli ordinamenti, contemplano previsioni specifiche per i dati digitali, soprattutto relative alle modalità tecniche da osservare come previsto a seguito del recepimento della Convenzione di Budapest.

Infine, il paragrafo 5 dell'art. 30, prevede che «5. I procuratori europei delegati possono disporre le misure di cui ai paragrafi 1 e 4 soltanto qualora vi sia fondato motivo di ritenere che le misure specifiche in

[33] Sulle modalità di acquisizione della *notitia criminis* di reati informatici in ambito transnazionale, A. GAMMAROTA, *Lo scambio,* cit.

questione possano fornire informazioni o prove utili all'indagine, e qualora non sia disponibile alcuna misura meno intrusiva che consenta di conseguire lo stesso obiettivo. Le procedure e le modalità per l'adozione delle misure sono disciplinate dal diritto nazionale applicabile». La norma condiziona le misure esaminate a un duplice principio: un principio di rilevanza, per cui il ricorso alle misure è giustificato non per la ricerca di notizie di reato, né in funzione meramente perlustrativa bensì, e solo, ad indagine già avviata e per la ricerca di informazioni o prove utili all'indagine; un ulteriore principio di gradualità, per cui il ricorso alle misure intrusive è consentito solo ove lo stesso obiettivo di raccolta informazioni e prove non sia ugualmente fruttuoso ricorrendo a misure meno intrusive di quelle rassegnate.

Tuttavia, il principio di gradualità, per come formulato, solleva non poche perplessità. Infatti, è veramente arduo pensare che tale previsione possa favorire l'approccio basato prioritariamente sulle tecniche di investigazione analogica basato, ad esempio, sulle attività classiche di appostamento, pedinamento, osservazione e controllo (APOC), rispetto alla immediata ricerca e acquisizione di dati digitali. È invero altamente probabile che si verifichi il contrario e che quantomeno un discutibile senso di efficacia ed economicità delle investigazioni, unitamente all'endemica ristrettezza delle risorse disponibili, faccia prediligere l'immediata ricerca ed acquisizione di dati digitali dai quali trarre informazioni utili alle indagini. Inoltre, la mancata previsione di qualunque effetto invalidante o sanzionatorio conseguente al mancato rispetto dei criteri di priorità lascia prefigurare una sostanziale innocuità della norma, cosicché essa può essere sin d'ora relegata al rango di mera petizione di principio priva di incisive forme di controllo e di conseguenze quantomeno sul piano dell'inutilizzabilità.

L'unica forma di controllo è quella prevista dall'articolo 31, paragrafo 4 lett. c) in tema di Indagini transfrontaliere qualora il procuratore europeo delegato richieda assistenza al procuratore delegato dello Stato nel quale la misura in questione deve essere eseguita, ma quest'ultimo ritenga che «c) una misura alternativa, ma meno intrusiva, consenta di conseguire gli stessi risultati della misura assegnata»*;* in tal caso, scatta la procedura che coinvolge il procuratore europeo incaricato della supervisione e consulta il procuratore europeo delegato incaricato del caso per risolvere la questione a livello bilaterale e, a seguire, la procedura di risoluzione del conflitto prevista dai paragrafi 6, 7 e 8 dell'art. 31 del Regolamento.

7. Conclusioni

Il Regolamento EPPO costituisce un passo importante e necessario verso l'integrazione degli strumenti investigativi e giudiziari dell'Unione per attualmente limitata ad un ambito circoscritto all'ambito finanziario comune. Parimenti, la previsione di particolari strumenti di indagine in materia informatica è ineludibile nel momento storico in atto caratterizzato dall'affermazione delle tecnologie digitali proprie della società dell'informazione.

Tuttavia, la mancanza di uniformità tra gli ordinamenti nazionali richiamati costituisce un grave pericolo per il principio di uguaglianza. Tale rischio è accentuato negli ambiti normativi rassegnati e rientranti nello spettro di particolare interesse dell'Informatica forense: è evidente la lacuna propria del Regolamento in merito alle misure investigative e di indagine aventi ad oggetto le tecnologie e i dati digitali.

Inoltre, vi sono diverse norme che concretizzano il rischio di disuguaglianze tra ordinamenti nazionali nel trattamento giuridico e tecnico dei dati digitali a fini investigativi e di indagine.

Tali rischi sembrerebbero limitati ai soli casi di reati finanziari commessi ai danni dell'Unione ove superiori alle soglie indicate.

Tuttavia, appare più che prevedibile che l'EPPO costituisca l'embrione dell'organo inquirente europeo al quale verranno attribuite competenze molto più ampie quali, ad esempio, quelle per i reati di terrorismo, criminalità organizzata e transnazionale, tratta di esseri umani, armi, stupefacenti, frode e riciclaggio[34]. In tal caso, le problematiche evidenziate avranno una portata ed una ricorrenza molto più ampia di quella fin qui ipotizzata per i soli reati finanziari.

Appare quindi ineludibile quantomeno l'implementazione delle norme rassegnate del Regolamento EPPO con i criteri giuridici e tecnici previsti dalla Convenzione di Budapest in tema di trattamento dei dati digitali a fini forensi. L'operazione, avvantaggiata dalla medesima matrice europea e da un approccio specifico al problema del trattamento dei dati digitali in ambito investigativo e di indagine, costituirebbe un notevole passo in avanti verso l'attuazione del principio di uguaglianza, delle garanzie dei diritti fondamentali e della qualità della giurisdizione.

[34] Cfr. A. DAVOLI, cit.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643022
pp. 431-448 (gennaio 2022)

La gestione delle prove digitali in ambito europeo: un necessario connubio tra la tecnologia e la legge

Maria Angela Biasiotti[1], Sara Conti[1]

1. Introduzione

Negli ultimi anni, si assiste nel settore della giustizia ad un forte interessamento verso il tema dello scambio delle prove "*elettroniche/digitali*"[2]. Se da un lato l'uso delle tecnologie della società dell'informazione rappresenta un elemento fondamentale per il miglioramento dell'amministrazione della giustizia, dall'altro esso apre nuovi scenari e questioni delicate in tema di sicurezza dei dati e delle procedure[3]. L'utilizzo di strumenti informatici è essenziale per garantire un efficiente funzionamento dell'attività giurisdizionale: ciò si ripercuote in un effettivo accesso alla giustizia per i cittadini, in procedure più snelle e semplici in caso di violazione della legge e infine in una più stretta ed efficace cooperazione delle autorità giudiziarie nazionali tra di loro e tra i diversi paesi dell'Unione europea. La disponibilità di strumenti che utilizzano *web services* e sistemi di archiviazione elettronica, la possibilità di scambiare elettronicamente documenti e atti giuridici, nonché l'avvio dei processi telematici mirano sicuramente a supportare coloro che operano nel settore della giustizia, incrementando l'offerta di adeguati servizi per il cittadino e per un'efficiente e trasparente amministrazione della giustizia. Tuttavia, in tale contesto il settore della giustizia dei diversi Stati membri si è trovato fino ad oggi di fronte ad un frammentato panorama normativo in materia di scambio transnazionale delle prove elettroniche/digitali, caratterizzato da differenti approcci

[1] Maria Angela Biasiotti è Dirigente di ricerca dell'Istituto di Informatica Giuridica e Sistemi Giudiziari (IGSG) del CNR, Sara Conti è tecnologo dell'Istituto di Informatica Giuridica e Sistemi Giudiziari (IGSG) del CNR.

[2] L'accezione con cui l'espressione prova digitale/prova elettronica è utilizzata nel contributo sarà chiarita *infra* § 2.

[3] G. Peruginelli, S. Conti, *L'impatto del Regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale*, in Ciberspazio e diritto, 1/2018, p. 123.

nazionali, nonché da diverse procedure relative alla raccolta, gestione e conservazione delle prove stesse che comportano, ad esempio, attività autorizzate in uno Stato membro e non permesse in un altro[4].

Il presente contributo intende focalizzarsi proprio sul cammino della prova elettronica/digitale in Europa tracciando il percorso fatto, fino agli attuali strumenti che le autorità giudiziarie degli Stati membri hanno a loro disposizione per scambiarsi le prove stesse utilizzando la tecnologia.

2. La definizione di prova "elettronica/digitale"

In una dimensione transfrontaliera, considerando la mancanza di uniformità all'interno delle legislazioni penali degli Stati membri, diventa fondamentale avere una definizione comune e condivisa sul significato di prova elettronica e/o digitale e di come dovrebbe essere trattata nel contesto degli Stati membri dell'UE.

L'8 giugno 2017 la Commissione europea ha presentato ai ministri della Giustizia dell'UE una serie di opzioni pratiche per migliorare l'accesso transfrontaliero alle prove elettroniche. I ministri hanno chiesto alla Commissione di presentare proposte legislative concrete da attuarsi nel prossimo futuro.

«I nostri attuali strumenti di indagine non sono adatti al modo in cui funziona il mondo digitale», ha dichiarato Věra Jourová[5], «Questi strumenti funzionano ancora entro i limiti del principio di territorialità, che è in contrasto con la natura transfrontaliera dei servizi e dei flussi di dati. Di conseguenza, il lavoro degli investigatori è rallentato».

«Le nostre autorità di contrasto hanno bisogno degli strumenti giusti per combattere le forme gravi di criminalità, tra cui il terrorismo e la criminalità informatica», ha aggiunto Dimitris Avramopoulos[6], «L'accesso transfrontaliero alle prove è una condizione preliminare per completare con successo quasi tutte le indagini sulla criminalità informatica o sul terrorismo».

Il trattamento delle prove elettroniche, così come lo scambio delle stesse tra le autorità giudiziarie dei vari Stati membri dell'UE, si basano su criteri e procedure diverse e non armonizzate. Ciò che manca è un

[4] *Ibidem*, pp. 124-125.
[5] Commissaria per la Giustizia, i consumatori e la parità di genere dell'Unione Europea.
[6] Commissario per la Migrazione, gli affari interni e la cittadinanza dell'Unione Europea.

quadro comune europeo per guidare i legislatori nazionali, le forze dell'ordine e le autorità giudiziarie quando si occupano di trattamento e scambio di prove elettroniche[7].

Inoltre, l'aumento dell'uso della tecnologia e delle comunicazioni online ha prodotto un aumento dell'incidenza della criminalità informatica, e ha portato alla nascita di alcune nuove tipologie di fattispecie criminali[8]. Tuttavia, l'assunto per cui per i reati informatici i riscontri siano da ricercare nelle tracce digitali, mentre per i reati comuni gli elementi probatori siano da rinvenire fra le potenziali prove tradizionali, ormai non è più valido[9]. Le investigazioni nei casi di reati comuni si affidano sempre più sulla ricerca di elementi di prova digitali. Le prove digitali non sono più soltanto quelle prove che possono essere utilizzate nel processo penale a carico o discarico di un c.d. reato *cyber*, ma anche di un reato comune[10].

Oggi, potrebbe risultare arduo immaginare un crimine che non abbia una dimensione per così dire "elettronica/digitale". È diventata quindi di estrema importanza la necessità di sviluppare una definizione quantomeno uniforme e comune di prova elettronica. Una definizione di prova elettronica deve essere sufficientemente ampia da includere tutti i tipi di prove indipendentemente dalla loro origine. C'è una forte necessità di rendere uniforme lo scambio di prove elettroniche, nonché di armonizzare la gestione delle stesse all'interno di un quadro comune europeo. Sulla base di queste premesse, viene proposta qui la seguente definizione:

> La prova elettronica è un qualsiasi dato risultante dall'output di un dispositivo analogico e/o digitale che abbia valore probatorio e che sia stato generato da, elaborato da, memorizzato su o trasmesso da, qualsivoglia dispositivo elettronico. La prova digitale è quella prova elettronica che sia stata generata o convertita in un formato numerico[11].

[7] S. Avveduto, S. Conti, D. Luzi, L. Pisacane, *The Conceptual Representation of the "Electronic Evidence" Domain*. In: Biasiotti M., Mifsud Bonnici J., Cannataci J., Turchi F. (eds) *Handling and Exchanging Electronic Evidence Across Europe*. Law, Governance and Technology Series, vol 39, 2018, pp.163-188.

[8] M. A. Biasiotti, S. Conti, F. Turchi, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard*, in Cadoppi A., Canestrari S., Manna A., Papa M. (a cura di) Cybercrime. Diritto e Procedura Penale dell'Informatica, Utet Giuridica, 2019, p. 1645-1646.

[9] *Ibidem*.

[10] *Ibidem*.

[11] La definizione è stata elaborata nell'ambito del progetto europeo Evidence, *European Data Informatics Exchange Framework for Courts and Evidence*, finanziato dalla Commissione europea nell'ambito del Settimo Programma Quadro (Grant Agreement 608185).

La nozione proposta ed elaborata permette di ricomprendere nel suo ambito qualsiasi tipo di dato, indipendentemente dalla metodologia con cui è stato raccolto: in Internet, memorizzato su un computer, uno *smartphone*, un disco rigido separato, un CD-ROM, una chiavetta USB. Non c'è distinzione tra i dati creati analogici o digitalizzati e quelli nati digitalmente[12]. Inoltre, si tratta di una definizione che riesce ad abbracciare una nozione molto ampia di prova digitale: in quanto ricomprende sia le prove nate digitali ma anche quelle che, nel loro ciclo di vita, vengono successivamente trasformate e poi memorizzate o scambiate in formato digitale[13].

Questa nozione ampia ben si presta ad essere utilizzata anche in contesti transnazionali. Infatti, è ormai evidente che la presenza della prova digitale non è correlata quasi mai alla giurisdizione territoriale di un determinato Paese dove il presunto reato è stato commesso o dove è in corso l'attività investigativa. Si assiste sempre di più alla instaurazione di processi penali che travalicano i confini nazionali, dove la necessità di acquisire prove anche di natura digitale non si limita al territorio di un determinato Stato.

3. La normativa europea in materia di scambio transnazionale delle prove: l'Ordine europeo di investigazione (OEI)

L'obiettivo di realizzare un quadro normativo europeo organico in materia di scambio della prova elettronica/digitale ha origine dall'esigenza di raff orzare la cooperazione giudiziaria in materia penale e fa riferimento principalmente alla nuova frontiera aperta dalla Direttiva relativa all'Ordine Europeo di Indagine (OEI)[14].

Quest'ultimo riveste un'importanza fondamentale in relazione proprio alla raccolta delle prove in ambito penale e, quindi, anche delle prove digitali. La direttiva mira a sostituire il vecchio quadro esistente

[12] Sotto questo profilo si possono ricomprendere nella definizione di "prova elettronica" anche le immagini scansionate. Inoltre, nella definizione attuale, qualsiasi prova fisica e analogica, che una volta è stata digitalizzata (ad esempio l'immagine inviata via fax e poi stampata di nuovo) è considerata prova elettronica.

[13] Si veda anche per un approfondimento la tesi di dottorato S. Conti, *Profili giuridici e tecnici dello scambio transnazionale delle prove digitali nei processi penali*, Università degli studi di Firenze, Dottorato in Ingegneria dell'Informazione, ciclo XXXII, 2016-2019, p. 19. https://flore.unifi.it/retrieve/handle/2158/1211795 /525184/ContiSara_PHDTesi_Definitivo.pdf.

[14] Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale.

per l'acquisizione delle prove: ad esempio, la disciplina introdotta dalla Decisione quadro 2003/577/GAI[15] risultava frammentaria essendo relativa soltanto all'esecuzione nell'Unione europea dei provvedimenti di blocco dei beni o di sequestro probatorio.

La decisione rispondeva soltanto alla «necessità dell'immediato riconoscimento reciproco dei provvedimenti intesi a impedire atti di distruzione, trasformazione, spostamento, trasferimento o alienazione di prove solo però con riferimento alla fase di blocco o sequestro»[16].

Tuttavia, poiché un provvedimento di blocco o di sequestro deve essere accompagnato da una distinta richiesta di trasferimento della fonte di prova nello Stato che emette il provvedimento (lo "Stato di emissione") in conformità delle norme applicabili all'assistenza giudiziaria in materia penale, ne derivava una procedura in due fasi che comprometteva l'efficienza di tale strumento[17].

Inoltre, tale regime coesisteva con gli strumenti tradizionali di cooperazione giudiziaria quindi le autorità competenti se ne avvalevano raramente nella pratica.

L'OEI rappresenta invece uno strumento innovativo, congegnato proprio per essere l'unico strumento da utilizzare per l'acquisizione e la circolazione delle prove in ambito europeo relative a procedimenti penali di rilevanza transfrontaliera. Le disposizioni di attuazione della direttiva dovevano essere adottate dagli Stati membri entro il 22 maggio 2017. Ad oggi tutti gli Stati membri hanno adottato misure di recepimento, tranne l'Irlanda e la Danimarca[18].

L'OEI dovrebbe facilitare la cooperazione giudiziaria tra Stati membri, introducendo per la prima volta il principio della disponibilità di misure investigative, dando la possibilità all'autorità di un Paese di richiedere all'autorità di un altro Paese che venga svolta una vera e propria indagine, con eventuale acquisizione di elementi di prova[19].

[15] Decisione quadro 2003/577/GAI del Consiglio, del 22 luglio 2003, relativa all'esecuzione nell'Unione europea dei provvedimenti di blocco dei beni o di sequestro probatorio, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32003F0577&from=IT.

[16] S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in Informatica e diritto, 2015, n. 1-2, p. 161.

[17] M. A. Biasiotti, S. Conti, F. Turchi, La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard, *cit.*

[18] Si veda, per quanto riguarda l'attuazione nei vari Stati membri della direttiva sull'OEI: https://eur-lex.europa.eu/legal-content/IT/NIM/?uri=CELEX:32014L0041&qid=1569499604719.

[19] Si veda per un approfondimento la tesi di dottorato S. Conti, *Profili giuridici e tecnici dello scambio transnazionale delle prove digitali nei processi penali*, Università degli studi di Firenze, Dottorato in Ingegneria dell'Informazione, ciclo XXXII, 2016-2019, p. 19 e ss.

Si tratta, quindi, di uno strumento processuale a disposizione dell'autorità giudiziaria per la ricerca della prova e la circolazione probatoria oltre i confini giurisdizionali di ciascuno Stato membro dell'Unione Europea.

Con la Direttiva 2014/41/UE, quindi, viene creato un "sistema globale di acquisizione delle prove aventi dimensione transfrontaliera"[20]: con l'ordine europeo di indagine lo Stato di emissione ottiene che venga compiuto in un altro Stato membro (c.d. di esecuzione) un determinato atto di indagine senza che siano necessarie ulteriori formalità e in modo veloce ed efficace[21].

A questo proposito, l'art. 9 della direttiva stabilisce che "l'autorità di esecuzione riconosce un ordine europeo di indagine, trasmesso conformemente alle disposizioni della presente direttiva, senza imporre ulteriori formalità e ne assicura l'esecuzione nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione"[22]. E l'art. 12 continua indicando che "l'autorità di esecuzione compie l'atto di indagine senza ritardo".

In definitiva, l'obiettivo della Direttiva in esame è quello di rendere più veloci ed efficaci le investigazioni transfrontaliere, mettendo a disposizione degli Stati membri uno strumento in grado di garantire la speditezza dei procedimenti penali e al contempo in grado di far fronte alla volatilità dei dati digitali che possono venire in rilievo durante un'attività di indagine.

Più nello specifico, dal punto di vista della procedura, l'OEI si concretizza in una particolare decisione giudiziaria emessa o convalidata

https://flore.unifi.it/retrieve/handle/2158/1211795/525184/ContiSara_PHDTesi_Definitivo.pdf.

[20] Considerando n. 6 della Direttiva 2014/41: "Nel programma di Stoccolma, adottato dal Consiglio europeo del 10-11 dicembre 2009, il Consiglio europeo ha considerato di perseguire ulteriormente l'istituzione di un sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera, basato sul principio del riconoscimento reciproco. Il Consiglio europeo ha rilevato che gli strumenti esistenti nel settore costituiscono una disciplina frammentaria e che è necessaria una nuova impostazione che, pur ispirandosi al principio del riconoscimento reciproco, tenga conto altresì della flessibilità del sistema tradizionale di assistenza giudiziaria. Il Consiglio europeo ha pertanto chiesto la creazione di un sistema globale in sostituzione di tutti gli strumenti esistenti nel settore, compresa la Decisione quadro 2008/978/GAI del Consiglio, che contempli per quanto possibile tutti i tipi di prove, stabilisca i termini di esecuzione e limiti al minimo i motivi di rifiuto".

[21] S. Conti, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, *cit*., p.160.

[22] *Ibidem*, p. 162.

da un'autorità competente di uno Stato membro ("Stato di emissione"), che ordina all'autorità giudiziaria di un altro Stato membro ("Stato di esecuzione") di compiere uno o più atti di indagine specifici al fine di acquisire delle prove o per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione (art. 1). A titolo esemplificativo si può trattare di sequestri, intercettazioni ambientali o telefoniche, o acquisizione diretta di documentazione a valore probatorio[23].

L'OEI deve essere emesso da un organo giurisdizionale o da un magistrato inquirente, oppure deve essere convalidato da questi ultimi, prima della trasmissione all'autorità di esecuzione (art. 2). L'OEI è trasmesso dall'autorità di emissione all'autorità di esecuzione con ogni mezzo che consenta di conservare una traccia scritta e che permetta allo Stato di esecuzione di stabilirne l'autenticità (art. 7).

Il riconoscimento e l'esecuzione dell'OEI avvengono senza alcuna ulteriore formalità: pertanto, l'autorità competente dello Stato di esecuzione è tenuta ad adottare immediatamente tutte le misure necessarie, secondo le stesse modalità che sarebbero osservate qualora l'atto di indagine fosse stato disposto da un'autorità dello Stato di emissione.

In conclusione, l'OEI è uno strumento con il quale si intende introdurre a livello europeo un quadro giuridico unico e completo per la cooperazione in materia penale, in particolare in relazione allo scambio delle prove (comprese quelle elettroniche/digitali).

Tuttavia, molteplici sono i profili di complessità di questa normativa, che hanno alimentato ampi dibattiti a livello europeo e nazionale.

Ad esempio, l'aumento delle misure investigative intrusive attuabili oltre i confini nazionali, quali ad esempio l'intercettazione delle telecomunicazioni, richiede un quadro normativo che contempli anche modalità e strumenti rivolti alla protezione dei dati personali che possono venire in rilievo quando viene data esecuzione all'OEI. Occorre, in altre parole, che la riservatezza dei dati personali degli individui coinvolti nelle procedure di OEI sia rispettata e sia garantita al tempo stesso l'integrità dei medesimi dati.

[23] M. A. Biasiotti, S. Conti, F. Turchi, *La raccolta transnazionale della prova digitale*, cit., p. 1641.

4. La nuova legislazione dell'UE sull'acquisizione di prove elettroniche

Il quadro delineato sopra mostra, al di là della necessità sentita a livello europeo di armonizzare le procedure di cooperazione in materia giudiziaria penale, come l'utilizzo delle tecnologie informatiche nel settore della giustizia si stia affermando in maniera sempre più pervasiva e ampia. In un documento del giugno 2016[24], il Consiglio dell'Unione europea ha adottato conclusioni per migliorare l'efficienza della giustizia penale laddove si tratti di reati commessi con l'uso di strumenti elettronici e di prove elettroniche da presentare in giudizio.

In particolare, in questo contesto, la proposta di uno strumento per l'accesso transfrontaliero alle prove elettroniche nell'UE rappresenta una questione urgente, data la sua importanza cruciale nella lotta contro il terrorismo, la criminalità informatica e la criminalità transnazionale nella sua interezza.

La maggior parte di tutte le indagini penali oggi include una richiesta transfrontaliera di accesso a prove elettroniche, come testi, e-mail o app di messaggistica. La Commissione europea ha proposto nuove norme il cui intento dovrebbe essere quello di rendere più facile e veloce per le autorità di polizia e giudiziarie di un determinato Stato accedere alle prove elettroniche che dovrebbero essere utilizzate in un processo in altro Stato.

Ad aprile 2018 la Commissione, quindi, ha presentato una proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018) 225 final)[25] e 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)[26]. Le due proposte sono tra loro complementari. L'obbiettivo complessivo della Commissione dovrebbe essere quello di migliorare la cooperazione tra autorità negli Stati membri e prestatori di servizi, compresi quelli che hanno sede fuori dall'UE.

[24] European Council of the European Union, 9.6.2016, "Council conclusions on improving criminal justice in cyberspace", http://www.consilium.europa.eu/en/press/press-releases/2016/06/ 09-criminal-activities-cyberspace.

[25] La proposta di regolamento è consultabile su https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0005.02/DOC_1&format=PDF.

[26] La proposta di direttiva è consultabile https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018PC0226&from=IT.

Ai fini del presente articolo, la proposta di regolamento rappresenta maggior interesse, in quanto come si evince dal considerando 15 della Relazione alla proposta stessa[27], il nuovo regolamento stabilirà «le norme in base alle quali, in un procedimento penale, un'autorità giudiziaria competente nell'Unione europea può ordinare a un prestatore di servizi, che offre servizi nell'Unione, di produrre o conservare informazioni elettroniche che possono servire come prova in tribunale».

In altre parole, l'operatività in futuro ad esempio di un ordine di produzione consentirà a un'autorità giudiziaria di uno Stato membro di ottenere prove elettroniche (quali e-mail, sms o messaggi nelle app, nonché informazioni per identificare l'autore del reato come primo passo) direttamente da un prestatore di servizi o dal suo rappresentante legale in un altro Stato membro, che saranno obbligati a rispondere entro 10 giorni, ed entro 6 ore in caso di emergenza (rispetto a un massimo di 120 giorni per l'ordinanza di indagine europea esistente o a una media di 10 mesi per una procedura di assistenza giudiziaria reciproca).

È della massima importanza individuare dove è stabilito il prestatore di servizi, in quanto la proposta di regolamento dovrebbe applicarsi in generale ai prestatori di servizi che offrono servizi nell'Unione e gli ordini previsti possono essere emessi solo per i dati relativi ai servizi offerti nell'Unione.

Più specificamente, i fornitori di servizi che dovrebbero rientrare nell'applicazione del presente regolamento, in quanto sono principalmente rilevanti per la raccolta di informazioni elettroniche nei procedimenti penali, sono «fornitori di servizi di comunicazione elettronica e fornitori specifici di servizi della società dell'informazione che facilitano l'interazione tra gli utenti» (considerando 16 della relazione)[28].

La questione chiave che emerge da questa nuova iniziativa legislativa è se l'articolo 82, paragrafo 1, del Trattato sul funzionamento

[27] Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM(2018)0225 C8-0155/20182018/0108(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Birgit Sippel, Bruxelles, 11.12.2020.
https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf.

[28] I fornitori di servizi di comunicazione elettronica sono definiti nella Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio. Includono comunicazioni interpersonali come voice-over-IP, messaggistica istantanea e servizi di posta elettronica. In generale, l'ordinanza di produzione e conservazione può essere emessa nei confronti di fornitori di servizi di comunicazione elettronica, social network, mercati online, altri fornitori di servizi di hosting e fornitori di infrastrutture Internet quali indirizzi IP e nomi di dominio, o nei confronti dei loro rappresentanti legali laddove esistano.

dell'Unione europea (TFUE) possa rappresentare la base giuridica adeguata per uno strumento che consenta alle autorità giudiziarie di uno Stato membro di obbligare le imprese private operante nel settore delle tecnologie dell'informazione all'interno dell'UE, per conservare e/o produrre prove elettroniche, senza alcun corrispettivo della giurisdizione in cui tale impresa ha sede e del luogo in cui i dati sono conservati.

Più specificamente, l'articolo 82, paragrafo 1 TFUE, si basa sul riconoscimento reciproco delle decisioni giudiziarie: un'autorità giudiziaria dello Stato di emissione può imporre direttamente obblighi a una persona giuridica in un altro Stato membro, senza il previo intervento di un'autorità giudiziaria in tale altro Stato membro[29].

Tale base giuridica può essere applicata ai meccanismi di cui al regolamento proposto. L'articolo 82, paragrafo 1 TFUE, infatti non fa altro che garantire il riconoscimento reciproco delle decisioni con cui l'autorità giudiziaria dello Stato di emissione si rivolge a una persona giuridica in un altro Stato membro e le impone obblighi, senza il previo intervento dell'autorità giudiziaria di tale altro Stato membro. L'ordine europeo di produzione o di conservazione può eventualmente comportare l'intervento dell'autorità giudiziaria dello Stato di esecuzione, ove necessario, per far eseguire la decisione stessa.

La nuova proposta non coinvolge direttamente le autorità di polizia o giudiziarie dello Stato membro in cui ha sede il prestatore di servizi oggetto della richiesta. La proposta cerca invece di attribuire alle autorità di polizia o giudiziarie di uno Stato membro la competenza extraterritoriale per rivolgersi direttamente a un soggetto privato in un altro Stato membro[30].

Le categorie di dati che possono essere richiesti e ottenuti con un ordine di produzione europeo dalle autorità competenti comprendono i dati degli abbonati, i dati di accesso, i dati relativi alle operazioni e/o transazioni (comunemente denominati congiuntamente "dati non relativi al contenuto") e i dati relativi ai contenuti memorizzati. Entrambe

[29] L'articolo 82, paragrafo 1, stabilisce che possono essere adottate, secondo la procedura legislativa ordinaria, misure volte a stabilire norme e procedure volte a garantire il riconoscimento in tutta l'Unione di tutte le forme di sentenze e decisioni giudiziarie. Possono inoltre essere adottate misure per facilitare la cooperazione tra le autorità giudiziarie o autorità equivalenti degli Stati membri in relazione ai procedimenti penali e all'esecuzione delle decisioni.

[30] Recitando 19 della Proposta di Regolamento.

le ordinanze, di produzione e di conservazione, possono essere utilizzate solo in procedimenti penali.

Ai sensi dell'articolo 3 della proposta di regolamento "L'ordine di produzione europeo e l'ordinanza europea di conservazione sono misure investigative che possono essere emesse solo nell'esecuzione di indagini penali o procedimenti penali per reati concreti. Il collegamento a un'indagine concreta la distingue dalle misure preventive o dagli obblighi di conservazione dei dati previsti dalla legge e garantisce l'applicazione dei diritti procedurali applicabili ai procedimenti penali. La competenza ad aprire indagini per un reato specifico è quindi un prerequisito per utilizzare il Regolamento".

Inoltre, ai sensi dell'articolo 5 della proposta di regolamento "L'ordine di produrre dati relativi agli abbonati o dati relativi agli accessi può essere emesso per qualsiasi reato. Per i dati relativi alle operazioni o al contenuto dovrebbero essere soddisfatti requisiti più rigorosi onde tener conto della natura più sensibile di tali dati e del corrispondente maggiore impatto dell'ordine rispetto ai dati relativi agli abbonati o agli accessi".

La natura di tali tipologie di dati, comporta che l'ordine possa essere emesso solo in relazione a quelle fattispecie di reato che comportano una pena detentiva della durata massima di almeno tre anni: la fissazione di una soglia consente un approccio più proporzionato, insieme a una serie di altre condizioni e garanzie che assicurano il rispetto della proporzionalità e dei diritti dei soggetti coinvolti.

L'ordine europeo di conservazione è soggetto a condizioni simili a quelle cui è soggetto l'ordine europeo di produzione. Più nello specifico, il suo obiettivo è impedire la rimozione, la cancellazione o la modifica di determinati dati in quelle situazioni in cui potrebbe occorrere più tempo per ottenere la produzione di tali dati, ad esempio quando saranno usati i canali della cooperazione giudiziaria. A differenza dell'ordine di produzione non è prevista per l'ordine di conservazione alcuna soglia correlata alla pena per il reato indagato.

Questi due strumenti consentiranno alle autorità giudiziarie e alle autorità di contrasto di condurre in modo completo le indagini penali, non sostituendosi all'OEI ma integrandosi ed aggiungendosi all'emanazione dello stesso. In altre parole, l'OEI, insieme agli ordini di produzione e conservazione, fornirà norme sovranazionali comuni che consentiranno anche l'accesso ai dati elettronici e la raccolta di informazioni elettroniche da utilizzare successivamente come prove in un processo penale.

5. Stato dell'arte delle politiche e iniziative delle Istituzioni europee per il rafforzamento della cooperazione giudiziaria in materia penale

Negli ultimi anni a livello europeo sono state molte le iniziative e le politiche adottate, volte alla creazione di un quadro comune in materia di cooperazione giudiziaria penale ed al rafforzamento degli strumenti già esistenti per lo scambio transnazionale delle prove elettroniche nei processi penali.

Le Istituzioni europee, coinvolte a vario titolo e con varie competenze nel rafforzamento della cooperazione giudiziaria in materia penale, hanno concretamente iniziato a collaborare, già da alcuni anni, in gruppi di lavoro, sulle modalità che possono essere adottate per consentire lo scambio delle prove a livello europeo con l'intento di facilitare anche l'operatività e il successo dell'OEI[31].

Il Consiglio europeo, nelle conclusioni di un suo documento del 2016[32], aveva delineato tre potenziali azioni per il miglioramento della giustizia penale e della cooperazione giudiziaria in Europa, quando vengono in rilievo reati informatici o reati comuni commessi con l'utilizzo di strumenti informatici:

- semplificazione delle procedure di assistenza giudiziaria reciproca e, ove applicabili, delle procedure di mutuo riconoscimento reciproco, attraverso l'utilizzo di moduli standardizzati e strumenti elettronici anch'essi standardizzati;
- miglioramento della cooperazione con i fornitori di servizi attraverso lo sviluppo e l'uso di moduli e strumenti allineati per la richiesta di specifiche categorie di dati;
- avvio di un processo di riflessione su possibili criteri di collegamento per la competenza esecutiva dell'autorità giudiziaria[33].

[31] M. A. Biasiotti, S. Conti, F. Turchi, *La raccolta transnazionale della prova digitale*, *cit*., p. 1648.

[32] Consiglio europeo, Conclusioni del Consiglio sul miglioramento della giustizia penale, 9 giugno 2016, in www.consilium.europa.eu/it/press/press-release/2016/06/09-criminal-activities-cyberspace.

[33] M. A. Biasiotti, S. Conti, F. Turchi, *La raccolta transnazionale della prova digitale*, *cit*., p. 1648, p. 1649.

Proprio sulla scorta di tale discussione la Commissione europea ha, quindi, iniziato a promuovere la realizzazione di un "Secure online portal"[34] al fine di consentire lo scambio transnazionale delle prove elettroniche. Ciò avrebbe dovuto rappresentare un concreto passo verso la creazione di un quadro europeo comune e sicuro per tale scambio in contesti transfrontalieri.

A tale scopo, sono stati nominati due gruppi di esperti: un "Expert group – on Reliable electronic platform MLA[35] and EIO requests"[36] e l'"Horizontal Working Party on Cyber Issues and JHA Counsellors"[37], volti entrambi a porre le basi per la creazione di tale piattaforma sicura.

In particolare, i lavori del primo gruppo hanno mirato a definire prioritariamente la natura che una piattaforma per lo scambio delle prove digitali dovrebbe avere per poter essere considerata sicura, affidabile e di non difficile gestione da parte della Commissione e degli Stati membri[38].

In particolare, due sono state le alternative proposte, ovvero realizzazione di una piattaforma a livello:

- centralizzato, e quindi direttamente gestito dalla Commissione europea a cui tutti gli Stati membri avrebbero dovuto connettersi e collegare i propri database nazionali; oppure
- decentralizzato, in cui gli Stati dialogano direttamente senza alcun intervento di gestione delle richieste e della trasmissione da parte della Commissione europea, mantenendo localmente i database nazionali.

[34] The e-Evidence Digital Exchange System e il suo front-end Reference Implementation Portal (e-EDES-RI). Nel febbraio 2018 lo sviluppo del sistema è stato completato e nei successivi due anni molti degli Stati membri hanno implementato il sistema messo a disposizione dalla Commissione Europea. https://data.consilium.europa.eu/doc/document/ ST-6429-2020-REV-1/en/pdf.

[35] Si tratta delle misure di Mutual Legal Assistance, ovvero delle misure di cooperazione giudiziaria in materia penale tra Stati membri.

[36] Principles and Options for an e-evidence exchange platform - Discussion Paper prepared by DG Justice and Consumers for the Expert Group on e-evidence, non pubblicato.

[37] Il gruppo di esperti è un organo consultivo che può essere istituito dalla Commissione o dai suoi servizi per ottenere consulenze e conoscenze specialistiche, è composto da membri del settore pubblico e/o privato che si riunisce più di una volta. I gruppi di esperti della Commissione sono soggetti alle regole orizzontali stabilite con decisione della Commissione C (2016)3301, che deve essere letta insieme alla comunicazione della Commissione C(2016)3300.

[38] M. A. Biasiotti et al., *La raccolta transnazionale della prova digitale*, *cit*., pp. 1648-1649.

Per quanto riguarda il secondo gruppo di lavoro sopra citato, che si occupa in modo specifico dei "Cyber Issues", particolare attenzione è stata posta dai vari esperti proprio sul tema specifico dello scambio della prova elettronica.

In una riunione tenutasi a Bruxelles il 20 gennaio 2017 il gruppo di esperti ha ribadito che il rafforzamento della cooperazione in materia penale rimane il fattore chiave per la lotta contro i reati informatici e il terrorismo e che questa passa necessariamente anche attraverso tre canali distinti ma strettamente collegati tra loro:

- incremento della consapevolezza degli strumenti a disposizione per la realizzazione di uno scambio sicuro delle prove digitali,
- aumento della reciproca fiducia tra Stati membri attraverso la predisposizione di procedure comuni e uniformi, infine
- realizzazione di sistemi che consentano lo scambio sicuro e affidabile delle informazioni e delle prove digitali tra le forze di polizia, le autorità giudiziarie e gli altri attori coinvolti nei processi penali.
- Questo gruppo ha sottolineato, in modo particolare, l'importanza strategica proprio in tema di prove digitali, di creare sinergie e sviluppare la cooperazione fra i vari stakeholders coinvolti, tra i quali un ruolo prioritario viene riconosciuto agli ISPs, e di costruire, insieme a questi, seguendo un metodo condiviso, la base normativa e il dialogo necessario a generare e aumentare la tanto auspicata fiducia reciproca.

In questo contesto si inserisce la struttura della piattaforma, il sistema di scambio digitale "e-Evidence Exchange System – eEDES" che la Commissione sta realizzando: un sistema decentralizzato di scambio sicuro tra le autorità competenti degli Stati membri, che dovrebbe consentire loro di comunicare rapidamente, efficacemente ed in modo sicuro nel contesto dell'EIO e delle MLA nel campo del diritto penale. In linea con le politiche europee sulla sicurezza e al fine di combattere efficacemente il crimine informatico, il sistema dovrebbe mirare a migliorare le possibilità per le autorità giudiziarie di diversi Stati membri di scambiare prove digitali tra loro nell'ambito dei processi penali. In altre parole, tale piattaforma dovrebbe facilitare e accelerare la cooperazione giudiziaria anche in casi particolarmente complicati, legati ad

esempio al terrorismo e alla criminalità organizzata, situazioni nelle quali la rapidità delle indagini potrebbe rappresentare un elemento fondamentale per la risoluzione del caso.

Per quanto riguarda lo sviluppo delle caratteristiche tecniche della piattaforma, è stato concordato nelle varie consultazioni con gli Stati membri che la piattaforma dovrà essere decentralizzata, utilizzando il sistema e-CODEX [39]come strumento per la trasmissione sicura dei dati. Le specifiche funzionali della piattaforma sono state adottate a febbraio 2018 e sono in corso lavori sull'implementazione della piattaforma stessa. Il sistema è entrato in funzione a fine 2019 ma ancora non è stato implementato da tutti gli Stati membri.

6. Stato dell'arte delle iniziative progettuali a livello europeo per il rafforzamento della cooperazione giudiziaria in materia penale

A livello europeo il crescente interesse per la tematica dello scambio transnazionale delle prove digitali è dimostrato anche dai numerosi progetti che sono stati finanziati direttamente dalla Commissione e che cercano di dare soluzioni concrete al dibattito sul tema.

Alcuni di questi progetti si sono occupati direttamente della tematica oggetto del presente lavoro, mentre altri sono stati incentrati su tematiche connesse: ad esempio la semplificazione delle procedure che consentono lo scambio delle prove digitali (c.d. e-MLA).

Tra i vari progetti europei merita particolare attenzione Evidence (European Informatics Data Exchange framework for Courts and Evidence), finanziato dalla Commissione europea nell'ambito del Settimo Programma Quadro, iniziato nel marzo 2013 e conclusosi nell'ottobre 2016. Il progetto si è posto proprio in linea con le iniziative europee sopra descritte, ovvero si è posto quale obiettivo finale la creazione di un comune quadro in materia di scambio transnazionale delle prove elettroniche.

Le attività di ricerca svolte nell'ambito del progetto Evidence si sono anche incentrate sull'obiettivo di creare una rete stabile di esperti forensi e di favorire la comunicazione tra i principali attori del processo penale (ad esempio, autorità giudiziarie, forze di polizia, ecc.) in modo

[39] Il sistema e-CODEX consente l'interoperabilità tra i sistemi informatici utilizzati dalle autorità giudiziarie di diversi Paesi. Permette ai diversi sistemi nazionali di giustizia elettronica di essere interconnessi in modo decentralizzato, al fine di espletare le procedure transfrontaliere in materia civile e penale. https://www.e-codex.eu.

da stimolare un dibattito continuo e mirato, e al tempo stesso uno scambio di idee, sui principali temi di interesse oggetto del progetto.

Altro progetto rilevante in materia, anche se non direttamente finalizzato allo scambio delle prove digitali, è il progetto e-CODEX finanziato per realizzare un'infrastruttura realizzata per migliorare l'accesso dei cittadini e delle imprese alle procedure giudiziarie transnazionali fra diversi Stati membri dell'Unione europea.

Proprio l'infrastruttura creata nell'ambito di e-CODEX potrebbe rappresentare lo strumento idoneo per lo scambio della prova digitale in Europa. Il progetto e-CODEX, per raggiungere l'obiettivo sopra descritto, ha proposto e realizzato una serie di soluzioni creando un'infrastruttura per la trasmissione e lo scambio di informazioni nel contesto di procedure giudiziarie transnazionali:

- *e-Delivery*, per la trasmissione di informazioni in modo sicuro e affidabile attraverso le frontiere;
- *e-Signature,* per la firma elettronica dei documenti e la convalida delle firme elettroniche;
- *e-Document*, per lo scambio di documenti comuni; infine,
- e-*Identity*, per l'identificazione dei soggetti tramite carte d'identità nazionali[40].

Il progetto e-Codex ha concentrato i propri sforzi di ricerca sulla realizzazione di una tale infrastruttura per la comunicazione delle informazioni relativa alla richiesta di mutua assistenza giudiziaria. Tuttavia, l'infrastruttura realizzata nell'ambito del progetto e-CODEX rappresenta un'ottima base di partenza per la realizzazione di un sistema sicuro ed uniforme di scambio anche delle prove digitali raccolte ed ottenute attraverso l'OEI.

In questo senso, la Commissione europea si è mossa avendo finanziato anche il progetto Evidence2e-CODEX (Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe).

Come si può evincere già dal titolo, il progetto mira, nello specifico contesto delle procedure MLA e dell'OEI, a sviluppare un *case study* per lo scambio sicuro ed affidabile delle prove digitali in Europa mettendo insieme l'infrastruttura veloce, sicura e affidabile realizzata dal

[40] Maria Angela Biasiotti, *Presente e futuro dello scambio della prova digitale in Europa, in Informatica e diritto*, 1-2/2015, p. 49.

progetto e-CODEX con quanto proposto dal progetto EVIDENCE sull'adozione di un linguaggio formale di scambio[41]. Questo caso di studio dovrebbe rappresentare un *building block* verso la realizzazione di una piattaforma sicura per lo scambio transnazionale delle prove digitali.

In parallelo al progetto sopra descritto, la Commissione ha anche finanziato EXEC (Electronic Xchange of e-Evidences with e-CODEX). Il progetto, terminato a febbraio 2020, ha avuto come obiettivo quello di consentire agli Stati membri partecipanti di scambiare gli ordini di indagine europei e relative prove digitali, completamente in formato elettronico attraverso soluzioni di back-end nazionali esistenti o in alternativa, attraverso l'implementazione di soluzioni *reference* fornite dalla Commissione europea[42]. L'infrastruttura di scambio per facilitare la consegna elettronica di OEI e prove digitali collegate è quella realizzata dal Progetto e-Codex basata su e-CODEX Building Blocks.

Il progetto e-MLA (2016-2019), coordinato dall'Interpol, ha l'obiettivo di modernizzare e razionalizzare i processi di trasmissione delle richieste di MLA nel quadro delle procedure esistenti a livello dell'Unione europea e del Consiglio d'Europa (CoE).

L'iniziativa progettuale mira senza dubbio ad aumentare l'efficacia della cooperazione giudiziaria in materia penale. Infatti, obiettivo ultimo del progetto è proprio la realizzazione di uno strumento elettronico molto pratico che permetta alle autorità competenti di scambiare informazioni correlate a procedure di assistenza reciproca, in conformità con gli impegni dei trattati esistenti, con la legislazione nazionale e con le altre iniziative a livello europeo sul tema.

A livello europeo, ma anche a livello dei singoli Stati membri, è sempre più pressante l'esigenza di creare un'infrastruttura comune di scambio delle prove digitali in ambito penale tra paesi diversi. E i progetti europei sul tema hanno contribuito, e contribuiscono, a creare i *building blocks* per la creazione di tale infrastruttura sicura.

[41] Si veda a tale proposito https://evidence2e-codex.eu.

[42] Si tratta del progetto e-Evidence della Commissione europea per la creazione di un'infrastruttura per lo scambio delle prove digitali in contesti penali transnazionali.

7. Conclusioni

L'idea da cui partire nella realizzazione dello scambio è passare dalla teoria alla pratica e iniziare a sperimentare quanto realizzato fino ad ora a livello di progetti europei, provando concretamente a implementare lo scambio, generando quella consapevolezza necessaria a rendere concrete, efficaci e operative le strategie introdotte fino ad ora[43].

Occorre quindi iniziare a verificare se quello che è stato implementato e pensato fino ad ora "sulla carta" possa veramente funzionare calato nella realtà concreta. A tale proposito sembra davvero utile lo sviluppo di un caso di studio per lo scambio di prove digitali, proposto nel progetto Evidence2e-CODEX, per utilizzare l'infrastruttura veloce, sicura e affidabile realizzata dal progetto e-CODEX con quanto proposto a livello progettuale sull'adozione di un linguaggio formale per la rappresentazione dei metadati per lo scambio.

I progetti europei da cui partire esistono, la volontà delle istituzioni europee di riferimento c'è, la consapevolezza da parte degli Stati membri sulla necessità di cooperare effettivamente nelle materie penali è notevolmente maturata, la crescente esigenza da parte delle forze dell'ordine è ormai chiara e nitida: non resta quindi che iniziare a lavorare concretamente sullo scambio effettivo delle prove in Europa e costruire quella piattaforma operativa che consentirà lo scambio sicuro ed affidabile di prove elettroniche.

[43] M. A. Biasiotti, S. Conti, F. Turchi, *La raccolta transnazionale della prova digitale*, *cit*., p. 1657.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643023
pp. 449-467 (gennaio 2022)

Sulla Procura Europea. Profili di Informatica giudiziaria

Silvia Moffa[1]

1. Introduzione

Mentre si realizza il presente contributo – una vera e propria "diretta" su un fenomeno dalla dirompente risonanza mediatica – la Procura Europea si sta materializzando. Infatti EPPO (acronimo inglese di *European Public Prosecutor Office*) dal 1 giugno 2021 ha assunto le funzioni giurisdizionali previste dal Regolamento (UE) 2017/1939 adottato il 12 ottobre 2017 ed entrato in vigore il 20 novembre successivo[2]. Il decreto legislativo n. 9 del 2 febbraio 2021[3] ha adeguato la normativa nazionale al Regolamento citato. Con questo contributo ci si prefigge di analizzare la normativa, raffrontandola con la concreta evoluzione che EPPO sta assumendo con particolare riferimento ai sistemi informativi utilizzati per la gestione delle notizie di reato. Sarà pertanto necessario, ai fini di una ricerca attendibile, non limitarsi all'analisi del dato normativo ma raffrontarlo con le osservazioni dei protagonisti[4] che

[1] Responsabile amministrativo Ufficio Registro Generale Procura della Repubblica di Bologna. Dottore di ricerca in Diritto e nuove tecnologie, Università di Bologna.

[2] Il Regolamento è articolato in 120 Articoli raccolti in 11 Capi: Capo I: Oggetto e definizioni, Capo II*:* Istituzioni, Compiti e principi di base dell'EPPO, Capo III: Status, struttura e organizzazione dell'EPPO, Capo IV Competenza ed eserizio della competenza dell'EPPO, Capo V: Norme procedurali applicabili alle indagini, alle misure investigative, all'azione penale e alle alternative all'azione penale, Capo VI: Garanzie procedurali; Capo VII: Trattamento delle Informazioni; Capo VIII: Protezione dei Dati, Capo IX: Disposizioni finanziarie e disposizioni relative al personale; Capo X: Disposizioni relative alle relazioni della Procura Europea con i partner, Capo XI: Disposizioni Generali.

[3] Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura Europea «EPPO».

[4] In ragione delle mansioni di cui mi occupo – ovvero la ricezione atti presso la Procura della Repubblica di Bologna – sono stata una spettatrice privilegiata per quanto concerne la nascita di EPPO e ho avuto modo di confrontarmi sull'argomento con personale togato e non togato anche in ragione del servizio che gestisco.

si stanno adoperando "dietro le quinte" per l'operatività della Procura Europea allo scopo di mettere in evidenza le difficoltà operative relative all'utilizzo dei sistemi informativi in uso presso gli Uffici dei PED (Procuratori Europei Delegati)[5]; sarà, inoltre, d'interesse analizzare l'interoperabilità tra i sistemi informativi degli uffici giudiziari coinvolti. Si tenterà di fornire un'istantanea focalizzata sui sistemi informativi in uso presso i PED e quelli utilizzati dalla Procura della Repubblica presso il Tribunale e dalle Forze dell'Ordine per interagire con EPPO al fine di rilevarne le criticità.

In via preliminare si può evidenziare come il decreto ministeriale 7 giugno 2021 abbia istituito il registro di carattere temporaneo "R.A. EPPO"[6] previsto dall'articolo 14, comma 3 del decreto legislativo n. 9 del 2 febbraio 2021. Si tratta sostanzialmente di un registro dove vengono inserite le annotazioni di carattere temporaneo e relative alle notizie di reato di presumibile competenza EPPO: infatti nel caso in cui la Procura Europea non eserciti la propria competenza, la Procura della Repubblica presso il Tribunale, entro 30 giorni, deve iscrivere la notizia di reato nel registro previsto dall'articolo 335 c.p.p.. Il medesimo decreto ministeriale del 7 giugno 2021 ha istituito presso gli Uffici dei PED anche i relativi registri delle notizie di reato attribuite a persone note (cd. Modello 21 - EPPO) ed il registro delle notizie di reato attribuite a persone ignote (cd. Modello 44 - EPPO).

Si osserva come non sia espressamente indicata la modalità di trasmissione della notizia di reato di competenza della Procura Europea da parte delle Forze dell'Ordine: si presume che vengano trasmesse al registro R.A. EPPO a cura delle Forze di Polizia tramite portale NDR ma non risulta espressamente nella normativa. Va chiarito il rapporto tra il registro R.A. EPPO "temporaneo" ed il registro ex articolo 335 c.p.p. ReGeWEB, modulo del SICP (Sistema Informativo della Cognizione Penale). Il concetto di temporaneità del registro R.A. EPPO merita anch'esso un approfondimento. Le annotazioni nell'R.A. EPPO assumeranno carattere definitivo una volta iscritte nei registri Modelli 21 e 44 appositamente creati dalla DGSIA per EPPO. La realtà operativa ha avuto il merito – a fronte di una normativa quanto mai essenziale –

[5] Gli Uffici dei PED italiani sono incardinati a Roma, Milano, Napoli, Palermo, Torino, Venezia, Bologna, Catanzaro e Bari.

[6] Registro Automatizzato EPPO.

di mettere in luce procedimenti interpretativi da parte degli Uffici giudiziari: in particolare dal registro R.A. EPPO si accede, in buona sostanza, al portale NDR per individuare l'annotazione di interesse al fine dell'eventuale iscrizione nei registri modelli 44 Eppo o 21 Eppo e nel quale le Forze dell'Ordine inseriscono le annotazioni di interesse PIF[7]. La stessa modalità operativa, però, è quella utilizzata presso la Procura della Repubblica: ovvero si accede, tramite SICP, alle annotazioni preliminari inserite nel portale a cura delle Forze dell'Ordine. Quindi il Registro R.A. EPPO è visibile solo da EPPO e non si tratta dunque di un registro anche ad uso della Procura della Repubblica presso il Tribunale[8].

Infine, uno sguardo ai rapporti tra EPPO, Eurojust e OLAF e alle relative modalità di scambio di informazioni inerenti le indagini e gli accertamenti svolti su un determinato "caso".

2. Riferimenti normativi e sfera di competenza della Procura Europea

2.1. *La Procura Europea e la tutela degli interessi finanziari dell'Unione Europea*

Il TFUE (Trattato sul funzionamento dell'Unione Europea modificato dall'articolo 2 del Trattato di Lisbona del 13 dicembre 2007 e ratificato dall'Italia con legge 2 agosto 2008 n.130) all'articolo 86 par. 1 prevede l'istituzione di un ufficio di Procura Sovranazionale, la cui previsione legislativa risale al 1997 quando Mirelle Delmas – Marticoloy, assieme ad altri giuristi, introdusse nel c.d. "Corpus Iuris" la previsione di un pubblico ministero europeo che avrebbe dovuto tutelare gli interessi finanziari dell'Unione Europea[9]. Anche la costituzione Europea prevedeva tale organo: siamo nel 2004 ma il progetto di costituzione Europea

[7] Con il Decreto Legislativon.75 del 14 luglio 2020 è stata recepita in via definitiva la Direttiva (UE) 2017/1371) cd. direttiva PIF (protezione interessi finanziari) del Parlamento Europeo e del Consiglio del 5 luglio 2017, recante norme per la "lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale".

[8] I corsi di formazione organizzati dal Ministero hanno chiarito le perplessità inizialmente sorte.

[9] Mireille Delmas-Marticoloy è una giurista francese, professoressa onoraria al Collège de France e membro dell'Accademia di scienze morali e politiche. Membro di numerose commissioni legislative e costituzionali, e coordinatrice del Comitato di esperti dell'Unione Europea Unione sul progetto "Corpus Juris".

naufragò. Solo nel 2007 il Trattato di Lisbona riconobbe al Consiglio la facoltà di istituire una Procura Europea. La Procura Europea è stata successivamente istituita dal Regolamento (UE) n.1939 del 2017 adottato il 12 ottobre 2017 dal Consiglio d'Europa, ed entrato in vigore il 20 novembre 2017[10]. Sono 22 gli Stati dell'Unione Europea che hanno aderito alla cooperazione rafforzata[11].

La Procura Europea è competente per i reati che "ledono gli interessi finanziari dell'Unione": a tal fine, infatti, l'articolo 86 par.1 prevede l'istituzione di una Procura Sovranazionale. Le indagini e le azioni penali di EPPO sono disciplinate, quindi, dal Regolamento 1939/2017 e solo per gli aspetti in esso non contemplati si applica il diritto interno dei singoli Stati; in caso di conflitto prevale ai sensi dell'articolo 5 par 3 del Regolamento il diritto sovranazionale.

Per analizzare le peculiarità proprie di EPPO è preliminarmente utile distinguere la competenza per materia e per territorio dell'organo sovranazionale.

2.2. *Competenza per materia*

L'articolo 22 del Regolamento 1939/2017 chiarisce la competenza materiale di EPPO:

> 1. L'EPPO è competente per i reati che ledono gli interessi finanziari dell'Unione di cui alla direttiva (UE) 2017/1371, quale attuata dal diritto nazionale, indipendentemente dall'eventualità che la stessa condotta criminosa possa essere qualificata come un altro tipo di reato ai sensi del diritto nazionale. Per quanto riguarda i reati di cui all'articolo 3, paragrafo 2, lettera d), della direttiva (UE) 2017/1371, quale attuata dalla legislazione nazionale, l'EPPO è competente soltanto qualora le azioni od omissioni di carattere intenzionale definite in detta disposizione siano connesse al territorio di due o più Stati membri e comportino un danno complessivo pari ad almeno 10 milioni di EUR. 2. L'EPPO è competente anche per i reati relativi alla partecipazione a un'organizzazione criminale definiti nella decisione quadro 2008/841/GAI, quale attuata dal diritto nazionale, se l'attività criminosa di tale organizzazione criminale è incentrata sulla commissione di uno dei reati

[10] Salazar L., Habemus EPPO!, La lunga marcia della Procura Europea, Archivio Penale, n. 3, 2017.

[11] Gli stati aderenti alla cooperazione rafforzata sono, ad oggi, Austria, Belgio, Bulgaria,Cipro, Croazia, Estonia, Finlandia, Francia, Germania, Grecia, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Portogallo, Repubblica ceca, Romania, Slovacchia, Spagna e Slovenia).

di cui al paragrafo 1. 3. L'EPPO è altresì competente per qualsiasi altro reato indissolubilmente connesso a una condotta criminosa rientrante nell'ambito di applicazione del paragrafo 1 del presente articolo La competenza riguardo a tali reati può essere esercitata solo in conformità dell'articolo 25, paragrafo 3. 4. In ogni caso, l'EPPO non è competente per i reati in materia di imposte dirette nazionali, ivi inclusi i reati ad essi indissolubilmente legati. Il presente regolamento non pregiudica la struttura e il funzionamento dell'amministrazione fiscale degli Stati membri.

Per chiarire i dubbi applicativi iniziali in particolare ai fini dell'individuazione dei reati di interesse per EPPO, ancorchè non vincolante al di fuori dell'Ufficio nel quale trova applicazione, sono sicuramente d'ausilio le circolari. A titolo esemplificativo la Circolare Procuratore della Repubblica di Bologna n. 209 del 17 maggio 2021 individua, quali reati di interesse per EPPO, i seguenti[12]:

- Reati contro la pubblica amministrazione (da 314 c.p. a 322 *bis* c.p.).
- Reati di truffa e frode nei quali particolare attenzione è da riservare allo stanziamento della somma che viene erogata. La competenza sarà di EPPO se, ad esempio, vengono impiegati fondi europei anche se erogato da un ente nazionale (316 *ter* c.p.; 640 comma 2 c.p., 640 *bis* c.p., 640 *ter* c.p.; 353,353 *bis* c.p., 356 c.p.).
- Reati tributari in materia di IVA (2,3,4,5,8,10 quater, 11 del decreto legislativo n.74 del 2000), solo qualora l'azione o l'omissione intenzionale sia connessa al territorio di due o più stati membri e comporti un danno complessivo pari ad almeno 10 milioni di euro. Per i reati che comportano un danno inferiore a 10 milioni di euro, EPPO potrà esercitare la propria competenza solo se il caso abbia ripercussioni a livello europeo che richiedano lo svolgimento di indagini da parte dell'EPPO oppure se possono essere sospettati di aver commesso il reato funzionari o altri agenti dell'Unione ovvero membri delle istituzioni dell'Unione (articolo 25, paragrafo 2).
- Reati di contrabbando (D.P.R. 23 gennaio 1973 n.43) per i quali la competenza è comunque EPPO in considerazione del fatto che i dazi doganali sono una risorsa esclusiva dell'Unione.

[12] Circolare Procuratore della Repubblica di Bologna n.209 del 17 maggio 2021.

- Reati di criminalità organizzata (416 c.p., 416 *bis* c.p.; 291 quater del D.P.R. 43 del 1973) purché l'attività criminosa dell'organizzazione sia incentrata sui reati di cui al paragrafo uno dell'articolo 22 che devono, perciò, essere la ragione della costituzione e dell'esistenza dell'associazione.
- Reati di favoreggiamento reale, ricettazione, riciclaggio, reimpiego, autoriciclaggio, favoreggiamento, interposizione fittizia (379 c.p.,648 c.p.,648 *bis* c.p., 648 *ter* c.p., 648 ter c.p., 512 *bis* c.p. quando le condotte siano lesive degli interessi finanziari dell'Unione.

Inoltre l'articolo 22 par 3 dispone che EPPO sia competente in caso «qualsiasi altro reato indissolubilmente connesso a una condotta criminosa rientrante nell'ambito di applicazione del paragrafo 1 del presente articolo»[13].

2.3 *Competenza per territorio e personale di EPPO*

Per quanto concerne la competenza per territorio e personale, l'articolo 23 e l'articolo 26 la delimitano; in particolare l'articolo 23 chiarisce che Eppo è competente per i reati di cui all'articolo 22 commessi nel territorio di uno o più Stati membri o commessi da un cittadino di uno Stato membro o «da una persona che al momento del reato era soggetta allo statuto o al regime applicabile a condizione che uno Stato membro sia competente per tali reati quando sono commessi al di fuori del suo territorio». L'articolo 26 delimita la competenza del procuratore europeo delegato chiarendo, tra l'altro, che:

> Un caso è di norma aperto e trattato da un procuratore europeo delegato dello Stato membro in cui si trova il centro dell'attività criminosa oppure, se sono stati commessi più reati connessi di competenza dell'EPPO, dello Stato membro in cui è stata commessa la maggior parte dei reati.

Viene poi individuata la funzione propria della camera permanente in ordine all'assegnazione dei casi anche a PED diverso da quello strettamente competente. Si può fin d'ora evidenziare che una competenza territoriale sovranazionale unita ad una struttura complessa quale EPPO

[13] Per approfonimenti V. il contributo di A.Gammarota, *Aspetti di Informatica forense nel Regolamento UE del Pubblico Ministero Europeo (EPPO, European Public Prosecutor Office.*

comporta inevitabilmente ripercussioni anche in ordine ai sistemi informativi, alla loro interoperabilità e alla disciplina di tale complessità informatica e organizzativa. Si anticipa altresì come la DGSIA abbia ampliato le funzionalità di Sicp (Sistema Informativo della Cognizione Penale) in uso ad EPPO impostando una base dati a livello nazionale per la gestione dei fascicoli di indagine a carico di persone note e di persone ignote. Per il Sicp in uso alla Procura nazionale la base dati è, invece, distrettale.

3. La struttura organizzativa della Procura Europea

Altro elemento caratterizzante della Procura Europea è la struttura organizzativa. Essa è un organo dell'Unione Europea ancorché unitario ha sia carattere "centrale" che "decentrato"; una struttura, quindi, su due livelli[14].

L'Ufficio centrale è composto dal Procuratore Capo (attualmente Laura Cadruta Kovesi) e i relativi sostituti (nel luglio 2020 il Consiglio ha nominato 22 procuratori europei), dal collegio, dalle camere permanenti, dai procuratori europei per Stato membro, dal direttore amministrativo e ha sede in Lussemburgo.

Il Collegio (articolo 9 Regolamento) è presieduto dal Procuratore capo europeo, il quale è componente del Collegio assieme ad un Procuratore europeo per Stato membro. Sono riservate al collegio le decisioni strategiche e l'uniformità di indirizzo in materia di azione penale della Procura Europea ma non tratta i singoli casi. Inoltre, il Collegio istituisce le camere permanenti (articolo 10 Regolamento) che sono anch'esse presiedute dal Procuratore capo europeo e garantiscono il coordinamento delle indagini transfrontaliere. Sono le Camere permanenti che promuovono l'azione penale, archiviano il caso, rinviano il caso all'autorità nazionale o riaprono un'indagine (cfr. articolo 36, paragrafi 1,3,4; articolo 39 paragrafo 1 lettere da a) a g) e paragrafo 2; articolo 34 paragrafi 1,2,3 e 6).

Il Procuratore Capo ai sensi dell'articolo 11 del Regolamento dirige la Procura Europea e la rappresenta di fronte alle istituzioni dell'Unione e degli Stati membri. Il Procuratore europeo per Stato membro (articolo 12 del Regolamento) funge da collegamento tra camere permanenti e

[14] SALAZAR, *ibidem.*

Procuratori europei delegati. Supervisiona le indagini e le azioni penali di cui i PED sono responsabili[15].

Una prima osservazione in merito ai sistemi informativi emerge analizzando la Decisione 15 del 2020 del Collegio relativa alle Camere permanenti. L'articolo 4 che tratta dell'assegnazione dei casi alle camere permanenti afferma che «all'avvio di un caso il sistema automatico di gestione dei fascicoli dell'EPPO lo assegna in modalità casuale ad una camera penale». In questo provvedimento – a testimonianza del fatto che non sono molte le fonti che affrontano il problema dell'interoperabilità dei sistemi informativi coinvolti nella gestione dei casi affidati ad EPPO – non si reperiscono chiarimenti in merito all'eventuale interoperabilità tra i sistemi informativi in uso a livello nazionale e quelli utilizzati a livello sovranazionale. L'articolo sembrerebbe solo rinviare ad un sistema automatico di assegnazione dei fascicoli sul tipo di quello presente in ReGeWEB dove i fascicoli vengono assegnati ai magistrati in virtù di un algoritmo che ne garantisce una distribuzione proporzionata e casuale tra magistrati. Sarebbe stato opportuno chiarire anche l'aspetto dell'interoperabilità tra il *Case Management System* di EPPO e di tutti i sistemi nazionali tra i quali anche il ReGeWEB italiano. Problema complesso, già risolto dalla UE in altre situazioni analoghe, es. interconnessione dei casellari; la realtà operativa qui fornisce una risposta negativa in merito alla sussistenza di interoperabilità tra i sistemi informativi considerati. Nel paragrafo 4 cercheremo di rispondere anche – grazie all'ausilio delle circolari[16] – ai quesiti sulle modalità di scambio dei dati tra Procura nazionale ed Eppo e tra Forze dell'Ordine ed EPPO.

L'articolazione decentrata, che è rappresentata dai PED, è disciplinata dall'articolo 13 del Regolamento del 2017/1939. I PED vengono nominati a cura del collegio della Procura Europea, su proposta del Procuratore capo europeo, una volta designati dal Consiglio superiore della magistratura. In ordine alle attribuzioni i PED agiscono per conto della Procura Europea nei rispettivi Stati membri seguendo le indicazioni della Camera permanente incaricata del caso e del Procuratore europeo incaricato della supervisione.

[15] Il Procuratore europeo per l'Italia è il Dr. Danilo Ceccarelli che è anche Vice Procuratore Capo europeo.

[16] Ci si riferisce alle circolari interne ad alcuni Uffici del Ministero della Giustizia ed in particolare delle Procure della Repubblica presso il Tribunale, come la citata Circolare della Procura della Repubblica di Bologna n. 209 del 17 maggio 2021.

Il Ministero della Giustizia nella fase preliminare all'operatività di EPPO ha raccolto dagli uffici requirenti i dati statistici sui procedimenti di competenza della Procura Europea finalizzati anche all'elaborazione delle proposte relative al contingente nazionale PED e alla loro distribuzione logistica e funzionale. Gli Uffici dei PED sono incardinati in Italia (articolo 10 decreto legislativo n. 9/2021), accorpando due o più distretti di Corte d'Appello [17]. Inoltre, l'articolo 96 par.6 del Regolamento sancisce il principio in base al quale sono le Autorità nazionali competenti a dotare i PED delle risorse e delle attrezzature necessarie per l'esercizio delle loro funzioni.

Il Regolamento prevede, inoltre, un accordo tra Ministro della Giustizia e Procuratore Capo Europeo in ordine al numero ed all'articolazione funzionale e territoriale dei PED all'interno dello Stato. In tale accordo non è stata recepita la possibilità per i PED di svolgere anche le funzioni di pubblici ministeri nazionali, nonostante l'articolo 13 citato lo contemplasse cosicché il loro impegno è *full time* ma restano nel ruolo organico della magistratura nazionale a differenza del Procuratore Europeo nazionale che è collocato fuori ruolo.

Fare un bilancio è prematuro: lo sforzo attualmente è teso all'organizzazione della struttura, mentre le pendenze sembrano al momento contenute e gestibili ma si attendono i dati ufficiali.

4. Sistemi informativi utilizzati dai PED italiani per la gestione-delle notizie di reato

4.1. *Lo stato dell'arte nazionale al momento di avvio dell'operatività di EPPO*

La descrizione tratteggiata nei paragrafi precedenti ha dato conto della complessità organizzativa e funzionale di EPPO e delle sue articolazioni in ciascun Paese aderente (PED). I sistemi informativi automatiz-

[17] Roma per i distretti di Roma, Perugia, Cagliari e L'Aquila; Milano per i distretti di Milano e Brescia. Napoli per i distretti di Napoli e Salerno; Palermo, per i distretti di Palermo, Catania, Caltanisetta e Messina; Torino per i distretti di Torino e Genova; Venezia per i distretti di Venezia, Trieste e Trento; Bologna per i distretti di Bologna, Ancona e Firenze; Catanzaro per i distretti di Catanzaro, Reggio Calabria e Potenza; Bari per i distretti di Bari, Lecce e Campobasso Per completezza espositiva va precisato che le sedi di Bari e Catanzaro sono, al momento, prive di copertura.

zati sviluppati rispecchiano, in conseguenza, tale complessità con la presenza di un sistema centrale ("Sistema automatizzato di gestione dei fascicoli" previsto e delineato dagli articoli 44 e seguenti del Regolamento UE 2017/1939) e di tanti sistemi decentrati nazionali che dovranno essere resi tra loro interoperabili (per l'Italia il sistema è stato regolato dall'articolo 14 del decreto legislativo n. 9/2021 che introduce una revisione e modifica dei sistemi informativi per la "comunicazione e iscrizione di notizie di reato di competenza della Procura Europea").

Quanto al sistema centrale, denominato semplicemente Case Management System (CMS), è stato progettato per assicurare tutte le funzioni relative ad ogni procedimento, in ogni fase del suo ciclo di vita: dall'avvio all'indagine, all'azione penale e alla definizione. Il sistema è stato sviluppato come un ambiente *on premise*[18] autonomo con infrastruttura dedicata, ed è stato riutilizzato, personalizzandolo, il CM in uso al Direttorato Generale per la Concorrenza della Commissione Europea denominato CASE@EC. Il sistema mette a disposizione degli utenti tre strumenti: un registro, un indice dei fascicoli, e un gestore documentale[19].

La realizzazione del progetto è stata molto complessa perché il flusso di informazioni è estremamente articolato: il regolamento descrive diverse situazioni in cui le informazioni possono essere trasferite sia tra le diverse articolazioni di EPPO, sia con altre agenzie dell'Unione Europea quali Eurojust[20] e Europol, nonché con le Autorità nazionali, in momenti diversi e in modo bidirezionale. Allo stato, tuttavia, anche a causa del fatto che il livello di informatizzazione dei procedimenti penali nei diversi Stati aderenti è alquanto dissimile, la prima versione realizzata nel febbraio 2021[21] non garantisce la piena interoperabilità tra tutti i sistemi. Per lo scambio di informazioni tra gli attori coinvolti e nelle diverse situazioni previste dal Regolamento, e con lo scopo di semplificare l'alimentazione delle basi di dati non ancora

[18] Definizione con cui si fa riferimento a *software* che sono installati fisicamente nei computer e nei server dell'organizzazione che ne fa uso.

[19] P. Pérez Enciso, *Exchange and Processing of Information Between the European Public Prosecutor's Office and National Authorities. The Case Management System*, in The European Public Prosecutor's Office, pp 253-279, a cura di L. Bachmaier Winter, 2018.

[20] Al momento lo scambio di informazioni con Eurojust è stato regolato da apposito accordo di lavoro siglato a febbraio 2021 disponibile in italiano al seguente indirizzo web: https://www.eurojust.europa.eu/sites/default/files/202102/working_arrangement_EPPOPED_it.pdf.

[21] K. Siitam-Nyiri, *EPPO and Digital Challenges*, 17/05/2021, reperibile all'indirizzo web: https://doi.org/10.30709/eucrim-2021-010 // BibTeX.

interconnesse, è stato creato un modulo standard in formato PDF editabile, denominato *EPPO Crime Report*, che consente di inserire le informazioni di cui è prevista la condivisione in modo standardizzato.

Quanto ai sistemi decentrati nazionali, in questo contributo esamineremo il caso italiano, dando conto di come sia stata realizzata l'infrastruttura digitale contemplata dal già menzionato articolo 14, comma 3, che ha imposto di creare uno specifico registro temporaneo «separatamente disponibile per ciascuna Procura della Repubblica italiana e, contemporaneamente, visibile sul piano nazionale dai PED»[22].

Prima di descrivere gli sviluppi specifici per assicurare l'operatività dei PED italiani, tuttavia, è opportuno richiamare sinteticamente le informazioni, accennate nelle pagine precedenti, sullo stato dell'arte degli applicativi in uso presso gli Uffici della Procura della Repubblica presso i Tribunali ordinari, esistente quando tali evoluzioni sono state avviate. Presso ciascuna Procura nazionale la gestione informatizzata dei procedimenti penali si regge su tre pilastri distinti, ma interconnessi: il Portale delle notizie di reato (Portale NDR)[23], il registro ufficiale gestito dal modulo ReGeWEB di SICP e il gestore documentale TIAP Document@ (Trattamento Informatizzato Atti Processuali).

Il Portale NDR rappresenta il punto di accesso nazionale che consente agli "Uffici Fonte" – che si identificano con gli organi di Polizia Giudiziaria operanti sia nelle Forze dell'ordine che in altri Enti – di inserire i dati delle comunicazioni notizie di reato (CNR) in un applicativo che colloquia con i registri informatici delle Procure della Repubblica. Esso consente, infatti, agli Uffici Fonte di iscrivere una "Annotazione Preliminare", con tutti i dati attinenti alla notizia di reato e la relativa documentazione in formato digitale, e di trasmetterla alla Procura competente. La Procura destinataria trova nelle proprie Annotazioni Preliminari di SICP la CNR trasmessa, e può trasferirla, dopo il provvedimento di iscrizione, nell'applicativo ReGeWEB che gestisce il Registro Generale delle Notizie di Reato (RGNR) previsto dall'articolo

[22] Circolare della Capo Dipartimento dell'Organizzazione Giudiziaria, del Personale e dei Servizi, n. 10882.U del 21/05/2021, "*Avvio dell'operatività dal 1° giugno 2021 della Procura Europea ai sensi regolamento (UE) 2017/1939 e del decreto legislativo 29 gennaio 2021, n. 9 – Ruolo e necessità organizzative e logistiche per i Procuratori europei delegati – Prime indicazion*i", https://www.giustizia.it/giustizia/it/mg_1_8_1.page? contentId=SDC333354.

[23] Per completezza di informazione occorre precisare che presso gli Uffici delle Procure di primo grado esiste un secondo portale denominato PDP (Portale Deposito atti Penali) riservato, ad oggi, all'attività dei Difensori.

335 del codice di procedura penale. Ad iscrizione avvenuta, il SICP crea il corrispondente fascicolo informatico nel gestore documentale TIAP Document@ contraddistinto dal medesimo numero del registro, nonché inoltra automaticamente al Portale NDR le informazioni relative all'iscrizione, quali il numero ed il tipo di registro, la data di iscrizione ed il Magistrato assegnatario.

È bene chiarire che la fase dell'iscrizione non è interamente informatizzata perché, ad oggi, non esiste un "cruscotto" che consenta al Procuratore Capo, o a suo delegato, di prendere visione della CNR e di adottare il provvedimento di iscrizione con un documento nativo digitale [24]. La ricezione della CNR, dunque, è affidata alla Segreteria della Procura che deve stampare su documento analogico quanto pervenuto e sottoporlo al magistrato per l'emissione del provvedimento di iscrizione, in seguito al quale dovrà trasferire i dati delle Annotazioni Preliminari nel ReGeWEB apportando le eventuali modifiche ed integrazioni disposta dal magistrato.

La criticità maggiore, tuttavia, è rappresentata dal fatto che l'utilizzo del Portale NDR è autorizzato, ma non obbligatorio. Così sul territorio nazionale si registrano situazioni difformi: accanto a Uffici di Procura della Repubblica che hanno massimamente incentivato la trasmissione delle notizie di reato direttamente e unicamente attraverso portale, altri hanno preferito lasciare spazio sia ai canali tradizionali, ossia il deposito a mani e la raccomandata, ma anche nella prassi riconosciuto efficacia ad un canale telematico non interoperabile con i sistemi interni quale è la PEC.

È evidente che tale scelta ha delle ripercussioni sull'organizzazione del lavoro all'interno degli Uffici, perché la pluralità di canali di trasmissione rende più difficile le attività di ricezione e avvio della fase di iscrizione.

In questo scenario, in vista dell'avvio della operatività di EPPO, la DGSIA ha seguito la strada della modifica evolutiva dei sistemi informativi già dispiegati al fine di renderli rispondenti alle nuove esigenze dei PED italiani. A tale fine da un lato sono stati approntati registri ufficiali autonomi per i PED replicando il modulo ReGeWEB, dall'altro si è sviluppato il registro previsto dall'articolo 14, comma 3, del decreto legislativo 9/2021.

[24] L'imprescindibilità del fascicolo cartaceo si desume dall'articolo 109 Disposzioni Attuative C.p.p. mentre la legittimazione al deposito telematico deriva dall'articolo 108 Disposiozioni Attuative C.p.p.: finchè il Legislatore non interverrà per apportare i doverosi chiarimenti in merito al raccordo tra queste due norme non sarà possibile prescindere dal deposito cartaceo.

Con decreto del Ministro della Giustizia del 7 giugno 2021, nel rispetto della normativa che regola la tenuta dei registri ufficiali informatizzati negli uffici giudiziari[25], sono stati formalmente istituiti – ai sensi dell'articolo 3 - presso gli Uffici dei PED, tanto il registro delle notizie di reato attribuite a persone note (denominato Modello 21 – EPPO), che quello delle notizie di reato attribuite a persone ignote (denominato Modello 44 – EPPO) per le ipotesi previste dall'articolo 14, comma 1 del decreto legislativo 9/2021[26].

L'articolo 2, ed è questa la novità maggiore, istituisce il "registro delle annotazioni" delle notizie di reato previsto dall'articolo 14, comma 3 [27], del decreto legislativo 9/2021 (denominato R.A. EPPO) accessibile esclusivamente ai PED ma sincronizzato al ReGeWeb moduolo Sicp della Procura nazionale per soddisfare l'obbligo di doppia comunicazione della CNR per reati PIF, obbligo che contempera la competenza esclusiva dell'EPPO e le esigenze di sollecita iscrizione ed adozione di atti urgenti da parte della Procura nazionale.

Il registro R.A. EPPO è stato sviluppato per gestire i casi concreti di CNR in cui la competenza EPPO è immediatamente ravvisabile. Viceversa, nei casi in cui il reato "EPPO" emerga nel corso delle indagini preliminari, e dunque dopo la formale iscrizione nel registro automatizzato della procura ordinaria, il PED dovrà percorrere la strada dell'avocazione di cui si dirà.

4.2. *Notizia di reato di competenza EPPO immediatamente ravvisabile.*

Qualora la Polizia Giudiziaria individui una fattispecie di reato di possibile competenza EPPO ai sensi dell'articolo 14 del decreto legislativo

[25] Decreto del Ministro della giustizia, di concerto con il Ministro del tesoro, del bilancio e della programmazione economica, del 27 marzo 2000, n. 264, *Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziar*i e Decreto ministeriale 27 aprile 2009, *Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia*.

[26] Articolo 14 comma 1: «Le comunicazioni di cui all'articolo 347 del codice di procedura penale, le denunce, le querele, gli esposti e gli ulteriori atti comunque denominati che hanno ad oggetto reati in relazione ai quali la Procura europea potrebbe esercitare la sua competenza ai sensi degli articoli 22 e 25, paragrafi 2 e 3, del regolamento sono presentati o trasmessi, oltre che al pubblico ministero nazionale, al procuratore europeo delegato».

[27] Articolo 14 comma 3: «Fuori dai casi previsti dal comma 2, il pubblico ministero dispone l'annotazione della notizia di reato in apposito registro, tenuto in forma automatizzata, che il Ministro della giustizia istituisce con proprio decreto da adottare entro trenta giorni dall'entrata in vigore del presente decreto».

n. 9 del 2021 rubricato "Comunicazione e iscrizione di notizie di reato di competenza della Procura Europea" dovrà darne comunicazione sia ad EPPO che alla Procura ordinaria.

Il registro provvisorio di cui all'art. 14 Decreto Legislativo 2 febbraio 2021 n. 9 contiene le annotazioni preliminari – con allegati i *files*.pdf delle notizie di reato – che le Forze dell'Ordine hanno trasmesso ad EPPO attraverso il portale NDR ed in cui sia stato contrassegnato l'interesse PIF. Nel Portale NDR è stato creato un nuovo campo che le Fonti debbono valorizzare per segnalare che la CNR che si trasmette è relativa a reati PIF. Con la valorizzazione di tale campo la CNR viene inviata nel registro temporaneo delle annotazioni dal quale sarà ribaltata nel registro SICP della procura nazionale ovvero nel registro informatizzato Modello 21 o 44 EPPO laddove il PED ravvisi la sua competenza. L'annotazione preliminare contrassegnata PIF sarà visibile anche dal ReGeWeb moduolo Sicp anche se acquisirà un numero identificativo diverso.

In concreto gli scenari ravvisabili posso essere così sintetizzati: a) all'arrivo della CNR PIF il Procuratore nazionale non iscrive nel proprio ReGeWEB, ma attende le determinazioni del PED; b) la regola appena descritta viene derogata nei casi di urgenza di cui all'articolo 14, comma 2, (ad esempio convalide di misure coercitive ovvero adozione di misure investigative il cui ritardo potrebbe pregiudicare l'indagine); c) il PED, che ha ricevuto la CNR PIF contemporaneamente al Procuratore nazionale, comunica di ravvisare la propria competenza; d) comunica di non ravvisare la propria competenza; e) non comunica nulla nel termine di legge di 30 giorni.

Ciascuno di questi scenari viene registrato nel RA EPPO e l'informazione è sintetizzata attraverso l'utilizzo di valori predeterminati che descrivono lo stato della CNR PIF[28] fino al momento di iscrizione della stessa in uno solo dei registri delle Autorità coinvolte (Procura nazionale o PED). Nell'ipotesi in cui EPPO manifesta interesse alla notizia

[28] I possibili valori, presentati alternativamente in un unico campo e resi più rapidamente decifrabili mediante icone con simboli e colori diversi, sono i seguenti: all'attenzione della Procura Europea (Annotazione Preliminare classificata "Interesse PIF", in attesa di valutazione da parte della Procura Europea); all'attenzione della Procura Europea – termini superati (in attesa di valutazione da oltre 30 giorni);Interesse EPPO (Annotazione Preliminare su cui la Procura EPPO ha manifestato la volontà di esercitare la sua competenza); iscritto presso la Procura Europea (Annotazione Preliminare iscritta presso il Registro Generale della Procura EPPO); no interesse EPPO (Annotazione Preliminare su cui la Procura EPPO ha manifestato la volontà di non esercitare la sua competenza).

di reato, sarà necessario definire la pendenza sul registro temporaneo "R.A. EPPO" con le stesse modalità proprie dell'iscrizione nell'ambito nazionale ovvero con l'iscrizione dell'annotazione preliminari di interesse PIF nel registro modello 21-EPPO o nel registro modello 44 - EPPO. Nei casi di urgenza di cui alla lettera b) rimane buona prassi il coordinamento tra PED e sostituto procuratore di turno per gli atti urgenti o procuratore aggiunto delegato o la stesura di un protocollo all'occorrenza. Alcune procure nazionali ritengono di iscrivere quale Fatto Non Costituente Reato (FNCR- Modello 45) la notizia di reato di interesse PIF per la quale EPPO abbia manifestato interesse: tale soluzione appare utile ai fini archivistici e statistici.

Da una prima valutazione delle modalità operative, il monitoraggio del portale NDR da parte della procura nazionale risulta essenziale al fine della tempestività delle iscrizioni delle notizie di reato per le quali EPPO non abbia manifestato interesse. Le Procure che monitorano il portale quotidianamente e lo utilizzano come formale canale di trasmissione delle notizie di reato risultano avvantaggiate in termini organizzativi in quanto quotidianamente e in tempo reale possono monitorare le annotazioni di interesse PIF. Per le procure che utilizzano altri canali formali di trasmissione delle notizie di reato (PEC, deposito a mani, raccomandata) appare necessario un controllo più mirato del portale. Ad esempio, un controllo periodico delle annotazioni preliminari selezionando, tra i criteri di ricerca, anche l'interesse PIF al fine di individuare celermente le eventuali annotazioni preliminari trasmesse dalle Forze dell'Ordine per le quali EPPO non abbia manifestato interesse con conseguente obbligo per la Procura di iscriverle. Può, inoltre, risultare determinante l'uso della query standardizzata di ARES per la ricerca delle annotazioni preliminari di interesse PIF. Sicuramente l'accorgimento ad opera della polizia giudiziaria di indirizzare la notizia di reato sia al PED che alla Procura nazionale competente, è uno strumento semplice ma quanto mai efficace a far scattare un *alert* da parte della procura nazionale che ricevendo l'atto (cartaceo) e notando il doppio indirizzo sarà indotta a tener monitorata tale notizia di reato al fine di verificare se EPPO abbia manifestato interesse all'esercizio dell'azione penale. Anche la prassi di comunicare a mezzo PEC da parte di EPPO l'interesse o il non interesse nei confronti di una notizia di reato è di estremo ausilio in particolar modo in questa fase di attivazione delle procedure di transizione.

4.3. *Notizia di reato per le quali la competenza EPPO emerga in un momento successivo*

Nel caso in cui la competenza EPPO emerga successivamente all'iscrizione della notizia di reato nel registro ReGeWEB della Procura nazionale, l'articolo 24 paragrafo 2 del Regolamento prevede che la Procura nazionale informi senza ritardo EPPO, quest'ultimo potrà attivare lo strumento giuridico dell'avocazione per subentrare nelle indagini acquisendo il procedimento.

Complessivamente, dunque, sono tre le situazioni in cui l'avocazione può essere esercitata: a) nei casi (eccezionali) di iscrizione da parte della Procura nazionale, laddove sia stata necessaria l'adozione di atti urgenti; b) nei casi in cui il reato "EPPO" sia emerso nel corso delle indagini preliminari e dunque dopo la formale iscrizione nei registri ordinari del SICP; c) in relazione ai procedimenti iscritti nel periodo intercorrente tra il 20.11.2017 e il 31.5.2021 che non siano già stati definiti con archiviazione ovvero con esercizio dell'azione penale.

La trasmissione per avocazione EPPO non è allo stato contemplata nel ReGeWEB che gestisce solo il meccanismo dell'avvocazione da parte del Procuratore Generale della Repubblica nei casi previsti dalla legge. Possiamo facilmente ipotizzare che prossimi rilasci dell'applicativo includano la gestione di questo istituto per registrare correttamente la definizione del procedimento nella Procura nazionale di provenienza.

Non esistendo allo stato un sistema automatizzato per il trasferimento di dati e documenti tra il sistema informativo nazionale e il CMS EPPO, si versa in una delle situazioni per le quali è stato elaborato il modello ECR (acronimo di EPPO *Crime Report*) di cui si è detto.

Benché non sussista un obbligo di utilizzo di tale modulo da parte della Procura nazionale per trasmettere i relativi dati ad EPPO, esso è fortemente raccomandato. In particolare, l'ECR consente e facilita la redazione delle informazioni obbligatorie finalizzate al possibile esercizio del potere di avocazione da parte dell'EPPO ex articolo 24(2) o (3) del Regolamento. Può essere altresì utilizzato, tuttavia, per la comunicazione di nuove notizie di reato che in concreto, per qualsiasi motivo, non siano state trasmesse ad EPPO con il PortaleNDR, e per le quali la Procura Europea possa esercitare la competenza, ex articolo 24(1) del Regolamento.

Qualora si utilizzi il modulo ECR, esso dovrà essere firmato digitalmente in formato PAdES al fine di garantirne l'immodificabilità. Il mancato utilizzo di ECR comporta un rallentamento nell'inserimento dei dati nel sistema automatico di gestione in uso ad EPPO. Non va, però, trascurato che i primi approcci all'ECR[29], in via sperimentale, hanno suscitato qualche preplessità in ordine all'immediatezza dell'utilizzo ragion per cui si auspica nella formazione a cura del Ministero della Giustizia per incentivarne eventualmente l'uso. Si conferma, anche in questo frangente, la difficoltà di uniformare i processi organizzativi in ambito giudiziario [30].

5. Rapporti tra EPPO, Eurojust e Olaf

Se Eurojust ha meri poteri di coordinamento, i PED possono condurre indagini anche se la collegialità dell'Ufficio centrale della Procura Europea di primo acchito potrebbe stridere con la necessaria speditezza che dovrebbe caratterizzare le indagini penali. Inoltre, Eurojust ha una competenza ben più vasta di EPPO che si limita all'area PIF.

È anche importante sottolineare come l'articolo 100 del Regolamento (UE) 2017/1939 evidenzi la necessità di cooperazione tra EPPO, che ha sede in Lussemburgo, e Eurojust che ha sede, però, nei Paesi Bassi in un'ottica di "sviluppo dei reciproci legami operativi". Sarà interessante vedere l'evoluzione di questa relazione e i risultati che verranno conseguiti considerando le differenze evidenziate tra i due organismi.

Olaf è organismo fondamentale e precursore di EPPO per quanto concerne la tutela degli interessi finanziari dell'Europa in quanto è competente a svolgere indagini di natura amministrativa nella c.d area PIF. I rapporti Olaf possono essere trasmessi alle autorità amministrative nazionali. Il coordinamento tra Olaf e EPPO è disciplinato dall'articolo101 del regolamento EPPO che ne prevede la necessità di scambio di informazioni ed in linea generale l'alternatività delle indagini non escludendo, però, la contestualità delle stesse. Il ruolo di Olaf rimane

[29] Acronimo che sta per PDF ADVANCED ELECTRONIC SIGNATURE. I files firmati col formato PAdES, al contrario di quanto accade con il formato p7n del CadES mantiene ferma l'estensione.pdf.

[30] Le problematiche relative alla difficoltà della diffusione dei sistemi informativi in ambito giudiziario sono state approfondite dalla sottoscritta nella tesi di dottorato, mi sia consentito citarla, "Verso il processo penale telematico" in Diritto e Nuove Tecnologie.

determinate anche in ragione delle attività legate agli stati non EPPO dell'Unione Europea e non dell'Unione Europea.

Per quanto riguarda l'interoperabilità tra i sistemi informativi di EPPO Eurojust e Olaf il Procuratore Capo Europeo Laura Kovesi ha firmato in data 15 febbraio 2021 un *Working Arrangement* tra Eurojust and EPPO e in data 5 luglio 2021 tra EPPO ed Olaf. L'articolo 5 e 6 del *Working Arrangement* del 15 febbraio 2021 ad esempio disciplina le modalità di accesso ai reciproci sistemi di gestione dei fascicoli.

Rimane il fatto che siamo di fronte a linee guida generali in cui si evidenzia la necessità di chiedere il reciproco consenso all'accesso ai rispettivi sistemi informativi. Va anche evidenziato che dal 16 febbraio 2021 la Procura Europea è collegata all'infrastruttura TESTA (acronimo di *Trans European Services for Telematics between Administrations*) che garantisce lo scambio di dati tra pubbliche amministrazioni e utilizzata dalle istituzioni e agenzie europee nonchè dagli stati UE e dalle organizzazioni che agiscono per loro conto. Quindi i presupposti anche formali affinché lo scambio di dati e informazioni tra organismi che si occupano di tutelare gli interessi finanziari dell'unione Europea dell'area PIF sussistono, ma si dovrà attendere il consolidarsi delle prassi operative per poter affermare se l'interoperabilità ha effettivamente attecchito. Al momento appare quale una significativa dichiarazione di intenti[31] [32].

6. Conclusioni

Chi interagisce o lavora nella pubblica amministrazione avrà avuto modo di scontrarsi con una problematica frequente: la formalizzazione di un provvedimento non comporta necessariamente il conseguimento dei risultati che l'atto si prefigge. Affinché alla formalizzazione consegua la realizzazione dell'obiettivo prefissato, è indispensabile che vi sia un'utilità tale da spingere i soggetti coinvolti (in particolare il personale delle amministrazioni pubbliche) ad adoperarsi affinché questo av-

[31] A. Venegoni e M. Minì, *I nodi irrisolti della nuova Procura Europea*, in Giurisprudenza Penale Web, 12, 2017.

[32] G. Guagliardi, *Procura Europea. Siamo davvero pronti in assenza di un codice di procedura penale europeo? Una nuova sfida per l'avvocatura e la magistratura*, in Giurisprudenza Penale Web, 2021, 2.

venga. Bisognerà attendere per verificare se la tutela degli interessi finanziari dell'Unione Europea sarà stato un "motore" prorompente in grado di far superare gli innumerevoli ostacoli di natura organizzativa ed informatica che si sono materializzati in questi primi mesi di operatività di EPPO. Un approccio pragmatico incrementale [33] [34], di gran lunga quello che consente di realizzare risultati concreti in ambito giudiziario, avrebbe optato per i PED logisticamente incardinati all'interno della procura nazionale, se possibile, per poi, solo in un secondo momento, valutare una sede distaccata? Non per prudenza sconfinante in immobilismo ma per consapevolezza della complessità giudiziaria che richiede, per la realizzazione di risultati concreti, oltre ad una motivazione inossidabile anche un approccio graduale all'innovazione tecnologica ed organizzativa. Questo uno dei quesiti sorti nel primo periodo di operatività di EPPO, ma la "diretta" sulla EPPO, in realtà, ha appena avuto inizio e sarà necessario ed interessante "accendere nuovamente le telecamere" sulla Procura Europea tra alcuni mesi.

[33] Mi sia consentito ricordare come le problematiche relative all'approccio pragmatico incrementale per l'implementazione dei sistemi informativi in ambito giudiziario siano state approfondite in S. MOFFA, *Verso il processo penale telematico*, tesi di dottorato in Diritto e Nuove Tecnologie, UniBo, 2017.

[34] CARNEVALI D. (a cura di) *Soggetti Smarriti. Perché innovazione e Giustizia non si incontrano quasi mai*, Franco Angeli, 2010, pp 196 e ss.

Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/979125994643024
pp. 469-491 (gennaio 2022)

Il Processo Penale Telematico (PPT) tra emergenza COVID e riforme

Giovanna De Rugeriis[1]

1. Introduzione

Nel volume dedicato alle "prime" Questioni di informatica forense, tra le tematiche trattate avevamo presentato anche lo stato dell'arte del processo penale telematico (d'ora in avanti PPT), allora in embrione, ipotizzandone una lunga gestazione: «Il percorso che porterà a un PPT propriamente detto sembra dunque ben avviato, ma ad essere realistici non si possono ipotizzare tempi brevi per arrivare alla meta del viaggio»[2].

In effetti, il cammino incrementale condotto dal Ministero della Giustizia per sviluppare, anche per il processo penale, una infrastruttura unitaria che consentisse agli utenti interni (magistrati, cancellieri e ufficiali giudiziari) e agli utenti esterni (avvocati, forze dell'ordine, cittadini) di svolgere il proprio lavoro o ricevere un servizio in modo completamente digitale e a distanza, era ancora in fase di progettazione, quando è sopraggiunta l'emergenza epidemiologica del COVID19. Il contratto per lo "*Sviluppo del Sistema Informativo Unitario Telematico, la manutenzione degli attuali sistemi dell'Area penale del Ministero della Giustizia e servizi correlati*"[3], infatti, era diventato esecutivo solo nel mese di ottobre 2019.

Il sopraggiungere dell'emergenza sanitaria ha impresso una significativa accelerazione alle attività di sviluppo in corso perché, anche in

[1] Dottore di Ricerca in Diritto e Nuove tecnologie, indirizzo Informatica Giuridica. Direttore amministrativo presso la Procura Generale della Repubblica di Bologna.

[2] G. De Rugerris, *Effetti delle innovazioni tecnologiche sul processo penale*, in C. Maioli (a cura di), *Questioni di informatica forense*, Aracne editrice, 2015, pp. 89-112.

3 Si veda DGSIA, "Ricognizione della digitalizzazione del processo civile e penale e della transizione digitale del ministero della giustizia", p. 39, disponibile all'indirizzo web https://www.giustizia.it/cmsresources/cms/documents/studio_dgsia_ricognizione_digitalizzazione_febbraio2021.pdf.,pagina.

questo settore come nel resto della società, si è assistito ad un accresciuto utilizzo delle tecnologie dell'informazione e della comunicazione (cui di seguito faremo riferimento con l'acronimo inglese ICT) per fare a distanza ciò che, a causa del distanziamento e della ridotta mobilità delle persone, non poteva più svolgersi in presenza.

Le leve sulle quali si è agito sono principalmente tre: normativa, tecnologica e organizzativa. A livello normativo sono state finalmente adottate norme di rango primario (benché a carattere temporaneo) per adottare le ICT nel processo penale. Anche sul piano tecnologico si sono realizzate novità apprezzabili, sia ricorrendo a prodotti software di mercato in aggiunta agli applicativi personalizzati sia accrescendo l'accesso da remoto agli applicativi interni. A livello organizzativo, infine, si è registrato un intenso confronto tra gli operatori del diritto che ha favorito una più completa presa d'atto degli strumenti disponibili e di quelli mancanti benché necessari.

Il punto di maggior interesse è rappresentato, a nostro avviso, dalla accresciuta consapevolezza negli operatori del settore tanto delle potenzialità quanto dei rischi specifici che le ICT portano nel dominio del processo in generale, ed in particolare in quello penale. Gli strumenti adottati con la normativa emergenziale, infatti, hanno ben presto posto in luce la necessità di bilanciare esigenze diverse: da un lato accrescere l'utilizzo delle ICT per tutelare la salute individuale e collettiva, dall'altro assicurare il pieno rispetto delle garanzie processuali e al contempo la protezione dei dati personali. Da più parti sono stati manifestati forti timori che tale legislazione possa condurre ad una giustizia sommaria. Non si può negare che il repentino scostamento dagli istituti procedurali ordinari potrebbe talora determinare la compressione delle regole costituzionali del giusto processo: «nel contraddittorio tra le parti, in condizioni di parità» (articolo 111 Costituzione), se le novità non fossero applicate con prudenza e con il supporto tecnologico adeguato.

Si tratta di una sfida di fondo che era stata presente sin dal momento in cui le ICT avevano iniziato a produrre effetti in modo diretto sul diritto penale e sostanziale[4] che, grazie alla rapida accelerazione imposta dal COVID19, si è palesata in tutta la sua evidenza tanto agli operatori del diritto che agli studiosi del diritto processuale, generando un acceso

[4] G. De Rugeriis, *La sfida dell'innovazioni tecnologica nel processo penale* in R. Brighi e S. Zullo (a cura di), Filosofia del diritto e nuove tecnologie, Aracne 2015, pp 497-509.

e proficuo confronto che non potrà non avere benefici effetti nella fase post emergenziale.

2. Il quadro normativo

La normativa in materia di giustizia adottata durante la pandemia da COVID19 ha raggiunto nel tempo una rilevante complessità. Nel riporcorrerne sinteticamente le tappe, porremo l'accento su un aspetto che riteniamo particolarmente interessante: poichè in un breve lasso di tempo sono stati adottati plurimi e ravvicinati decreti-legge, si è registrata una informale quanto proficua interlocuzione "botta e risposta" tra legislatore e operatori del diritto che non si era mai conosciuta in precedenza, o almeno non in questa modalità. Spesso, infatti, con un nuovo decreto si agiva sul precedente per rispondere ai dubbi interpretativi o alle criticità che l'applicazione pratica aveva evidenziato. Questo fenomeno, in altre parole, ha facilitato l'emersione delle aspettative e dei timori verso le nuove tecnologie di tutti gli attori del processo penale, ed è questo un lascito importante per il Governo chiamato dalla legge 27 settembre 2021, n. 134 ad adottare, tra l'altro, anche i decreti legisltivi in materia di processo penale telematico.

2.1. *La legislazione primaria*

La primissima norma di rango primario adottata fu il d.l. 2 marzo 2020, n. 9 che stabiliva il rinvio d'ufficio delle udienze dei procedimenti civili e penali, tranne alcune eccezioni, nonché la sospensione di termini processuali e della prescrizione, dal 3 marzo 2020 al 31 marzo 2020 per quella che all'epoca era la c.d. zona rossa.

L'articolo 10, comma 12, introduceva per la prima volta la possibilità temporanea di utilizzare le ICT oltre i limiti ordinari per svolgere attività da remoto. Per le udienze non rinviabili, infatti, si prevedeva il ricorso, ove possibile, alla videoconferenza o ad altri collegamenti da remoto individuati e regolati con provvedimento del Direttore generale dei sistemi informativi automatizzati del Ministero della giustizia. Per mediare tra l'esigenza di svolgimento di dette udienze e la tutela dei diritti processuali si prevedeva l'applicazione delle disposizioni di cui al comma 3 (contestuale, effettiva e reciproca visibilità delle persone presenti in luoghi diversi e possibilità di udire quanto viene detto), al

comma 4 (colloqui riservati tra imputato e suo difensore, se presenti in luoghi diversi, per mezzo di strumenti tecnici idonei) e, in quanto compatibili, al comma 5 (equiparazione tra luogo del collegamento e aula di udienza) dell'articolo 146 *bis* "Partecipazione al dibattimento a distanza" delle norme di attuazione del cpp.

A distanza di pochi giorni l'incalzare degli eventi portò ad adottare il d.l. 8 marzo 2020, n. 11 per tutto il territorio nazionale. Semplificando si può dire che il modello delineato era bifasico: ad un primo periodo c.d. di contenimento in cui si prevedevano la sospensione di termini processuali e rinvii di udienze stabiliti direttamente dal legislatore (dal 9 al 22 marzo 2020), seguiva un periodo c.d. di convivenza nel quale azioni graduate in base alla situazione locale, da selezionare all'interno di un perimetro delineato dal legislatore stesso, potevano essere assunte dai capi degli uffici giudiziari in accordo con autorità sanitarie e classe forense (dal 23 marzo al 31 maggio 2020).

A distanza di una decina di giorni, con il d.l. 17 marzo 2020, n.18, per il quale all'epoca fu coniato il suggestivo appellativo di "Cura Italia", le misure in precedenza adottate furono meglio specificate, trovando un assetto per così dire "evoluto", benché ancora non definitivo. Fu esteso il periodo temporale della sospensione sino al 15.04.2020, poi prorogato al 11.05.2020, mentre il susseguente periodo di convivenza passò dal 16.04.2020 (poi 12.05.2020) al 30 giugno 2020.

La logica che sorregge l'articolo 83 del d.l. n. 18 resta invariata: rinvio dei procedimenti qualora non si verifichi una compressione dei diritti processuali o sostanziali eccessivamente ingiusta o pericolosa, e svolgimento delle attività non rinviabili con modalità da remoto, favorendo nel massimo grado l'utilizzo degli strumenti tecnologici a disposizione, al fine di limitare la compresenza dei diversi operatori del diritto e delle parti interessate.

Le prescrizioni relative all'utilizzo delle nuove tecnologie per il processo penale, possono essere raggruppate in due famiglie: trasmissioni documentali telematiche con valore legale (categoria nella quale includiamo tanto il deposito di atti e documenti quanto le comunicazioni e notificazioni), e partecipazione a distanza alle udienze e più in generale alle attività giudiziarie che richiedono la presenza delle parti interessate.

Quanto alle trasmissioni telematiche da un lato i commi 13, 14 e 15 prescrivono l'utilizzo della Posta Elettronica Certificata (PEC) o di altri strumenti telematici per effettuare le comunicazioni o le notificazioni relative agli avvisi e ai provvedimenti adottati per contenere gli effetti

dell'epidemia sui procedimenti penali, dall'altro i commi 12 *quater.1* e 12 *quater.2* introducono la possibilità di deposito presso l'ufficio del pubblico ministero tramite due distinti portali web, uno per i difensori e un altro per la polizia giudiziaria, di cui si dirà. In questa fase della c.d. prima ondata della pandemia, tuttavia, l'attivazione del deposito a mezzo portale è legata ad un articolato meccanismo che prevede la richiesta del Procuratore della Repubblica, l'accertamento dell'idoneità tecnologica da parte del Direttore generale SIA e l'adozione di un decreto da parte del Ministro della giustizia.

Quanto alla trattazione dei procedimenti penali con soggetti collegati a distanza viene ribadita al comma 12 per le persone detenute. Un ampliamento significativo è previsto al comma 12 *bis* che ne contempla la possibilità per le udienze penali che non richiedono la partecipazione di soggetti diversi dal pubblico ministero, dalle parti private e dai rispettivi difensori, dagli ausiliari del giudice, da ufficiali o agenti di polizia giudiziaria, da interpreti, consulenti o periti. Deve sottolinearsi che un correttivo in senso restrittivo è stato inserito in questo comma dall'articolo 3 del d.l. 30 aprile 2020, n. 28, che ha escluso la partecipazione a distanza, salvo che le parti vi acconsentano, per le udienze di discussione finale e per quelle nelle quali devono essere esaminati testimoni, parti, consulenti o periti. È facile comprendere che si tratta di situazioni nelle quali assicurare la pienezza del contraddittorio garantita dalla presenza fisica è stata ritenuta esigenza processuale non comprimibile. Per l'udienza da remoto il legislatore comunque ribadisce il principio cardine per cui «lo svolgimento dell'udienza avviene con modalità idonee a salvaguardare il contraddittorio e l'effettiva partecipazione delle parti». Principio che si traduce nel dovere per il giudice di accertare che sia sempre attivo il collegamento tra le parti, disponendo la rinnovazione degli atti qualora tale collegamento non fosse stato in concreto idoneo a permettere un'efficace interlocuzione ai soggetti del giudizio.

Giova evidenziare come il legislatore sia stato contrario a svincolare del tutto l'udienza dalla presenza fisica nell'ufficio giudiziario: l'ausiliario del giudice deve necessariamente esservi presente per redigere il verbale d'udienza (analogico) nel quale dà atto delle modalità di collegamento da remoto utilizzate, delle modalità in cui è stata accertata l'identità dei partecipanti, dell'impossibilità di sottoscrivere il verbale e di vistarlo a norma del cpp. Si tratta di scelta forse inevitabile allo stato tecnologico attuale, che tuttavia esemplifica bene come la gestione

ibrida favorisca un dettato normativo macchinoso che insegue le regole disegnate per un processo interamente analogico.

Altre ipotesi di partecipazione a distanza sono, infine, previste al comma 12 *ter* per la Cassazione; 12 *quater* per le indagini preliminari e 12 *quiquies* per le delibazioni collegiali in camera di consiglio.

Altro tassello importante per il progressivo ampliamento delle ICT nel processo penale è stata l'adozione del decreto legge 19 maggio 2020, n. 34 battezzato "Decreto rilancio" che apre una terza fase che potremmo definire di "primo parziale consolidamento". L'articolo 221 di tale d.l., infatti, detta al comma 11, concernente il deposito presso gli uffici del pubblico ministero nella fase delle indagini preliminari, una norma non soggetta a limite temporale. Tale comma non innova il sistema differenziato per difensori e polizia giudiziaria già presente nell'articolo 83, così come continua a prescrivere un decreto di avvio del Ministro della giustizia (che diventa unico nazionale), ma la natura non temporanea di tale norma primaria è una novità di per sé di grande rilievo.

Sull'assetto sin qui delineato, si è abbattuta nell'autunno del 2020 la c.d. seconda ondata dell'epidemia da COVID19. In questa reiterata emergenza sanitaria acuta, l'esperienza dei mesi precedenti ha consentito da un lato di evitare qualunque sospensione generalizzata dei procedimenti con il conseguente rinvio delle udienze e dei termini processuali, dall'altro di accrescere l'utilizzo delle ICT quale soluzione per evitare spostamenti e accesso agli uffici giudiziari, di nuovo potenziando sia le trasmissioni telematiche con valore legale di atti e documenti, che la trattazione da remoto per le attività che prevedono la presenza delle parti.

Nel giro di una decina di giorni due nuove misure hanno delineato il volto della giustizia nella nuova recrudescenza della pandemia: il d.l. 28 ottobre 2020, n. 137 c.d. "Decreto ristori", e il d.l. 9 novembre 2020, n. 149, ma è soprattutto il primo che rileva per l'analisi che stiamo conducendo. Con l'articolo 23 vengono reintrodotti gli strumenti per la partecipazione a distanza: al comma 2 per le attività della fase di indagini preliminari che richiedono la presenza delle persone interessate, introducendo la significativa novità che il difensore della persona indagata possa opporsi; al comma 4 per la partecipazione alle udienze dei detenuti, internati e persone in stato di custodia cautelare; al comma 5 in via generale per le udienze penali salve le eccezioni previste e con margini per il difensore di opporsi; al comma 9 per le deliberazioni collegiali in camera di consiglio. È soprattutto l'articolo 24, tuttavia, relativo alle

disposizioni per la semplificazione delle attività di deposito di atti, documenti e istanze che contiene le novità più rilevanti. Anche nella prima ondata della pandemia si era incentivato il ricorso ai mezzi telematici per le notificazioni e comunicazioni (dei provvedimenti e avvisi adottati per fronteggiare emergenza), nonché per i depositi, ma questo avviene ora in grado decisamente maggiore.

È importante sottolineare come, nel riconoscere quali canali idonei al deposito con valore legale da un lato i portali e dall'altro la PEC, viene innegabilmente delineato uno scenario che molto opportunamente preferisce i primi alla seconda, ammessa sì, ma solo fino a quando non potrà essere progressivamente esteso il numero di atti depositabili via portali. Nel dettaglio i primi tre commi dell'articolo 24 sono dedicati alla già prevista possibilità di deposito mediante portale di memorie, documenti, richieste e istanze presso l'ufficio del pubblico ministero dopo la chiusura delle indagini preliminari. Le novità di rilievo sono due: per il deposito telematico diviene obbligatorio (beninteso, fino al perdurare dello stato di emergenza) utilizzare il portale nei casi previsti; l'attivazione dello stesso viene estesa a tutti gli uffici di Procura della Repubblica eliminando la necessità del decreto del Ministro, a seguito della verifica tecnologica del Direttore generale SIA, che avevano rallentato la diffusione dei portali nella prima ondata della pandemia[5]. Di più, il comma 2 anticipa la progressiva estensione dell'utilizzo del portale del processo penale ad altri atti (e uffici), mentre il comma 6 evidenzia come non sia consentito l'invio tramite PEC per gli atti da depositarsi via partale. Significativa altresì l'introduzione, su sollecitazione della classe forense, dei commi 2 *bis* e 2 *ter* con i rimedi in caso di malfunzionamento del portale.

Quanto agli atti depositabili via PEC, proprio per la loro natura "residuale" (benché numericamente siano ad oggi la assoluta maggioranza), il loro ambito viene individuato in negativo rispetto a quelli per i quali sussiste obbligo di deposito sul portale. Qui giova aggiungere, per concludere, che perché il deposito via PEC abbia valore legale sono comunque necessarie le condizioni specifiche indicate al comma 4 (modificato): la casella PEC di provenienza deve essere inserita nel c.d. ReGIndE (registro generale degli indirizzi elettronici di cui all'articolo

[5] Prima del d.l. n. 137 avevano ottenuto l'autorizzazione ad utilizzare il portale depositi penali unicamente 8 Procure della Repubblica: Ancona, Bari, Brescia, Catania, Firenze, Napoli, Perugia e Salerno.

7 del DM 44/2011); la casella PEC dell'ufficio giudiziario di destinazione deve essere selezionata tra l'elenco delle caselle PEC appositamente create; il documento da depositare deve avere uno dei fermati previsti e deve essere firmato digitalmente.

2.2. *Il confronto tra legislatore e operatori del diritto*

È opportuno sottolineare quanto la generalizzata possibilità di deposito telematico (ossia di trasmissione telematica da parte delle parti private con valore legale) di atti, documenti e istanze a mezzo PEC sia senza ombra di dubbio una novità di portata rilevantissima. Le pressioni per ottenere questa possibilità erano state forti anche durante la prima ondata della pandemia, ma il legislatore aveva percorso per il deposito unicamente la strada dei portali, sicché le aperture in tale direzione, che pure si erano registrate, erano avvenute esclusivamente in sede locale a mezzo dei provvedimenti dei capi degli uffici, di concerto con la classe forense, di cui si è detto. Scelta condivisibile quella del legislatore della primavera 2020, a parere di chi scrive, alla luce della maggiore efficienza tecnologica della soluzione.

Ancor più forte, pertanto, è stata la sorpresa ingenerata quando "il confine" del deposito via PEC è stato aperto dal legislatore dell'autunno 2020. Una scelta così rilevante, contenuta sì in un decreto legge, ma affidata ad una formula letterale tanto aperta quanto sintetica non ha mancato di destare incertezze. All'indomani della pubblicazione del d.l. n. 137, dunque, è iniziato un acceso confronto tra gli operatori del diritto sulle novità, a cominciare dalla possibilità di utilizzare o meno la PEC per il deposito degli atti di impugnazione nel processo penale. Possibilità che, è bene ricordarlo, prima di questo d.l. era stata negata in plurimi pronunciamenti giurisprudenziali anche della Suprema Corte di Cassazione[6].

Prima di andare avanti nella disamina della questione, vogliamo chiarire che la nostra è una angolazione più sociologica che strettamente giuridica. In altre parole, più che riferire le serie argomentazioni giuridiche a favore e contro l'ammissibilità del citato deposito, qui interessa raccontare la vicenda perché sintomatica delle difficoltà da superare per introdurre le ICT nel processo penale anche in presenza di

[6] Per il panorama della giurisprudenza precedente si rinvia alla Relazioni su novità normativa dell'Ufficio del Massimario e del Ruolo, Servizio penale, della Corte di Cassazione n. 1/2021.

una norma primaria. Difficoltà di cui occorrerà tener conto quando saranno predisposti i decreti legislativi di attuazione della legge 134/2021[7], e il Goversno potrà finalmente affrontare le questioni con calma, esplorando ogni ramificazione delle norme processuali ivi incluse le norme di attuazione del cpp e i non trascurabili aspetti fiscali, cosa che non è riuscita al legislatore dei dd.ll. Covid incalzato come era dalla crisi sanitaria.

In prima battuta possiamo dire che è facile comprendere perché i dubbi siano caduti proprio sulla possibilità di presentare le impugnazioni a mezzo PEC: la disciplina codicistica prevede specifiche forme e modalità di presentazione che arrivano ad incidere sull'ammissibilità dell'impugnazione stessa. Si è dunque faticato a credere che tali forme potessero essere derogate senza espressa e inequivoca menzione da parte del legislatore di tale deroga.

A meno di una settimana dalla pubblicazione del d.l. n. 137, la prima Sezione della Cassazione si è pronunciata sull'articolo 24, comma 4, con la sentenza n. 32566 del 3.11.2020, Sandrini, RV 279727, stabilendo che:

> Va dichiarata l'inammissibilità della proposizione di motivi nuovi inviati dal p.m. via PEC alla cancelleria della Cassazione, non essendo tali modalità conformi alle disposizioni ex artt. 582 e ss. c.p.p., essendo tassativa la modalità di presentazione delle impugnazioni e non essendo stata tale modalità derogata dalle previsioni introdotte dall'art. 24, c. 4, del D.L. n. 137/2020, mancando inoltre l'individuazione, tramite necessarie norme tecniche, dell'indirizzo PEC abilitato alla ricezione e delle specifiche tecniche relative ai formati degli atti che possono essere trasmessi.

La soluzione interpretativa individuata con la citata sentenza è stata resa inattuale dalla successiva integrazione dell'articolo 24 apportata dal legislatore in sede di conversione. Ad essa va comunque riconosciuto un duplice merito: di aver dato voce alle perplessità largamente diffuse tra gli operatori del diritto, e di aver favorito tra i commentatori alla sentenza stessa[8] un approfondito dibattito sulle norme che regolano

[7] L'articolo 1, comma 13, lettera b) della legge 134/2021 prevede che nell'esercizio della delega sia seguito il criterio di "coordinare la disciplina del deposito degli atti di impugnazione con quella generale, prevista per il deposito di tutti gli atti del procedimento".

[8] Per tutti si cita l'articolo "Inammissibilità (presunta?) degli atti di impugnazione depositati a mezzo PEC nel processo penale" di Giuseppe Vitrani e Roberto Arcella, in ilProcessoTelematico.it, 27-11-2020.

oggi l'utilizzo delle ICT nel processo penale e, in particolare, sul loro rapporto con il Codice dell'Amministrazione Digitale (CAD).

La legge 18 dicembre 2020, n. 176 di conversione dei dd.ll. n. 137 e n.149, in buona sostanza ha introdotto, con i commi dal 6 *bis* al 6 *decies*, regole procedurali espresse ed articolate per il deposito telematico via PEC delle impugnazioni, la cui violazione si traduce anche in nuovi motivi di inammissibilità dell'impugnazione stessa che si aggiungono a quelli già presenti nel cpp.

In primo luogo, per rispondere alla critica più radicale sulla inadeguatezza della PEC ad assicurare la paternità dell'atto, si introduce a livello legislativo la necessità di firma digitale dell'atto in forma di documento informatico, previsione che era già stata anticipata nel provvedimento del Direttore generale SIA del 9.11.2020.

Sono stati regolati, inoltre, altri aspetti generali che avevano creato incertezze interpretative, in particolare si è stabilito come debba avvenire il deposito degli allegati che eccedono la dimensione massima consentita dalla PEC; e affermato che il deposito è tempestivo a condizione che avvenga entro la fine del giorno di scadenza del termine.

In questa sede è importante sottolineare come la principale criticità della scelta (obbligata?) di ricorre alla PEC per il deposito di tutti gli atti processuali di parte fosse e resta, anche dopo la legge di conversione, quella di aver dato vita ad un sistema ibrido e non interamente automatizzato nel quale, in mancanza di strumenti tecnologici di gestione e conservazione (primo fra tutti il fascicolo informatico in ogni ufficio e in ogni stato e grado del processo penale), il compito di assicurare l'allineamento tra cartaceo e informatico è affidato giocoforza all'attività certificativa – manuale – del personale amministrativo. L'iniziale previsione generale in tal senso, contenuta sin dall'origine nel comma 5, sia per il personale di segreteria (uffici requirenti) che di cancelleria (uffici giudicanti), viene espressamente richiamata per le impugnazioni dal comma 6 novies. Le operazioni di stampa cartacea di atti pervenuti telematicamente, pertanto, assorbono un apprezzabile quantità di tempo lavoro e sono foriere di possibili errori nel flusso documentale, con inevitabili ricadute processuali.

Le regole aggiunte in sede di conversione si fermano comunque alle sole modalità di deposito nella cancelleria del giudice del provvedimento impugnato. Il legislatore nulla ha detto sugli adempimenti conseguenti al deposito dell'atto, né sulle conseguenti modalità di trasmissione al giudice *ad quem* né sulla formazione del relativo fascicolo. Gli

operatori del diritto, pertanto, richiamata la previsione per alimentare il fascicolo cartaceo dell'articolo 24, ne hanno tratta la conseguenza che la trasmissione telematica dovesse fermarsi al deposito stesso[9].

Tale interpretazione restrittiva, poi, è stata fatta propria anche dal Direttore generale degli Affari Interni del Ministero della giustizia per gli aspetti fiscali[10]. Nel silenzio del legislatore si è ritenuto che l'articolo 24 del d.l. n. 137 mirasse a garantire unicamente il rispetto del termine per proporre impugnazione, e non abbia, pertanto, inciso né sull'articolo 164, comma terzo, disp att. cpp (che pone a carico della parte impugnante le spese dei diritti per le copie effettuate dalla cancelleria quando all'impugnazione non sono allegate il numero di copie previste), né sull'articolo 272 del TU spese di giustizia DPR n. 115/2002 (che per il caso in esame triplica l'ammontare ordinariamente dovuto). I difensori che abbiano depositato la loro impugnazione a mezzo PEC, pertanto, dovranno pagare l'importo dei diritti di copia triplicato, a meno che i singoli uffici non adottino soluzioni organizzative che consentano, nel rispetto delle misure di contenimento dell'emergenza sanitaria, il deposito in cancelleria delle copie cartacee dell'atto di impugnazione trasmesso via PEC.

Se ben si comprende la difficoltà di disapplicare norme fiscali in assenza di espressa previsione legislativa, pure non si può negare come la necessità di pagare somme maggiorate ovvero di accertare come ciascun singolo ufficio abbia eventualmente regolato il deposito successivo delle copie cartacee, sia in grado di scoraggiare il difensore che volesse utilizzare la PEC per depositare un atto di impugnazione malgrado l'espressa facoltà a lui riconosciuta dal legislatore dell'emergenza.

2.3. *Le nuove tecnologie nella legge 27 settembre 2021 n. 134*

Molto presto, sin dai giorni più difficili della pandemia, si è iniziato ad auspicare tra gli addetti ai lavori che l'esperienza di un maggior utilizzo delle ICT nel processo penale divenisse sistemica. Speranza non vana a leggere la legge 134/2021 che, come noto, rappresenta un intervento di ampio respiro che modificherà in modo rilevante l'intero assetto del processo penale. L'occasione ideale, dunque, per accrescere in modo

[9] Si veda nota 6.

[10] Nota n. 53167.U del 12.03.2021 disponibile al seguente indirizzo: Direttiva_ ministeriale_deposito_atti_impugnazione_caselle_PEC_copie_e_pagamento_diritti.pdf (ordineavvocati.bari.it).

meditato il ricorso alle ICT soppesando a fondo il loro effetto sulle dinamiche processuali.

Già l'originario disegno di legge, che era stato presentato nel marzo del 2020 dall'allora Ministro della giustizia Alfonso Bonafede, conteneva norme relative al PPT, ma esso prevedeva un sistema basato sulla generale facoltatività del deposito telematico e sulla mera possibile individuazione, sulla base di un DM, di specifici uffici e tipologie di atti per i quali prevedere il deposito obbligatorio (art. 2, lett. a e lett. b).

Il 24 maggio 2021 la Commissione Lattanzi, istituita dalla nuova Ministra della giustizia Marta Cartabia per elaborare proposte di emendamenti al disegno di legge Bonafede, ha ribaltato tale impostazione e introdotto il principio generale della obbligatorietà dell'utilizzo di modalità digitali sia per il deposito di atti e documenti che per le comunicazioni e notificazioni, mentre l'impiego di modalità non telematiche rappresenterà l'eccezione. Tale impostazione è stata confermata dallalegge in esame.

Le disposizioni di interesse per noi sono contenute nell'articolo 1, comma 5 (Processo penale telematico), comma 6 (Notificazioni all'imputato), comma 8 (Utilizzo delle videoregistrazioni e dei collegamenti a distanza), nonché nell'articolo 2, commi 18 e 19 (Transizione digitale) e commi 20 e 21 (Commissione di esperti).

Con il comma 5 vengono stabiliti i principi e i criteri direttivi cui dovranno dare attuazione i decreti legislativi sul PPT. Benché, come già evidenziato, la trasmissione telematica diventi la regola (con possibili eccezioni), la lettera a) di questo comma stabilisce che i documenti possono essere formati e conservati anche digitalmente, non che debbano essere sempre nativi digitali. Il legislatore delegato, dunque, non ha avuto un mandato cogente a rendere interamente informatico l'intero ciclo di vita del processo penale, bensì può ancora progettare forme ibride di originali analogici che vengano poi digitalizzati per la trasmissione. Dispiace non si sia osato di più, soprattutto perché alla lettera c) del medesimo comma, molto opportunamente, viene prescritto un regime transitorio che tenga conto dei molteplici aspetti coinvolti non solo tecnologici ma anche umani (idonea formazione). L'eccezione al deposito telematico per gli atti che le parti compiono personalmente avrebbe egualmente potuto costituire il limite all'obbligo di atti nativi digitali.

Quanto al mezzo di trasmissione telematica la lettera f) del comma 5 prevede che esso possa avvenire anche mediante soluzioni tecnologiche diverse dalla PEC che, tuttavia, attraverso la generazione di un mes-

saggio assicurino il perfezionamento del deposito. Pur nella neutralità tecnologica che ben si addice ad una legge delega, il rinvio al sistema dei portali sperimentato durante la pandemia sembra inequivoco.

Altro tema che torna dall'esperienza della normativa emergenziale è quello dei rimedi al malfunzionamento dei sistemi. La lettera e) del comma 5 ripropone la necessità di modalità di deposito alternative in caso di malfunzionamento, l'accertamento preciso dello stesso, e forme di pubblicità adeguata.

Quanto al processo a distanza, che come illustrato ha avuto un ruolo tanto rilevante nell'emergenza pandemica, la legge prevede al comma 8, lettera c) che nell'esercizio della delega dovranno essere individuati i casi in cui la partecipazione all'atto del procedimento e all'udienza possa avvenire a distanza, individuando come condizione necessaria il consenso delle parti. Un principio espresso in via così generale, senza correttivo alcuno che lo ancori a situazione nelle quali in concreto si possa temere una lesione dei diritti processuali a causa della presenza in luoghi diversi, rischia di diventare una insuperabile barriera al processo a distanza.

Per facilitare l'avvento del PPT, infine, con l'articolo 2 si prevede da un lato l'adozione di un piano triennale per la transizione digitale della amministrazione della giustizia (commi 18-19), e dall'altro la costituzione un Comitato tecnico-scientifico quale organismo di consulenza e supporto nelle decisioni connesse alla digitalizzazione del processo (commi 20-21).

3. Il quadro tecnologico

Il quadro normativo primario tratteggiato nel paragrafo precedente è una componente fondamentale per l'assetto delle ICT nel processo penale dell'emergenza, ma certamente non l'unica. Lo scenario che stiamo delineando sarebbe del tutto parziale se non si desse conto delle soluzioni tecnologiche in concreto dispiegate.

I plurimi provvedimenti del Direttore generale dei sistemi informativi automatizzati del Ministero della giustizia adottati in ottemperanza ai dd.ll. sopra esaminati, sono una buona chiave di lettura perché ancorati agli applicativi che erano disponibili e a ciò si è potuto rapidamente realizzare.

3.1. *Il processo penale a distanza*

Prima dell'emergenza pandemica nel nostro ordinamento erano già presenti ipotesi di collegamento a distanza, ma si tratta di ambiti limitati. È importante sottolineare, perché incide sulla soluzione tecnica, come nelle ipotesi ordinarie l'aula d'udienza mantiene la sua centralità: tutte le parti sono ivi presenti tranne l'imputato/i (ed eventualmente i loro difensori) che si collegano da remoto, principalmente da istituti di detenzione.

Dal punto di vista tecnologico per effettuare tali collegamenti è stato dispiegato un robusto e collaudato sistema di multivideoconferenza per collegare aule di udienza e istituti penitenziari: 360 tra aule e sale collegabili tra loro, con la possibilità di visibilità reciproca fino a 20 aule e sale. Il sistema assicura la effettiva e reciproca visibilità e possibilità di ascolto, nonché colloqui riservati tra imputato e difensore. Le risorse disponibili erano parametrate al limitato utilizzo del sistema pre-pandemia.

La normativa COVID, come già ricordato, per un verso ha accresciuti gli ambiti nei quali è possibile ricorrere a collegamenti da remoto per svolgere attività processuale (attività d'indagine, udienze pur con eccezioni, camera di consiglio, Cassazione) per altro verso ha ampliato i luoghi da cui è possibile collegarsi (uffici di polizia giudiziaria; studio del difensore; da casa per i magistrati) tanto che si è parlato di frammentazione della scena processuale.

L'impatto sulle soluzioni tecnologiche da dispiegare è stato duplice perché è stato necessario garantire sia un numero di collegamenti di gran lunga superiore al passato, sia individuare mezzi che fossero in grado di collegare luoghi di natura diversa incluse private abitazioni.

La necessità, peraltro, di reperire tali risorse in tempi rapidissimi ha spinto il DGSIA a ricorre a prodotti disponibili sul mercato, prodotti che erano già stata acquistati per attività strumentali (riunioni, formazione ecc.), di cui è stata accresciuta le personalizzazioni per renderli idonei alle attività giurisdizionali.

I sistemi disponibili sono individuati oggi dal provvedimento del Direttore generale SIA n. 10632 del 2 novembre 2020.

Il primo sistema, denominato MVC1 (Multi-Video-Conferenza)[11] era il solo utilizzato per il procedimento penale prima dell'emergenza.

[11] Per un approfondimento su questa tematica si rinvia a "Dall'udienza penale a distanza all'aula virtuale", di Sebastiano Napolitano, Sistemapenale n. 7/2020 del 06.07.2020, https://www.sistemapenale.it/it/articolo/napolitano-dalludienza-penale-a-distanza-allaula-virtuale-microsoft-teams.

Si tratta di un sistema che poggia sul servizio di connettività della pubblica amministrazione SPC2, basato su piattaforma AVAYA-Equinox, che consente il collegamento audiovisivo con canale di comunicazione criptato. La rete telematica dedicata è interna alla Rete Unitaria Giustizia, ha una sala di regia dedicata, e il sistema di gestione e controllo su infrastruttura dell'Amministrazione. La criticità è nelle sue limitate potenzialità: può essere utilizzato al massimo per 75 procedimenti in contemporanea[12].

Il secondo sistema, denominato MVC2, è un prodotto di mercato: la piattaforma Microsoft Teams, acquistato mediante la convenzione della Consip "Microsoft Enterprise Agreement 4" del 2016. Rispetto al prodotto base la DGSIA ha richiesto specifiche personalizzazioni per aumentare la sicurezza quali un sistema di gestione e controllo su cloud ubicati nel territorio dell'Unione Europea e amministrate dalla DGSIA che detiene in via esclusiva le chiavi di accesso ai log di sessione. Il servizio è reso con canale di comunicazione criptato su rete telematica pubblica utilizzabile sia dall'interno sia dall'esterno della Rete Unitaria Giustizia, senza sala regia. Il vantaggio di questa soluzione è la sua grande disponibilità, nonché l'elevato numero di possibili partecipanti, sino ad un massimo di 250, con la visibilità contemporanea, allo stato, di 9 di essi.

Anche il terzo sistema disponibile, MVC3, la piattaforma Microsoft Skype for Business, è un prodotto di mercato acquistato attraverso la medesima Convenzione Consip del precedente. Anche qui il servizio è reso con canale di comunicazione criptato su rete telematica pubblica utilizzabile sia dall'interno sia dall'esterno della Rete Unitaria Giustizia, senza sala regia, con un sistema di gestione e controllo in data center dell'Amministrazione; assicura il collegamento audiovisivo a distanza sino ad un massimo di 250 partecipanti e con la visibilità contemporanea di 5 di essi.

L'estensione dei casi di partecipazione a distanza per le udienze penali ha suscitato grande preoccupazione tra gli operatori del diritto e gli studiosi perché rischia di compromettere il principio di oralità, di immediatezza, il contraddittorio sulla prova, il diritto di difesa stesso. Le

[12] In sostanza i collegamenti avvengono tra un'aula d'udienza detta "Aula Master" e una o più salette presso istituti penitenziari o anche altre aule di diversi uffici giudiziari. Il Sistema è stato progettato sia per garantire massima sicurezza che esperienza d'uso qualitativamenteadeguata (attraverso un canaletrasmissivo di ampiezza adeguata). Gli apparecchi sono integrati in un sistema di domotica che consente il monitoraggio da una unica cabina di regia (remotizzazione dei servizi).

perplessità, dunque, diventano tanto più forti quanto più si utilizzino collegamenti da remoto per svolgere le attività che rappresentano il cuore del processo accusatorio quali l'istruttoria dibattimentale, ragione per la quale si ricorderà, il legislatore dell'emergenza ha finito per escludere le udienze di discussione finale e quelle nelle quali devono essere esaminati testimoni, parti, consulenti o periti.

La tematica è tanto seria quanto complessa, qui ci limiteremo a porre l'accento sull'importanza della qualità del collegamento: è evidente che la perdita della connettività si traduce in interruzioni del procedimento che possono arrivare a compromettere l'attività processuale. Il problema non è di facile soluzione perché la larghezza della banda internet dipende dai luoghi da cui ci si connette che possono includere abitazioni private e studi professionali. Non meno critica può rivelarsi la mancanza di conoscenze adeguate tra i partecipanti all'udienza per far fronte alle difficoltà tecnologiche; dovrà perciò investirsi su una idonea formazione, su manuali utenti, nonché su adeguati servizi di supporto tecnico da remoto.

La tematica non è evidentemente limitata al nostro ambito nazionale. Molto interessanti per approfondire le problematiche tecnologiche sono gli studi sulla "Remote Criminal Justice" fioriti nei paesi anglosassoni nei quali, seguendo la connaturata vocazione empirica, sono stati sviluppati sia progetti di studio fondati sulla celebrazione di udienze virtuali[13], che condotte ricerche somministrando questionari agli utenti realmente impegnati in udienze a distanza[14].

3.2. *Le trasmissioni telematiche: Portali versus PEC*

Prima del Covid le trasmissioni telematiche di documenti erano già possibili, ma unidirezionalmente (verso l'esterno) e a mezzo PEC. A decorrere dal 15 dicembre 2014, infatti, le notificazioni a persona diversa dall'imputato a norma dell'art. 148 c.p.p., comma 2 *bis*, artt. 149 e 150 c.p.p. e art. 151 c.p.p., comma 2, nei procedimenti dinanzi ai tribunali e alle corti di appello, erano effettuate via PEC[15].

[13] Per lo studio commissionato dal Governo del Regno Unito si veda L. Mulcahy, "Exploring the Case for Virtual Jury Trials during the COVID-19 Crisis: An Evaluation of a Pilot Study Conducted by JUSTICE", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3876199.

14 Per l'esperienza del Texas si veda J. I. Turner, "Remote Criminal Justice", disponibile sul web all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699045.

[15] Si veda l'articolo 16 del decreto-legge 18.10.2012, n. 179, convertito con modificazioni dalla legge 17.11.2012, n. 221.

Per la trasmissione con valore legale verso gli Uffici giudiziari, invece, non vi era una previsione normativa di rango primario. Le Fonti della notizia di reato utilizzavano il Portale NDR (Notizie Di Reato) anche per anticipare la trasmissione di file documentali, tuttavia senza sostituire il deposito degli originali analogici.

Nessun valore legale, poi, veniva riconosciuto ai depositi dei difensori via PEC anche se, in via di fatto, era già iniziata una timida apertura della breccia per gli atti processuali che potremmo approssimativamente definire "non propulsivi", restando però un'alea in capo al difensore sulla effettiva efficacia del suo deposito[16].

Dopo le novità introdotte dai dd.ll. emergenziali già illustrati, l'assetto delle trasmissioni telematiche verso la Procura della Repubblica presso i Tribunali ordinari (escluse dunque le Procure presso i Tribunali per i minorenni), dove il procedimento penale si incardina, si regge su tre pilastri: il Portale NDR, il Portale Deposito Penale (PDP) e la PEC (unico sistema al momento disponibile per gli Uffici giudiziari diversi dalla Procura).

Il portale nazionale delle notizie di reato (Portale NDR)[17], è il canale di comunicazione a disposizione non solo delle Forze di Polizia, ma anche di tutte gli altri Uffici fonte (strutture nelle quali sono inseriti dipendenti con le qualifiche di Ufficiali o Agenti di Polizia Giudiziaria) che normalmente trasmettono notizie di reato alla Procura della Repubblica (es. Polizia Municipale, Aziende Sanitarie Locali, INPS ecc.). L'accesso è limitato alle Fonti che siano state preventivamente formate e abilitate dalla Procura di riferimento.

La cooperazione applicativa lo collega sia al registro ufficiale che al gestore documentale: le Fonti compilano campi che, attraverso le cd Annotazioni Preliminari, possono essere "ribaltati" in modo automatico, dopo il provvedimento di iscrizione del Procuratore, nel registro informatico denominato ReGeWEB, modulo del SICP (Sistema Informativo Cognizione Penale); le Fonti trasmettono, altresì, file che alimentano il relativo fascicolo digitale nell'applicativo TIAP-Document@ (Trattamento Informatizzato degli Atti Processuali).

[16] A titolo esemplificativo si può citare la sentenza della Cassazione, sez. 6 n. 35217 del 19.4.2017 Rv 270912, in tema di possibile efficacia, nonostante l'irritualità rispetto al modello legale ex art. 121 cod. proc. pen., della richiesta di rinvio dell'udienza per legittimo impedimento del difensore, inviata a mezzo posta elettronica certificata all'indirizzo dell'ufficio di cancelleria del giudice procedente.

[17] Il portale è accessibile all'indirizzo: https://portalendr.giustizia.it /NdrWEB/home.do.

Il provvedimento del Direttore generale SIA n. 8086 del 28 luglio 2020, stabilisce le caratteristiche tecnologiche: gli atti in forma di documento informatico contenenti le comunicazioni della notizia di reato (di cui è possibile segnalare l'urgenza), e gli atti contenenti le note informative successive (cd seguiti), devono essere in formato PDF; essere ottenuti da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti (non è pertanto ammessa la scansione di immagini); essere sottoscritti con firma digitale o firma elettronica qualificata (CAdES e PAdES)[18]. Molto stringenti i dispositivi di sicurezza per proteggere la trasmissione (algoritmi di cifratura asimmetrica e chiavi di sessione) che includono un meccanismo di cancellazione dal portale stesso dei dati trasmessi una volta completato il ciclo di trasferimento.

Il Portale PNR genera la ricevuta di accettazione nel momento in cui la comunicazione diviene disponibile nelle "Annotazioni Preliminari da Portale" di ReGeWEB. Le fonti possono ottenere in risposta informazioni sul numero del procedimento e del magistrato assegnatario.

In conclusione, può dirsi che l'attuale utilizzo del PortaleNDR rappresenti un significativo passo in avanti nella direzione del PPT. Occorre, tuttavia, evidenziare che la procedura non è ancora interamente automatizzata e digitalizzata: una volta arrivati nelle annotazioni preliminari i dati immessi e i file digitali trasmessi dalle Fonti, il provvedimento di iscrizione del Procuratore della Repubblica o suo delegato viene emesso al di fuori del sistema e su supporto analogico.

Quanto agli strumenti per il deposito dei difensori, come già anticipato nel paragrafo 2, l'attuale scenario è più articolato: l'upload dei documenti attraverso il PDP non è ancora l'unico strumento previsto, benché in prospettiva dovrebbe divenire tale. Non essendo tale sistema ad oggi compiutamente sviluppato si è fatto temporaneamente ricorso anche alla PEC.

La nuova scelta architetturale basata sull'upload, ossia sul trasferimento dei dati e dei file degli atti da depositate immessi direttamente dall'utente su una pagina web appositamente creata dal Ministero della giustizia, è una scelta tecnologicamente neutrale e più avanzata della PEC e di utilizzo molto più semplice per l'utente esterno. L'upload dei

[18] Gli allegati, invece, devono rispettano requisiti meno stringenti: essere sempre in formato PDF, ma non necessariamente sottoscritti. Tanto gli atti quanto gli allegati possono avere una dimensione massima complessiva di 30 Megabyte.

documenti prodotti dagli utenti, inoltre, facilita l'interoperabilità con i sistemi informativi automatizzati interni, e consente di avviare processi interamente automatizzati per accrescere l'efficienza del sistema a vantaggio di tutti.

Migliora, altresì, il profilo della sicurezza informatica in quanto si evita il transito di documentazione su provider esterni (gestori di posta) e si assicura una gestione documentale degli atti di rilevanza giudiziaria tutta interna al perimetro applicativo del Ministero della giustizia.

Il novero degli atti oggi depositabili via portale, come detto, è piuttosto limitato, nonostante alle originarie memorie, istanze e documenti di parte successivi alla chiusura delle indagini preliminari, contemplati nell'articolo 24 del d.l. n. 137, si siano aggiunti l'istanza di opposizione alla richiesta di archiviazione, la denuncia, la querela e la relativa procedura speciale, la nomina del difensore, la revoca e la rinuncia al mandato, introdotti con decreto del Ministro della giustizia del 13 gennaio 2021.

Le regole tecniche per l'utilizzo del portale sono stabilite con provvedimento del Direttore generale SIA, n. 1690 del 24 febbraio 2021.

Al PDP accedono i soli avvocati con ruolo attivo nel ReGIndE tramite apposita smartcard e, più di recente, con credenziali SPID, da qualsiasi dispositivo fisso o mobile. L'accesso avviene attraverso il più generale portale dell'amministrazione giudiziaria, denominato Portale dei Servizi Telematici (PST) che ospita anche servizi per il PCT e per i pagamenti telematici.

Quanto al formato degli atti, il provvedimento replica in buona sostanza quanto stabilito per gli atti del Portale NDR, con qualche specifica aggiuntiva, ad esempio dimensioni e formato del PDF.

Molto interessante, per l'effetto sulle dinamiche processuali, è l'introduzione da parte del Direttore generale dell'obbligo per il difensore di depositare insieme alla nomina un c.d. "atto abilitante", ossia un atto da cui risulti la conoscenza dell'esistenza di un procedimento relativo al proprio assistito e il relativo numero, qualora il procedimento sia ancora in fase di indagine preliminare e non sia stato emesso uno degli avvisi di cui agli articoli 408, 411 e 415 *bis* cpp.

Si può supporre che con questa previsione si sia voluto colmare il repentino divario che si era aperto tra gli atti previsti dell'articolo 24, comma 1, del d.l. n. 137, che si ricorderà sono tutti successivi all'avviso di cui all'articolo 415 *bis* cpp, e gli atti aggiunti con il DM emesso il 13.01.2021 (ai sensi dell'articolo 24, comma 2 del predetto d.l.), che possono essere antecedenti a tale momento, e tentato di trovare una

soluzione per "tutelare il segreto investigativo e scongiurare la pratica di nomine puramente esplorative"[19].

Conferme dell'intento di garantire un miglior bilanciamento degli interessi in gioco, perseguito con questa previsione, possono trarsi dall'intervento del Sottosegretaria di Stato per la Giustizia Anna Macina alla seduta della Camera dei deputati del 11 maggio 2021:

> […] attraverso il portale del processo penale telematico si attiva un canale di strutturata interazione tra difensore e ufficio requirente che non può prescindere dalla conoscenza da parte del difensore del numero del procedimento iscritto, o previo rilascio di certificazione ai sensi dell'articolo 335 del codice di procedura penale o con allegazione del cosiddetto atto abilitante. La previsione dell'atto abilitante risponde, in buona sostanza, alla finalità tecnica di assicurare il corretto esercizio del diritto di difesa nel rispetto dell'altro principio che governa la fase delle indagini preliminari, che è quello della segretezza delle medesime a norma dell'articolo 329 del codice di procedura penale.

Il provvedimento del Direttore generale SIA in esame stabilisce, altresì le condizioni e le modalità per il deposito da parte dei difensori. Requisito preliminare per ottenere la visibilità dei procedimenti ed effettuare il deposito è la preventiva annotazione nel Re.Ge.WEB della nomina del difensore, per ottenere la quale si può attivare un'apposita funzione di sollecito annotazione nomina (che non prevede allegazioni documentali). Non sfugge, dunque, l'importanza di tale inserimento, che tuttavia viene effettuata manualmente dagli operatori: una potenziale criticità per superare la quale sono state diramate agli uffici indicazioni volte ad assicurare la tempestività di questa operazione.

Una volta che sia eseguita correttamente la procedura prevista sul PDP, il sistema genera la ricevuta di accettazione del deposito che contiene, tra l'altro, la data e l'orario dell'operazione di invio rilevati dai sistemi del Ministero: è quello il momento in cui il deposito si intende eseguito ed è tempestivo, come già detto, se effetuato entro le ore 24 del giorno di scadenza. Il PDP, inoltre, consente al difensore di verificare lo stato di lavorazione del proprio deposito[20].

[19] Ordine degli Avvocati di Varese, "Memorandum Portale" reperibile all'indirizzo web: https://www.ordineavvocativarese.it/wp- conent/uploads/2021/04/Memorandum-portale-PPT.pdf.

[20] Il PDP presenta al depositante sia gli stati di attraversamento ordinari (Inviato; In transito; In fase di verifica; Accolto) che gli eventuali problemi (Rigettato: rifiuto del deposito con motivazione; Errore Tecnico: si è verificato un problema in fase di trasmissione; il difensore viene invitato ad effettuare nuovamente il deposito).

Come per il Portale NDR, anche gli atti depositati attraverso il PDP giungono in apposita area dell'applicativo ReGeWEB. Il personale amministrativo deve collegarsi e attraverso i criteri di ricerca più consoni all'organizzazione del proprio lavoro (es. il lasso temporale dall'ultima verifica effettuata) deve periodicamente monitorare i depositi sopraggiunti. Anche questa è una criticità dell'attuale sistema, foriera di possibili disfunzioni tanto maggiori quanto maggiore è il numero di persone addette al compito.

Ad avviso di chi scrive occorrerà sviluppare quanto prima una consolle in grado di fornire in automatico, con apposite funzioni di allarme, le informazioni sul numero e sulla tipologia dei depositi non ancora presi in carico. Viceversa, molto opportunamente, sono stati introdotti controlli automatici mediante OCR che verificano la corrispondenza tra le informazioni digitate dal difensore nei campi del portale e quanto indicato nell'atto depositato, e segnalano al personale le incongruenze. Con l'accettazione dell'atto depositato il relativo file va ad alimentare, in modo automatico, il corrispondente fascicolo informatico presente nell'applicativo TIAP-Document@.

Pur con tutte le sue imperfezioni, in buona misura ingenerate dalla necessità di procedere con la rapidità dettata dai tempi della pandemia, non si può negare che il PDP abbia rappresentato un significativo balzo in avanti. Il prossimo passaggio per estendere l'utilizzo del PDP in funzione di deposito riguarderà gli uffici del Dibattimento dei Tribunali ordinari per il deposito delle costituzioni di parte civile, delle liste testi, memorie e note, nonché nomine revoche e rinunce al mandato da parte dei difensori. A tale fine è stata avviata una sperimentazione presso il Tribunale di Torino.

Prospettiva ulteriore, è quella di utilizzare il PDP quale punto di accesso per la consultazione da remoto, da parte degli avvocati, dei fascicoli informatici del processo di cognizione penale presenti nel gestore documentale TIAP-Document@. A tal fine è stata avviata una sperimentazione presso gli uffici dei distretti di Milano e Palermo[21].

Quanto al deposito via PEC degli atti non ancora suscettibili di upload nel PDP, il Direttore generale SIA ha dettato le regole tecniche con un primo provvedimento, n. 10791 dal 9 novembre 2020, fornendo gli indirizzi delle circa 1.100 caselle create per gli Uffici giudiziari. Il

[21] Si veda DGSIA, "Ricognizione della digitalizzazione del processo civile e penale e della transizione digitale del ministero della giustizia", già citato in nota 3.

numero di caselle assegnate è variabile a seconda delle dimensioni degli uffici, e ciascuno di essi ha provveduto ad individuare l'articolazione organizzativa/settore cui corrisponde ciascuna delle proprie caselle. Non esiste, tuttavia, una pagina web centralizzata, navigabile, per trovare le informazioni su queste assegnazioni interne, il che ha portato i difensori ad utilizzare comunque tutte le caselle assegnate ad un determinato ufficio, creando grossi problemi di gestione, ritardi ed errori.

Il problema più serio legato al deposito via PEC, tuttavia, resta la destinazione del documento informatico depositato. L'inserimento dell'atto nel fascicolo informatico non è ad oggi possibile in tutti gli stati e gradi del processo perché non esiste per ognuno di essi un gestore documentale quale il TIAP-Document@ che è sviluppato per il solo processo di cognizione di primo grado. Vero è che nel menzionato ReGeWEB, così come nei registri delle esecuzioni penali e delle misure di prevenzione, è possibile inserire documenti informatici, ma essi non offrono le funzionalità evolute di classificazione e ricerca presenti in un vero e proprio gestore documentale.

Ad avviso di chi scrive è proprio lo sviluppo di un gestore documentale unico il tassello mancante per il PPT che andrebbe prioritariamente sviluppato.

4. Conclusioni

Il quadro normativo e tecnologico tratteggiato ha posto in luce l'impatto rilevante della legislazione dell'emergenza sul futuro del PPT. L'eredità di questa esperienza, ancora in corso, è molto evidente nella legge n. 134/2021. Non c'è dubbio che tale intervento, volto a realizzare una razionalizzazione della materia penale e accrescere l'efficienza dei servizi allo scopo di ridurre la durata del processo penale, rappresenti il contesto ideale in cui sviluppare il PPT.

Nell'anno concesso al Governo per l'esercizio delle deleghe parlamentari si potrà dedicare piena attenzione al miglior bilanciamento possibile tra le ragioni del processo e le ragioni della tecnologia. La presenza di norme abilitanti il PPT già all'interno del codice di rito rimuoverà in modo permanente il più serio ostacolo all'utilizzo delle ICT che la legislazione dell'emergenza ha solo temporaneamente scavalcato.

Al momento non è possibile fare previsioni accurate sul volto che il PPT assumerà quando i decreti legislativi saranno stati adottati, ma l'esperienza della pandemia ne ha probabilmente anticipato la sagoma.

Finito di stampare nel mese di gennaio del 2022
dalla tipografia «System Graphic S.r.l.»
via di Torre Sant'Anastasia, 61 – 00134 Roma