LE SFIDE DELLA PROVA DIGITALE: SEQUESTRI, CHAT, PROCESSO PENALE TELEMATICO E INTELLIGENZA ARTIFICIALE

di Siro De Flammineis

L'avanzamento incessante della tecnologia comporta un continuo aggiustamento della normativa e delle prassi interpretative ed applicative in tema di formazione ed acquisizione delle prove digitali. A tal proposito è in corso di approvazione in Senato il d.d.l. S 806 in tema di perquisizioni e sequestri dei dati informatici. Non solo questo, però: le sfide della prova digitale riguardano anche la realtà del processo penale telematico e la frontiera dell'intelligenza artificiale.

1. Premessa, i reati mediante tecniche informatiche e la prova digitale.

La modernità tecnologica è ormai una realtà ben presente nei perimetri della giustizia penale e, ancor prima, nelle modalità realizzative dei fatti criminali. La realizzazione di reati che coinvolgono strumenti tecnologici prima e, dopo, l'accertamento di tali fatti nell'ambito dei procedimenti penali pone al centro di ogni analisi il tema della prova digitale. Quest'ultima vive costantemente nelle dinamiche delle trasformazioni tecnologiche e, di conseguenza, anche l'analisi giuridica su questo tema conosce continue sfide interpretative, necessarie per adattare l'impianto normativo e l'attuale ordinamento a tali cambiamenti. Per cercare di affrontare alcune questioni interpretative sfidanti occorre tuttavia segnare alcuni aspetti concettuali di partenza.

Intanto, la prova digitale rilevante nel processo penale può riguardare sia fattispecie di reato ordinarie che i crimini strettamente informatici[1]. Si può cioè, formare un elemento di prova digitale nell'ambito della consumazione di un reato che non coinvolge naturalmente un apparato informatico ovvero, maggiormente, le prove

[1] Per un'analisi dei profili sostanziali e processuali dei reati informatici si veda, di recente, A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, 2023, Torino; ed ancora, C. PARODI, V. SELLAROLI, *Diritto penale dell'informatica*, Milano, 2019; AA.VV. *I reati informatici. Nuova disciplina e tecniche processuali di accertamento*, 2010, Padova.

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

digitali sono quelle evidenze che concernono la consumazione di reati realizzati con modalità informatiche.

I reati informatici (già introdotti nel Codice penale dal 1993, con la l. n. 547) sono quelli realizzati con tecniche informatiche, che ovviamente producono elementi di prova digitale che diventano essenziali per la dimostrazione di tali fattispecie. Si tratta di fattispecie di reato realizzate con modalità sempre più tecnologicamente avanzate: da semplici accessi abusivi ai sistemi informatici si è passati alle forme sofisticate di *hacking* internazionale. Queste forme di aggressione ai sistemi informatici avvengono da remoto, appoggiandosi a server ubicati nei più disparati Paesi del mondo, con un rimbalzo continuo di dati ed informazioni da uno Stato all'altro, che complicano notevolmente lo svolgimento delle indagini e l'acquisizione delle prove. Diventa, dunque, sempre più importante l'acquisizione delle prove digitali che vengono formate all'estero dove si trovano i server di appoggio alle manovre informatiche. Ciò, come detto, non riguarda comunque in modo esclusivo i reati nativi informatici, cioè di matrice prettamente tecnologica, ma anche i reati comuni: ad esempio, tra tutti, il riciclaggio è diventato un reato che può manifestarsi in modalità informatiche se si pensa agli impieghi speculativi in criptovalute dei proventi illeciti; in questo caso è il profitto del reato che viene digitalizzato e le modalità realizzative del reato sono digitali.

La gran parte dei reati, però, che occupano le scrivanie delle Procure e le aule dei Tribunali sono le truffe mediante attacchi informatici ovvero con le tecniche di *phishing* (specie se affiancato ad un virus *malware*) che servono per ottenere le credenziali di accesso a dati personali (sistemi *cloud*, conti correnti bancari, posta elettronica, etc…)[2]. Si tratta di fattispecie di reato diventate ormai seriali; con esse anche la prova digitale è diventata un elemento centrale dei percorsi investigativi che deve manovrare il pubblico ministero e con cui occorre fare i conti *quotidie*. Sms, messaggi di vario tipo, *chat*, pagine internet, *social network*, sono tutte piattaforme digitali in cui si insinuano costantemente gli inganni e sguazzano gli ingannatori per avvicinare le vittime e, ottenendone le credenziali o dati sensibili (o bloccando i sistemi di società ed aziende tramite un *ransomware*), per appropriarsi dei loro denari.

La prova digitale è la rappresentazione (per la sua conoscibilità esterna) di un fatto (art. 234 c.p.p.), ovvero tutto ciò che può essere oggetto di prova *ex* art. 192 c.p.p. incorporata in una base materiale con metodo digitale ("qualsiasi altro mezzo" per come indicato dall'art. 234 c.p.p.)[3]. Quindi la prova digitale può ritenersi equivalente al documento informatico[4]; peraltro, il documento informatico è interamente equiparato al documento analogico con riguardo ai delitti in materia di falso *ex* art. 491-*bis* c.p. Diversamente, la produzione degli *screenshot* delle *chat* o di *files* (video, foto…) non sostituisce la prova digitale; dunque, le informazioni complete di quel dato

---

[2] Sull'argomento si veda A. VELE E J. LAZZARI, *Tra reati informatici e profili processuali penali nel documento digitale*, Torino, 60, 60 ss.

[3] Sul tema, tra gli altri, L. CUOMO, *La prova digitale*, in *Prova scientifica e processo penale*, a cura di G. CANZIO E L. LUPARIA DONATI, Padova, 2022, 623 ss.

[4] Il documento informatico è stato riconosciuto equivalente al documento analogico dal punto di vista della validità ed efficacia giuridica specie con l'art. 15, co.2., della l.n. 59/1997 (c.d. legge Bassanini).

(riconducibilità soggettiva, data, ora, etc…) non offerte dalla mera riproduzione fotografica dell'immagine del dato stesso, si possono ottenere solo acquisendo in originale il *file* o comunque il contenuto informatico.

Il documento informatico è dematerializzato (cioè *file* espresso in mp3, pagina internet, *chat* contenute ad esempio sul canale *whatsapp*, etc…)[5] perché esiste a prescindere dal suo supporto, dalla sua base materiale che eventualmente lo incorpora (*hard disk*, *pen drive*, *Cd*, *Dvd*); il problema immediato è, quindi, preservarne nell'acquisizione e conservarne nell'incorporazione la sua genuinità perché è facilmente modificabile. Il pregio del documento informatico è quello di essere facilmente trasferibile da un supporto all'altro ma questo è anche il suo problema principale perché è per definizione facilmente alterabile dunque fragile. In particolare, sono facilmente alterabili i dati e le informazioni del contenuto informatico, come detto, infatti, a differenza del documento analogico il documento digitale contiene molti più dati (orario, data, luogo…). Dunque, un tema giuridico ed interpretativo centrale nell'analisi della prova digitale, ed in generale nel campo della *computer forensic*[6], è quello della sua incorporazione[7].

2. Perquisizione e sequestro della prova digitale, la riforma del d.d.l. n. 806.

Prima dell'incorporazione nella copia dei documenti informatici c'è il passaggio dell'acquisizione tramite i mezzi di ricerca della prova: perquisizione, ispezione e sequestro. La Convenzione del Consiglio d'Europa di Budapest sul Cybercrime del 23 novembre 2001, ratificata con l. n. 48 del 18 marzo 2008 impone le cautele necessarie per l'acquisizione e poi l'incorporazione e conservazione genuina di queste prove. Sono cinque le garanzie previste: 1) il dovere di conservare inalterato il dato informatico originale nella sua genuinità (garanzia prevista oggi per le ispezioni e perquisizioni, anche della P.G., negli artt. 244, co.2, 247, co.1-*bis*, 352, co.1-*bis*, 354, co.2, c.p.p.); 2) il dovere di impedire l'alterazione successiva del dato originale (garanzia prevista oggi per le ispezioni e perquisizioni, anche della P.G., negli artt. 244, co.2, 247, co.1-*bis*, 352, co.1-*bis*, 354, co.2, c.p.p.); 3) il dovere di formare una copia che assicuri la conformità del dato informatico acquisito all'originale (oggi negli artt. 354, co.2, 354-*bis* c.p.p., solo però per il sequestro dell'A.G. presso i fornitori di servizi e non presso altri come ad esempio le banche, e si prescrive anche che il supporto deve essere "adeguato"[8]); 4) il dovere di assicurare la non modificabilità della copia del documento informatico (la c.d. catena di custodia, oggi previsto nell'art. 254-*bis* c.p.p. e quindi non per tutti i tipi di sequestro); 5) la garanzia dell'installazione di sigilli informatici sui documenti acquisiti (c.d. *hash*, previsto dall'art. 260 c.p.p. ma come facoltativa per il sequestro.

---

[5] In termini generali R. BORRUSO, voce *Informatica giuridica*, in *Enc. dir. Agg.*, I, Milano, 1997.

[6] *Computer forensic* (informatica forense) è la scienza che studia le tecniche di individuazione, analisi, estrapolazione e conservazione delle prove informatiche.

[7] Cfr. P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico*, in *Cybercrime*, cit., 1308.

[8] Sul tema S. ATERNO, *Acquisizione ed analisi della prova informatica*, in *Dir. pen. proc.*, 2008, n.6).

La perquisizione informatica è disciplinata dall'art. 247, co.1-*bis* c.p.p. (introdotto dalla l. 48/2008), che impone, infatti, l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

In caso di sequestro di dati informatici presso i fornitori di servizi informatici (es anche e-mail) la legge di ratifica n. 48/2008 ha introdotto l'art. 254-*bis* c.p. che prescrive l'utilizzo di procedure di copia dei dati che garantiscano la conformità con l'originale e la loro immodificabilità.

Bisogna distinguere tra l'acquisizione dei documenti informatici *on going*, cioè dinamica, specie tramite captatore informatico e che quindi è disciplinata dalle norme sull'intercettazione telematica dall'acquisizione (e incorporazione) statica, che deve avvenire secondo le norme relative alle attività di perquisizione e sequestro. In entrambi i casi, comunque, attualmente non vi è una normativa dettagliata sulle modalità tecniche, dal punto di vista delle regole scientifiche di cautela, di acquisizione della prova informatica.

Invero, per l'incorporazione statica la modalità che garantisce il rispetto delle cautele sopra indicate è quella della creazione della c.d. *bit-stream image*, ovvero della realizzazione dell'immagine *bit a bit* del contenuto del supporto da acquisire; viene quindi formata una copia *bit a bit*, cioè viene clonato il supporto originario del documento, specie l'*hard disk*, creando un supporto identico al primo che con il sistema di sigillo digitale (c.d. *hash*) garantisce l'identità assoluta con l'originale. Benché si parli di copia, in realtà il nuovo supporto potrebbe definirsi un secondo originale, proprio perché non è il supporto che identifica il documento informatico, stante la facile trasferibilità, ma il suo contenuto.

Terza situazione sarebbe quella della perquisizione *on line*, cioè da remoto, come forma atipica di acquisizione della prova, una sorta di ibrido tra intercettazione e perquisizione perché sarebbe una forma di sorveglianza a distanza[9]. Non si intravede, però, un valido spazio operativo per questa ipotesi perché l'acquisizione mediante sorveglianza dinamica è sempre inquadrabile come intercettazione; oggi i *software* più moderni consentono sofisticate tecniche di sorveglianza, consentendo ad esempio di acquisire schermate video, monitorare la digitazione della tastiera, etc.

Ulteriore tema molto delicato e particolarmente attuale riguarda l'acquisizione delle *chat* trasmesse ad esempio sulla piattaforma *Whatsapp* o dei messaggi Sms. Si è fatto riferimento in passato all'utilizzo della norma sull'acquisizione ordinaria di documentazione *ex* art. 234 c.p.p. escludendo l'applicabilità della disciplina sul sequestro di corrispondenza (art. 254 c.p.p. che disciplina il sequestro della corrispondenza presso i fornitori dei servizi postali e telematici) che riguarderebbe solo i casi di spedizione di comunicazioni in corso e non già inviate e ricevute dal destinatario[10]. Da ultimo, però la Corte Costituzionale con la sentenza n. 170/2023 ha

---

[9] Sul tema C. CONTI – M. TORRE, *Spionaggio digitale nell'ambito dei social network*, in AA.VV., *Le indagini atipiche*, II ed., a cura di A. SCALFATI, Torino, 2019, 535 ss.

[10] Cfr. Cass., sez. V, sent. 16 gennaio 2012, rv. 272319. Si veda anche Cass., sez. VI, sent. n. 22417 del 16/03/2022, Rv. 283319 secondo cui: «In tema di mezzi di prova, i messaggi "whatsapp" e gli sms conservati nella memoria di un telefono cellulare hanno natura di documenti ai sensi

stabilito che i messaggi contenuti nelle *chat* (tra cui sicuramente quelle che viaggiano sulla piattaforma *WhatsApp*) e nelle email incorporati dentro un apparecchio telefonico o un altro supporto informatico sono da ricondursi al concetto di corrispondenza, anche se già ricevuti dal destinatario, perché la loro tutela non si esaurisce con la ricezione del messaggio da parte del destinatario *ma perdura fin tanto che esso conservi carattere di attualità e interesse per gli interlocutori,* cioè fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico". Questo interesse alla riservatezza (ricondotto alla garanzia costituzionale di cui all'art. 15 Cost.), il cui accertamento potrebbe in concreto risultare difficoltoso e lasciare eccessivi margini di discrezionalità interpretativa, deve, soggiunge la Corte, presumersi, sino a prova contraria, quando si discuta di messaggi scambiati a una distanza di tempo non particolarmente significativa rispetto al momento in cui dovrebbero essere acquisiti. È la particolare attualità, quindi il criterio individuato dalla Corte costituzionale per discernere se vi sia in concreto l'esigenza di tutela della riservatezza dei dati e dei messaggi che, quindi, in questo caso non potrebbero che essere acquisiti se non attraverso la procedura del sequestro di corrispondenza *ex* art. 254 c.p.p.[11] Su questo argomento, a breve, ritorneranno le Sezioni Unite della Cassazione, chiamate a dirimere la questione in via interpretativa (vedi *infra*).

Invero, anticipando le determinazioni di quest'ultima Corte suprema, è in corso di approvazione definitiva il d.d.l. n. S 806, presentato al Senato della Repubblica il 19 luglio 2023 che contiene, tra l'altro, importanti modifiche alla disciplina sulle perquisizioni e sul sequestro dei documenti informatici. Tale testo è stato, poi, da ultimo

---

dell'art. 234 cod. proc. pen., sicché è legittima la loro acquisizione mediante mera riproduzione fotografica, non trovando applicazione né la disciplina delle intercettazioni, né quella relativa all'acquisizione di corrispondenza di cui all'art. 254 cod. proc. pen. (Fattispecie relativa a dati – allegati in copia cartacea o trasfusi nelle informative di polizia giudiziaria – acquisiti in separato procedimento, in cui la Corte ha precisato che non è indispensabile, ai fini della loro autonoma valutabilità, l'acquisizione della copia forense effettuata nel procedimento di provenienza, né dell'atto autorizzativo dell'eventuale perquisizione)»

[11] La Corte costituzionale a sostegno della propria pronuncia richiama pronunce della Corte europea dei diritti dell'uomo che ha riportato nell'alveo della «corrispondenza» tutelata dall'art. 8 CEDU anche i messaggi informatico-telematici nella loro dimensione "statica", ossia già avvenuti (con riguardo alla posta elettronica, Corte EDU, sentenza Copland, paragrafo 44; con riguardo alla messaggistica istantanea, Corte EDU, sentenza Barbulescu, paragrafo 74; con riguardo a dati memorizzati in floppy disk, Corte EDU, sezione quinta, sentenza 22 maggio 2008, Iliya Stefanov contro Bulgaria, paragrafo 42). Indirizzo, questo, recentemente ribadito anche in relazione a una fattispecie del tutto analoga a quella oggi in esame, ossia al sequestro dei dati di uno smartphone, che comprendevano anche SMS e messaggi di posta elettronica (Corte EDU, sentenza Saber, paragrafo 48). La Corte costituzionale fissa il concetto di "corrispondenza", ritenendolo "ampiamente comprensivo, atto ad abbracciare ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza", secondo l'insegnamento della stessa Consulta, che aveva in passato già affermato che «la tutela accordata dall'art. 15 Cost. – che assicura a tutti i consociati la libertà e la segretezza «della corrispondenza e di ogni altra forma di comunicazione», consentendone la limitazione «soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge» – prescinde dalle caratteristiche del mezzo tecnico utilizzato ai fini della trasmissione del pensiero, «aprendo così il testo costituzionale alla possibile emersione di nuovi mezzi e forme della comunicazione riservata» (Corte cost. n. 2/2023).

emendato, in sede di Commissione giustizia del Senato il 15 febbraio 2024 con un articolato normativo che prevede, tra l'altro, l'introduzione nel codice di procedura penale dell'art. 254*ter*, intitolato *"Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute"*[12]. Con questa normativa si intende attribuire al Giudice per le indagini preliminari il potere di disporre il sequestro dei supporti informatici, su richiesta del p.m., salvi i casi d'urgenza, in cui il G.i.p. è chiamato a convalidare il sequestro del p.m. o della polizia giudiziaria (su richiesta dello stesso p.m.). Il meccanismo prevede, poi, che il p.m. proceda, dopo l'esecuzione del sequestro, al conferimento d'incarico per la duplicazione dei supporti informatici, che deve avvenire, con avviso alle parti, con tutte le garanzie e cautele necessarie per la salvaguardia dei dati: il comma 9 dell'articolo, infatti, sancisce che la duplicazione avviene su adeguati supporti informatici mediante una procedura che assicuri la conformità del duplicato all'originale e la sua immodificabilità. Solo dopo tale fase, cioè dopo l'analisi del duplicato informatico da parte del p.m., quest'ultimo può procedere con *ulteriore* decreto al sequestro dei dati, delle informazioni e dei programmi strettamente pertinenti al reato in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione. Questi dati sequestrabili devono essere quelli freddi, statici; qualora, invece, il pubblico ministero intenda procedere al sequestro dei dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute, lo richiede al Giudice per le indagini preliminari, che provvede con decreto motivato, disponendo il sequestro in presenza dei presupposti di cui al primo periodo e agli articoli 266, comma 1, e 267, comma 1 (cioè la disciplina delle intercettazioni).

Si intende, quindi, introdurre una strutturazione bifasica del sequestro dei supporti informatici, con un primo momento di sequestro *tout court*, motivato, dell'apparato informatico-digitale, cioè dell'*hardware* e, poi, dopo la duplicazione dello stesso, l'analisi e, quindi, il sequestro del suo contenuto. Quest'ultimo secondo momento comporta una distinzione, rimessa al p.m. ed alla sua analisi tra contenuto di dati ed informazioni sequestrabili direttamente (fotografie, file, etc…) e dati ed informazioni comunicative sequestrabili solo con un apposito provvedimento del G.i.p.

La normativa si pone, invero, sul solco tracciato dalla giurisprudenza della Corte costituzionale sopra richiamata per la differenziazione tra dati statici e dati sensibili ma rimette tale distinzione alla capacità discretiva del p.m. (eventualmente supportato da esperti tecnici), senza precisare i criteri distintivi attraverso i quali effettuare le scelte procedurali e cioè individuare i dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute: sotto tale profilo si deve aver riguardo ai principi affermati dalla Corte costituzionale e, dunque, alla giurisprudenza che si è pronunciata sul punto e quella che andrà formandosi sullo specifico tema.

Tutte le ulteriori modifiche ipotizzate dal disegno riforma della disciplina sulle perquisizioni e sequestri dei supporti informatici prevedono questo tipo di garanzia,

[12] I testi sono rinvenibili sul sito www.senato.it

ovvero il controllo del G.i.p. qualora il contenuto di tali supporti riguardi, appunto, dati inerenti a comunicazioni.

Di certo, questa disciplina inevitabilmente ingolfa il procedere delle indagini preliminari, prevedendo, pur senza un vero contradditorio anticipato tra le parti[13], un duplice intervento provvedimentale e, sempre, la formazione dei duplicati informatici con la partecipazione delle parti, a prescindere dal tipo di supporto informatico sequestrato.

Da segnalare, inoltre, la totale equiparazione, in tutte le normative che si intendono introdurre con questo disegno di legge, alla stregua delle interpretazioni sopra evidenziate, tra dispositivi informatici, sistemi informatici o telematici e memorie digitali.

Infine, sull'acquisizione dei documenti informatici all'estero: la l. n. 43 del 2015 (conversione del d.l. n. 7 del 2015) ha introdotto l'art. 234-*bis* c.p.p. sull'acquisizione dei documenti informatici all'estero[14] in aderenza all'art. 32 della Convenzione di Budapest. La norma prevede la necessità del consenso del legittimo titolare dei documenti per l'acquisizione salvo che si tratti di documenti disponibili al pubblico (*open source intelligence*). Sul legittimo titolare che dovrebbe dare il consenso deve preferirsi il riferimento al *gestore dei dati* e non chi li ha immessi nel server che potrebbe essere l'indagato e che quindi mai darebbe il consenso. Per gli Stati aderenti non c'è mai bisogno di chiedere anche l'autorizzazione dello Stato (si potrà avviare un trasferimento diretto dei dati), mentre per gli altri Stati sarà necessaria l'autorizzazione. Si tratta, quindi, di un nuovo mezzo di ricerca ed acquisizione della prova. Ovviamente anche per questa acquisizione si devono comunque adottare le cautele previste dalla convenzione di Budapest.

2.1. Le questioni in concreto e le prassi, le indagini a livello internazionale.

A fronte della disciplina prevista (e di quella in adozione) in tema di acquisizione delle prove digitali vi sono alcune questioni pratiche particolarmente problematiche dal punto di vista interpretativo.

Intanto deve ribadirsi che nel caso delle prove digitali la prova non è il supporto materiale ma il suo contenuto immateriale. La disciplina del codice di rito, introdotta con la ratifica della Convenzione di Budapest non indica le modalità concrete e operative per l'acquisizione ed incorporazione della prova digitale ma si specificano solo le cautele e le garanzie da rispettare; similmente, nessun criterio tecnico-operativo è offerto dal disegno di legge in fase di approvazione da questo punto di vista. Dunque, è compito dell'operatore giuridico procedere con l'ausilio della p.g. e degli esperti informatici, per formare valide copie forensi dei supporti ovvero acquisire prove digitali originali nel modo adeguato.

---

[13] Come invece previsto nel precedente testo del disegno di legge prima dell'emendamento.

[14] Cfr. sul tema M. TORRE, *sub art. 234bis c.p.p.*, in *Comm. Giarda-Spangher*. VI ed., Milano, 2023. In tema anche Cass., sez. VI, sent. n. 18907 del 20 aprile 2021, in CED rv. 281819.

Intanto, un passaggio pratico fondamentale, per il rispetto contemporaneamente delle garanzie di difesa e per la salvaguardia della prova acquisenda è quello della idonea e completa motivazione che deve riguardare i provvedimenti di perquisizione (anche informatica) e sequestro dei supporti probatori. La c.d. riforma Cartabia (d.l. 150/2022), nel novellare il comma 4 dell'art. 352 c.p.p. sull'obbligo di motivazione dei provvedimenti di convalida da parte del p.m. delle perquisizioni eseguite dalla p.g. e con l'introduzione del comma 4-*bis* nel medesimo articolo, che prevede la possibilità, per l'indagato e coloro nei cui confronti è stata disposta o eseguita la perquisizione, quando questa non è seguita da sequestro, di fare opposizione, ha valorizzato l'importanza di una adeguata motivazione dei decreti di perquisizione e successivo sequestro.

Così, nel caso di perquisizione e successivo sequestro che riguardi un supporto informatico poiché la motivazione del provvedimento non può non riguardare anche l'aspetto delle cautele da adottare per la salvaguardia del dato che si intende acquisire, occorre dare atto di ciò, prescrivendo alla p.g. ed agli ausiliari tecnici eventualmente nominati per tale compito di rispettare quanto previsto dal codice di rito a tal fine. Sempre in questo contesto occorre che il provvedimento contempli il necessario rispetto del principio di proporzionalità tra esigenze investigative e materiale da acquisire; un concreto motivo di opposizione al decreto in questione potrebbe essere infatti quello della violazione della proporzionalità tra quanto necessario ai fini della prova del reato e quanto effettivamente sottoposto a perquisizione e sequestro. Dunque, anche la p.g. nell'esecuzione di tali strumenti di ricerca della prova deve effettuare in concreto una selezione dell'oggetto dell'attività in modo da arrecare meno danno possibile sia al dato informatico che alle persone nei cui confronti viene svolta la perquisizione ed il sequestro. Si afferma, infatti, nella più recente giurisprudenza che: «È illegittimo, per violazione del principio di proporzionalità ed adeguatezza, il sequestro a fini probatori di un dispositivo elettronico che conduca, in difetto di specifiche ragioni, alla indiscriminata apprensione di una massa di dati informatici, senza alcuna previa selezione di essi e comunque senza l'indicazione degli eventuali criteri di selezione. (Fattispecie relativa a sequestro di un telefono cellulare e di un tablet)»[15]. Anche il successivo mantenimento in sequestro dei beni deve essere limitato ed adeguato alle concrete esigenze tecniche ed investigative; a tal proposito si afferma che: «In tema di sequestro probatorio avente ad oggetto dispositivi informatici o telematici, la finalizzazione dell'ablazione del supporto alla sua successiva analisi, strumentale all'identificazione e all'estrazione dei dati rilevanti per le indagini, implica che la protrazione del vincolo, nel rispetto dei principi di proporzionalità e di adeguatezza, debba essere limitata al tempo necessario all'espletamento delle operazioni tecniche, dovendosi, tuttavia, valutare la sua ragionevole durata in rapporto alle difficoltà tecniche di apprensione dei dati, da ritenersi accresciute nel caso di mancata collaborazione dell'indagato che non fornisca le chiavi di accesso alle banche dati contenute nei supporti sequestrati».[16]

---

[15] Cfr. Cass., sez. VI, sent. n. 6623 del 09/12/2020, Rv. 280838.

[16] Cfr. Cass., sez. II, sent. n. 17604 del 23/03/2023, Rv. 284393.

Dunque, p.m. e p.g. nel rispetto del principio di proporzionalità devono procedere con un'adeguata selezione a monte del materiale da sottoporre a sequestro e poi con un'altrettanta adeguata e spedita devono effettuare la selezione del materiale rilevante ai fini probatori tra quelli sequestrati, in modo da poter restituire agli aventi diritto, una volta formata la copia digitale, i beni in sequestro e tutto ciò che non è rilevante ai fini dell'indagine, specie se sequestrato a terzi estranei al reato[17]. In ogni caso, appare opportuno che la p.g. rediga una accurata relazione in ordine alle modalità con cui vengono eseguite le attività di perquisizione e di sottoposizione a sequestro degli strumenti informatici (si potrebbe pensare, ad esempio, visto oggi l'aumento delle previsioni di videoripresa delle attività investigative, ad una videoregistrazione delle attività da parte della p.g.) cui, poi, eventualmente seguirà altresì la relazione tecnica dell'esperto relativa alla realizzazione della copia forense. Questa refertazione appare necessaria per consentire alla difesa di vagliare le modalità esecutive dei provvedimenti giurisdizionali ai fini dell'ammissibilità delle prove acquisite *ex* art. 190 c.p.p. Inoltre, con la riforma intervenuta nel 2022 sono aumentate le occasioni di confronto tra ipotesi di accusa e tesi difensive nel corso delle indagini preliminari, in un progetto di valutazione anticipata di tutte le problematiche e questioni che possono fare insorgere dei dubbi sulla sostenibilità delle tesi accusatorie; tali occasioni poi culminano nella nuova regola processuale della ragionevole previsione di condanna di cui all'art. 408 c.p.p.[18] Ebbene, quello dell'acquisizione, analisi e copia dei contenuti informatici ai fini del loro utilizzo come prove digitali diventa un momento particolarmente centrale nel corso delle indagini preliminari per far valere eventuali dubbi, ipotesi di violazione di regole scientifiche e protocolli da parte delle difese, specie quando le prove digitali diventano elementi determinanti per il sostegno accusatorio ad ipotesi di reati commessi con modalità informatiche. Si richiede, allora, in tali situaizoni un sempre maggior impegno e partecipazione delle attività difensive in tali fasi, per poter sciogliere eventuali nodi tecnici in via anticipata, anche con l'intervento di esperti e consulenti di parte, senza che le questioni vengano trascinate in avanti e fino ad un giudizio dove le stesse problematiche dovranno essere nuovamente affrontate e risolte.[19]

Nell'ambito della valutazione sulle adeguate garanzie da adottare per la salvaguardia della prova e la tutela dei diritti e delle garanzie dell'indagato in caso di perquisizione e sequestro di documenti informatici, inoltre, si pone sovente la problematica relativa alla scelta sull'effettuazione della copia forense del supporto con

---

[17] Cfr. altresì Cass., *sez.* VI, sent. n. 34265 del 22/09/2020, Rv. 279949.

[18] Sul tema sia consentito il rinvio a S. DE FLAMMINEIS, *La valutazione dei fatti ai fini dell'archiviazione ovvero dell'esercizio dell'azione penale: poteri e responsabilità del pubblico ministero*, in *questa Rivista*, 23 maggio 2023.

[19] Su tale argomento si segnala, da ultimo, Cass., sez.VI, sent. n. 46482 del 27/09/2023, Rv. 285363, secondo cui: «In tema di prove digitali, l'indisponibilità della tecnologia di "hackeraggio" utilizzata per estrarre e mettere in chiaro la messaggistica criptata non determina alcuna lesione dei diritti di difesa, atteso che l'ordinamento interno non obbliga alla ostensione degli attrezzi virtuali con cui si sia ottenuta la decodifica di contenuti telematici, fatta salva la possibilità per l'imputato di allegare anomalie tecniche che facciano fondatamente dubitare della correttezza delle acquisizioni, e che depongano per l'inquinamento del risultato. (Fattispecie relativa ad intrusione nel server delle piattaforme "Sky-Ecc" ed "Encrochat", mediante programma "software" non reso noto per il segreto opposto dalle autorità francesi)».

le modalità garantite di cui all'art. 360 c.p.p. o, invece, con le forme semplificate dell'art. 359 c.p.p. In termini astratti, la tecnica della *bit-stream image* garantirebbe l'assoluta conformità e identità del contenuto del nuovo supporto informatico rispetto all'originale sequestrato, non vi sarebbero ragioni per considerare quindi l'attività di copia come irripetibile. Tuttavia, questa valutazione deve essere compiuta in termini concreti e caso per caso[20]. L'irripetibilità delle operazioni per lo più risulta garantita quando l'apparecchio da copiare è spento, non vi sono accessi alla rete internet e non vi sono rischi di modifiche ed alterazioni ai dati utente con l'accesso al sistema perché si hanno a disposizione i codici di accesso e le password; ciò riguarda soprattutto gli apparecchi che hanno come *software Ios*. Quando, invece, si tratta di apparecchio acceso, specie con *software Android*, l'accesso al sistema per effettuare la copia potrebbe produrre alterazioni in grado di inficiare la genuinità dei dati utente in esso contenuti; in questi casi, quindi, risulta preferibile procedere con le forme di cui all'art. 360 c.p.p.

Quanto finora detto sugli aspetti esecutivi pratici di perquisizione e sequestro di prove digitali può essere messo a confronto con le previsioni del disegno di riforma in materia già menzionato.

Ebbene, circa l'obbligo di motivazione di perquisizioni e sequestri ai fini del rispetto dei principi di necessarietà e proporzionalità, questi ultimi sono espressamente menzionati dalla nuova proposta di disciplina sopra indicata, contenuta nel disegno di legge n. S 806. Al comma 1 del proposto nuovo art. 254-*ter* c.p.p., infatti, si indica espressamente la necessità che il sequestro avvenga nel rispetto del criterio di proporzione – con connessa adeguata motivazione da parte di p.m. richiedente e giudice disponente o convalidante – e che le copie dei supporti e, cioè, la formazione del duplicato informatico avvenga con tutte le garanzie previste per le parti informate. Inoltre, il comma 2 dello stesso nuovo articolo in fase di approvazione sancisce che «il sequestro è eseguito con modalità tecniche idonee ad evitare l'alterazione o la perdita dei dati e, a tal fine, il pubblico ministero adotta le misure tecniche necessarie o impartisce specifiche prescrizioni»[21]. I medesimi principi sono ribaditi nel comma 12

---

[20] Cfr. in proposito S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, p. 223 e ss.; per la giurisprudenza, sulla ripetibilità delle operazioni di copia forense salvo valutazioni da effettuarsi in concreto si veda da ultimo Cass., sez. I, sent. n. 38909 del 10/06/2021, Rv. 282072 (conforme già Cass. sez. II, sent. n. 29061 del 01/07/2015, Rv. 264572 secondo cui: «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»).

[21] Inoltre, secondo il testo di riforma in corso di approvazione, all'articolo 354, comma 2, il secondo e il terzo periodo sono sostituiti dai seguenti: «In relazione ai dispositivi, sistemi informatici o telematici o memorie digitali ovvero ai dati, alle informazioni e ai programmi informatici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti, osservando le disposizioni di cui all'articolo 352, comma 1-*ter*, quando il sequestro ha ad oggetto dati, informazioni o programmi informatici» e dopo il comma 2 è inserito il seguente: «2-*bis*. Quando risulta

dell'articolo, quando indica al p.m. di rispettare i criteri di necessità e proporzione nel momento di disporre il sequestro dei dati a seguito della formazione del duplicato informatico.

Come detto, poi, la proposta riforma prevede sempre la formazione, nel contraddittorio tecnico delle parti, del duplicato informatico, senza distinguere tra tipologie di supporti in sequestro ed eventuali *software* in uso. Ed ancora, al comma 13 della norma si stabilisce che i dati sequestrati siano riversati su idonei supporti con modalità tecniche idonee ad assicurare la loro conformità ai medesimi dati, informazioni e programmi contenuti nel duplicato e la loro immodificabilità.

Dunque, la normativa che si intende introdurre per un verso convalida le acquisizioni giurisprudenziali finora raggiunte in tema di perquisizioni e sequestri delle prove digitali e rafforza la partecipazione delle parti private interessate nelle procedure di formazione dei duplicati informatici, in modo da anticipare eventuali questioni e problematiche sul punto. Inoltre, la normativa che si intende introdurre supera le eventuali scelte da compiersi circa l'effettuazione delle operazioni di duplicazione delle prove con le modalità garantite o senza le stesse, disciplinando una procedura di duplicazione sempre garantita[22].

Tuttavia, per altro verso, il disegno di legge, nel confermare il necessario rispetto dei principi di proporzionalità e necessarietà nell'adozione dei provvedimenti di sequestro, non offre ulteriori spunti interpretativi, rimandando alle opzioni giurisprudenziali già formate sul punto. Inoltre, la normativa non si sofferma sugli aspetti tecnici ed operativi da adottare per rispettare le garanzie di immodificabilità dei dati, vincolando solo gli operatori a formare ogni duplicato con le garanzie del contraddittorio.

A questo punto, occorre confrontarsi con un sensibile tema emerso nella prassi, proprio relativo alla problematica sopra segnalata e che la disciplina di modifica finora descritta non chiarisce del tutto, relativo all'individuazione della tipologia di dati informatici che si intendono sottoporre a sequestro. Il tema riguarda, per l'appunto, la distinzione tra prove digitali contenenti dati non comunicativi e prove che includono dati che vengono definiti dal disegno di legge citato *inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute*.

Ed invero, come detto in premessa, la realizzazione di reati con modalità informatiche avviene sempre più attraverso condotte che coinvolgono più Stati: non soltanto i *server* su cui si appoggiano gli autori degli attacchi informatici sono nella maggior parte dei casi allocati in Paesi diversi da quello in cui viene consumata

---

necessario sottoporre a sequestro un dispositivo, un sistema informatico o telematico o una memoria digitale, si applicano le disposizioni di cui all'articolo 254-*ter* e la polizia giudiziaria procede ai sensi del comma 4 dello stesso articolo.».

[22] Il comma 6 dell'articolo prevede infatti che entro cinque giorni dal deposito del verbale di sequestro, il pubblico ministero avvisa la persona sottoposta alle indagini, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione, la persona offesa dal reato e i relativi difensori, del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico per la duplicazione del contenuto dei dispositivi informatici, dei sistemi informatici o telematici, o delle memorie digitali in sequestro, e della facoltà di nominare consulenti tecnici.

l'aggressione ma questo Paese può essere anche diverso da quello dove si trova fisicamente l'autore delle condotte e ancora diverso da quello in cui vengono fatti confluire gli eventuali profitti del reato. Invero, tale circostanza non riguardano solo i reati propriamente informatici ma tutti i reati ordinari per la cui dimostrazione è necessario acquisire prove digitali che si sono formate o sono comunque allocate all'estero. Dunque, inevitabilmente le indagini che richiedono l'acquisizione di prove digitali devono spesso affrontare la necessità di acquisire le stesse all'estero, attivando le regole e le forme della cooperazione internazionale di polizia e giudiziaria.

Così, per lo svolgimento delle perquisizioni (anche informatiche) e dei sequestri di strumenti informatici all'estero occorre eseguire un ordine d'indagine europeo ovvero agire in rogatoria, rispettando le forme e le previsioni dell'ordinamento in cui tali attività vengono svolte. L'utilizzabilità, poi, delle prove così acquisite anche nel nostro ordinamento dipenderà dal rispetto di tali regole ma anche dal rispetto delle cautele previste dalla Convenzione di Budapest e ormai introitate nel nostro sistema processuale per l'acquisizione e conservazione dei dati informatici; ciò non potrà che riguardare anche i casi di acquisizione di prove digitali presso un ordinamento che non ha sottoscritto e ratificato tale Convenzione.

Sul tema dell'acquisizione di prove digitali all'estero recentemente si è posta una questione interpretativa seria ed importante relativa alla qualificazione giuridica ed alla conseguente regola processuale di apprensione delle *chat* di gruppo scambiate tra i membri mediante un sistema cifrato (nella specie Sky-ECC) e decriptate dallo Stato estero[23]. La questione è seria perché tali prove sono risultate determinanti o comunque particolarmente rilevanti per la costruzione di procedimenti aventi ad oggetto reati di criminalità organizzata in diversi tribunali d'Italia[24]. È emersa, invero, una divergenza tra interpretazioni della Corte Suprema di Cassazione laddove, secondo un orientamento, l'acquisizione di tali chat mediante ordine d'indagine europeo presso l'A.G. straniera costituisce acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-*bis* c.p.p. o di documenti *ex* art. 234 c.p.p., perché tali *chat* costituiscono dato informativo documentale conservato all'estero e non flusso comunicativo, non trovando applicazione la disciplina delle intercettazioni di cui agli artt. 266 e 266-*bis* c.p.p. e non essendo necessario un controllo sulla legittimità dell'acquisizione da parte dell'A.G. italiana[25]. Un secondo orientamento, invece, pone delle distinzioni ritenendo che

---

[23] Le questioni riguardanti la piattaforma Sky-ECC originano dall'operazione congiunta della polizia francese, belga e olandese che nel 2021 ha condotto ad accedere e decriptare le chat di oltre 70.000 utenti provenienti da diversi Paesi.

[24] Sull'argomento F. DI VIZIO, *Chat criptate e diritto processuale penale*, in *dirittogiustiziaecostituzione.it*, 21 febbraio 2024, *ivi* anche G. AMATO, *L'utilizzabilità delle chat criptate SkyEcc al vaglio delle Sezioni Unite: analisi del dibattito e prospettive di riforma del codice di rito*, 21 febbraio 2024 e F. NICOLOCCHIA, *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla* querelle *giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, in *questa Rvista.*, n. 2/2024.

[25] Cfr. Cass., sez. IV, sent. n. 16347 del 05/04/2023, Rv. 284563 In motivazione, la Corte ha chiarito che non rileva se i messaggi siano stati acquisiti dall'autorità giudiziaria straniera "ex post" o in tempo reale, poiché al momento della richiesta i flussi di comunicazione non erano in atto. Tale orientamento distingue tra l'operazione di captazione del messaggio cifrato in transito verso il destinatario e le operazioni di

l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma "SKY-ECC" non costituisce dato informatico utilizzabile ai sensi dell'art. 234-*bis* c.p.p., sicché, in tale ipotesi, l'attività acquisitiva, se riguardante comunicazioni avvenute nella fase "statica", deve essere inquadrata nelle disposizioni in materia di perquisizione e sequestro e, in particolare, in quella di cui all'art. 254-*bis* c.p.p., mentre se avente ad oggetto comunicazioni avvenute nella fase "dinamica", deve essere inquadrata nella disciplina degli artt. 266 e ss. c.p.p. in materia di intercettazioni telematiche[26]. Inoltre, si ritiene, sempre secondo questo orientamento che per l'utilizzabilità di tali prove sia necessario un controllo da parte dell'A.G. italiana se sussistevano le condizioni originarie per l'autorizzabilità in sede giurisdizionale delle relative attività investigative oggetto degli ordini europei.

Dunque, ancora una volta, la questione riguarda il rapporto tra acquisizione di documento, sequestro di corrispondenza ed attività di intercettazioni. Per dirimere tale contrasto la III^ Sezione della Cassazione, con ordinanza n. 47798 del 30.11.2023 ha rimesso alle Sezioni Unite le questioni riguardanti soprattutto: a) la disciplina applicabile per l'acquisizione di chat criptate dall'estero (Sky-ECC), ovvero se il trasferimento all'Autorità giudiziaria italiana, in esecuzione di ordine europeo di indagine, del contenuto di comunicazioni effettuate attraverso criptofonini e già acquisite e decrittate dall'Autorità giudiziaria estera in un proprio procedimento penale, costituisca acquisizione di documenti e di dati informatici ai sensi dell'art. 234-*bis* c.p.p. o di documenti *ex* art. 234 c.p.p. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove; b) la necessità di una verifica di legittimità di tale acquisizione da parte dell'Autorità giurisdizionale italiana e c) se tale acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati in tal modo versati in atti, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte della Autorità Giurisdizionale nazionale che ha emesso l'o.i.e.

---

acquisizione e decriptazione del contenuto già inoltrato, ritenendo applicabile solo al primo caso la disciplina delle intercettazioni, in quanto flussi di comunicazioni *ex* art. 266*bis* c.p.p. I messaggi ormai inviati e ricevuti, invece, rappresenterebbero una mera documentazione di tali flussi comunicativi, utilizzabili come prova allorquando vi sia la disponibilità della chiave crittografica che consenta di decifrarne il tenore ed acquisibili dal p.m. tramite un O.I.E. grazie all'art. 234*bis* c.p.p. Inoltre, questa opzione giurisprudenziale ha sostenuto che nessun controllo deve essere effettuato dal Giudice italiano rispetto alla prova acquisita nell'ambito del procedimento giurisdizionale estero perché l'attività di acquisizione è stata eseguita secondo la legislazione dello Stato estero, di propria iniziativa e non su richiesta dell'A.G. italiana

[26] Cfr. Cass., sez. VI, sent. n. 44155 del 26/10/2023, Rv. 285362. Nello stesso filone interpretativo soggiunge ancora la Cassazione che: «In tema di prove informatiche, l'art. 234-*bis* cod. proc. pen. – che, a fini di contrasto al terrorismo, ha trasposto la regola di cui all'art. 32 della Convenzione sul "cybercrime", ratificata con legge 18 marzo 2008, n. 48 – non è applicabile nel caso di prove documentali acquisite mediante ordine europeo di indagine (nella specie, messaggistica tratta dalla piattaforma criptata "Sky Ecc"), in quanto tale norma consente di acquisire documentazione digitale reperibile in rete da fonti aperte, salva la necessità di consenso del titolare del documento in caso di accesso protetto, senza il ricorso a procedure di collaborazione con lo Stato ove i documenti geograficamente si trovano», così Cass., sez. VI, sent. n. 46482 del 27/09/2023, Rv. 285363.

Con decisione del 29 febbraio 2024[27] le SS.UU. hanno stabilito, con riguardo al primo quesito che il trasferimento di cui sopra rientra nell'acquisizione di atti di un procedimento penale che, a seconda della loro natura, trova alternativamente il suo fondamento negli artt. 78 disp. att. cod. proc. pen., 238, 270 cod, proc. pen. e, in quanto tale, rispetta l'art. 6 della Direttiva 2014/41/UE; mentre con riguardo al secondo quesito che non sia necessaria tale verifica, rientrando nei poteri del pubblico ministero quello di acquisizione di atti di altro procedimento penale; con riferimento alla terza questione si è deciso che l'Autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo.

In attesa delle motivazioni che sorreggono le decisioni sopra indicate contenute nella pronuncia delle SS.UU. – che fa il pari con quanto dovranno decidere le stesse SS.UU. sul tema già sopra segnalato della qualificazione giuridica delle chat – non può che ritenersi che le indicazioni derivanti dalla pronuncia della Corte costituzionale n. 170/2023, sul rispetto delle garanzie previste dall'art. 15 della Costituzione necessariamente illuminano anche la qualificazione della *natura* degli atti del procedimento, da cui deriva in concreto la disciplina applicabile, per come statuito dalle Sezioni Unite[28]. In effetti, se la comunicazione anche in fase statica, cioè già avvenuta e non in corso tra due o più persone deve qualificarsi come corrispondenza anziché mero documento, allora la garanzia costituzionale deve estendersi ad ogni mezzo che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, dovendo procedersi agli strumenti della perquisizione e del sequestro per la legittima acquisizione del dato comunicativo rappresentato digitalmente.

Tale interpretazione, poi, appare essere quella sposata in sede di proposta di riforma come sopra rimarcato, con la prevista introduzione dell'art. 254-*ter* nel codice di rito.

Piuttosto, qualora, come avvenuto per il caso francese, si intenda acquisire queste comunicazioni direttamente a monte sul *server* del fornitore del servizio dove vengono alloggiate, in modo da evitare i sistemi di criptazione che intervengono al momento dell'uscita del dato dallo stesso *server*, viene in rilevo un'ulteriore garanzia da rispettare nel procedimento di apprensione. Il principio di proporzionalità, infatti, impone anche in questo caso che si effettui una selezione a monte dell'oggetto della ricerca probatoria, con individuazione anche dei limiti temporali della relativa apprensione e mantenimento del dato. In altri termini, non pare potersi ritenere proporzionato secondo

---

[27] Informazioni provvisorie nn. 3-4/2024, in *questa Rivista*, 1° marzo 2024. Per un commento si veda G. SPANGHER, *Criptofonini: fissati i punti di diritto*, in giustiziainsieme.it, 6 marzo 2024.

[28] Oltre a richiamare le pronunce della Corte EDU, sent. 5/09/2017, Barbulescu c. Romania, § 72; Corte EDU, sent. 3/04/2007, Copland c. Regno Unito, § 41; Corte EDU, sent. 17/12/2020, Saber c. Norvegia, § 48. Inoltre, questo orientamento valorizza l'introduzione in via d'urgenza delle disposizioni di cui all'art. 132 Codice privacy (d.l. 132/2021, convertito in l. 178/2021), con cui il legislatore ha scelto di sottoporre la procedura di acquisizione dei dati esterni di traffico telefonico e telematico nel procedimento penale (c.d. tabulati) ad un provvedimento autorizzatorio motivato del giudice.

l'ordinamento nazionale[29], qualsivoglia processo acquisitivo a strascico di flussi comunicativi tra persone perché generico e non selettivo nell'*an*, nel *quando* e nel *quantum*.

Da ultimo, la IV sezione della Cassazione, con ordinanza del 15 gennaio 2024 (dep. 18 gennaio 2024), n. 2329 ha rimesso alle Sezioni Unite una questione interpretativa similare a quella relativa all'acquisizione, mediante o.i.e., di *chat* decriptate; ovvero: «1) se l'***acquisizione***, mediante ***ordine europeo di indagine***, dei risultati di intercettazioni disposte dall'***Autorità giudiziaria estera*** su una piattaforma informatica criptata integri, o meno, l'ipotesi disciplinata nell'ordinamento interno dall'***art. 270 cod. proc. pen.***; 2) se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'Autorità giudiziaria estera attraverso l'inserimento di un ***captatore informatico*** sul "server" di una piattaforma criptata sia soggetta nell'ordinamento interno ad un ***controllo giurisdizionale***, preventivo o (ulteriore quesito) successivo, in ordine alla *utilizzabilità* dei dati raccolti».

Anche su questo tema le Sezioni Unite della Cassazione hanno assunto una decisione sempre in data 29 febbraio 2024, con motivazioni ancora non disponibili. Si è deciso in senso affermativo sulla necessità di applicare la disciplina *ex* art. 270 c.p.p. in caso di acquisizione dei risultati di intercettazioni; sulla non necessità di preventiva autorizzazione del giudice per il trasferimento di tali prove e invece sulla necessità di verifica da parte dell'Autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine del rispetto dei diritti fondamentali.

3. La prova digitale nel processo penale telematico.

Nell'ambito delle disposizioni transitorie previste dalla riforma Cartabia l'art. 87 D.lgs. n. 150/2022 ha previsto l'emanazione, entro il 31 dicembre 2023, di un decreto del Ministero della Giustizia per disciplinare il deposito telematico degli atti penali, in vista del passaggio esclusivo al portale dei servizi telematici, con conseguente progressivo abbandono degli altri canali di deposito, cartaceo e PEC, in definitiva il c.d. *processo*

[29] E, di conseguenza, tale aspetto deve essere considerato in caso di emissione di un O.I.E. Infatti, l'art. 6 della Direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014, relativa all'Ordine Europeo di Indagine penale, indica, quali "condizioni di emissione e trasmissione di un OEI", che tale emissione sia "necessaria e proporzionata" ai fini del procedimento penale "tenendo conto dei diritti della persona sottoposta a indagini o imputata", e che l'atto o gli atti di indagine richiesti nell'OEI "avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo". Entrambe tali condizioni devono essere "valutate dall'autorità di emissione per ogni caso". Anche il D.lgs. 21 giugno 2017, n. 108 (Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio), all'art. 1 detta la "Disposizione di principio", per cui esso si propone di attuare la citata direttiva "nel rispetto dei principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione europea in tema di diritti fondamentali, nonché in tema di diritti di libertà e di giusto processo".

penale telematico. In attuazione di tale delega è stato adottato il D.M. Giustizia n. 217/2023, pubblicato il giorno successivo nella Gazzetta ufficiale n. 303 del 2023, ed entrato in vigore (pur non nella sua totalità) il 14 gennaio 2024 (che ha abrogato i precedenti D.M. del 4 luglio 2023 e D.M. del 18 luglio 2023) che prevede, appunto, il progressivo passaggio al deposito esclusivo degli atti del procedimento penale tramite il portale c.d. APP.

In particolare, l'art. 3 del suddetto D.M. sancisce che il deposito di atti, documenti, richieste e memorie ha luogo con modalità telematiche ai sensi dell'articolo 111-*bis* del codice di procedura penale. A sua volta, il novellato art. 111-*bis* c.p.p. oggi prevede che: «1. Salvo quanto previsto dall'articolo 175-*bis*, in ogni stato e grado del procedimento, il deposito di atti, documenti, richieste, memorie ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione degli atti e dei documenti informatici. 2. Il deposito telematico assicura la certezza, anche temporale, dell'avvenuta trasmissione e ricezione, nonché l'identità del mittente e del destinatario, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. 3. La disposizione di cui al comma 1 non si applica agli atti e ai documenti che, per loro natura o per specifiche esigenze processuali, non possono essere acquisiti in copia informatica. 4. Gli atti che le parti compiono personalmente possono essere depositati anche con modalità non telematiche».

Infine, l'art. 2 del medesimo decreto prevede modifiche per il D.M. n. 44 del 21 febbraio 2011, inserendo l'art. 7-*bis* che dispone che: «1. Il portale dei depositi telematici consente la trasmissione in via telematica da parte dei soggetti abilitati esterni degli atti e dei documenti del procedimento. 2. Il portale delle notizie di reato consente la trasmissione in via telematica da parte del personale di polizia giudiziaria e di ogni altro soggetto tenuto per legge alla trasmissione della notizia di reato di atti e documenti su canale sicuro protetto da un meccanismo di crittografia, in modo da assicurare l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività. 3. L'accesso ai portali di cui ai commi 1 e 2 avviene a norma dell'articolo 64 del codice dell'amministrazione digitale[30] e secondo le specifiche stabilite ai sensi dell'articolo 34. 4. Il portale dei servizi telematici mette a disposizione dei soggetti abilitati esterni i servizi di consultazione, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34». Infine, il comma 9 dello stesso decreto è sostituito dal seguente: «3. Restano fermi gli obblighi di conservazione dei documenti originali unici su supporto cartaceo previsti dal codice dell'amministrazione digitale o di atti e documenti depositati o comunque acquisiti in forma di documento analogico in conformità alla disciplina processuale vigente».

La prospettiva disegnata da questa normativa appare chiara: tutti gli atti e provvedimenti del procedimento penale diventeranno per definizione documenti informatici essendo rappresentati da file inseriti in un sistema informatico e gestiti da

[30] Ovvero il decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale».

un *software* appositamente dedicato. Ciononostante, resta valida la distinzione interna al perimetro della famiglia dei documenti informatici tra quelli che vengono formati nel procedimento penale (atti e provvedimenti) e quelli che invece si formano altrove, come le prove digitali, e che vengono acquisiti come elementi di prova nel procedimento penale ma sono nativi digitali. Pertanto, mentre i primi nascono direttamente all'interno della piattaforma APP costituita per la gestione telematica del procedimento penale, i secondi devono essere inseriti nella piattaforma dall'esterno. Questo inserimento, che deve essere in concreto regolamentato, nella maggior parte dei casi potrà essere gestito direttamente dalla polizia giudiziaria che ha provveduto all'acquisizione della prova digitale. Il portale, quindi, deve consentire alla polizia giudiziaria procedente di interfacciarsi con il sistema in modo da poter caricare le prove digitali per come oggi previsto dall'art. 111-*bis* c.p.p. In effetti, la natura digitale delle prove informatiche pare poter escludere l'evenienza che talune di esse rientrino nell'eccezione prevista dal comma 3 dell'art. 111-*bis* c.p.p. prevista per quegli atti e documenti che per loro natura o per specifiche esigenze processuali non possono essere acquisiti in copia informatica.

In ogni caso, però, l'acquisizione della prova digitale, specie all'esito di un'attività di perquisizione e sequestro, dovrà pur sempre passare dall'incorporazione all'interno di un supporto contenente la copia forense dei file di interesse investigativo, non potendosi immaginare un travaso diretto della prova digitale nel portale del procedimento penale nella stessa fase della sua acquisizione. Dunque, dovrà immaginarsi uno spazio dove comunque far confluire i supporti *hardware* che contengono la prova digitale acquisita nel corso delle indagini preliminari, ciò anche per la dimostrazione dell'avvenuto rispetto di tutte le procedure acquisitive e delle cautele previste per tale processo informatico (in conformità al nuovo dettato dell'art. 9, co.3, del D.M. n. 344/2011 sopra richiamato). Inoltre, anche il travaso successivo dal supporto contenente la copia forense al portale telematico delle prove digitali dovrà seguire delle procedure che garantiscano la conformità totale del contenuto travasato a quello della copia contenuta nel supporto realizzato dalla p.g. (o dal consulente tecnico) che a sua volta deve essere conforme all'originale dato informatico che dovrebbe andare a costituire la prova. Il deposito telematico della prova digitale, infatti, per come previsto dal comma 2 dell'art. 111-*bis* c.p.p. *assicura la certezza, anche temporale, dell'avvenuta trasmissione e ricezione, nonché l'identità del mittente e del destinatario*; anche il comma 2 del nuovo art. 7-*bis* del D.M. n. 44/2011 sopra riportato fa riferimento alla sola garanzia di protezione degli atti e documenti trasmessi dalla p.g. sul portale attraverso *un meccanismo di crittografia, in modo da assicurare l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività*. Tema diverso, invece è quello della protezione ed assicurazione della conformità del dato informatico inserito nel portale dalla p.g., o da altri soggetti tenuti per legge alla trasmissione, al *contenuto* del dato originale (peraltro già a sua volta copia); anche il contenuto della prova digitale deve essere garantito nella sua conformità all'originale al momento del suo inserimento nel portale. È chiaro che il travaso del contenuto della copia forense nel portale telematico da parte della p.g. (o del consulente tecnico) è un processo non equiparabile a quello della stessa formazione della copia forense; quest'ultimo deve rispettare le cautele finora descritte mentre il primo riguarda un meccanismo di *upload* che non dovrebbe comportare problematiche di

alterazione dei dati scaricati, venendo invece primariamente in rilievo il tema dell'identificabilità del soggetto che procede allo scaricamento. Tuttavia, potrebbe essere opportuno prevedere anche per questo secondo percorso un sistema di verifica dell'identità del contenuto del dato scaricato con quello della fonte.

Le moderne tecnologie di certo potranno facilitare lo svolgimento di questi passaggi dei documenti informatici dal contenitore originario fino al portale telematico; peraltro, l'inserimento di un dato nativo digitale in un portale telematico favorirà senz'altro la sua consultazione e la sua analisi. Basti pensare alla visione di file video o l'ascolto di file audio: non si dovranno più aprire supporti esterni che sono sempre soggetti a danneggiamenti o malfunzionamenti, potendo avere attraverso il portale un accesso diretto al *file* oggetto della prova. In questo modo non si dovrebbero più trasformare le prove digitali in prove analogiche per la loro lettura ed analisi; ciò ovviamente comporta un grande cambiamento culturale e di approccio alle investigazioni abituate tradizionalmente a confrontarsi con la carta che trasforma in analogico i dati nativi digitali. La consultazione diretta digitale di dati nativi informatici ne consente indubbiamente la comprensione e verifica in ogni aspetto e dettaglio, con riguardo ad esempio alla sua origine, alle eventuali modifiche, al momento e luogo di produzione ed al soggetto autore.

La prevista introduzione dell'art. 254-*ter* nel codice di rito, di cui al d.d.l. sopra indicato, non pare porre problematiche di rapporti tra la procedura di sequestro dei dati informatici ivi disciplinata e l'ingresso degli stessi nel portale telematico. Una volta formato il duplicato digitale, con il controllo tecnico delle parti appositamente informate, infatti, non pare possano sorgere problemi sul successivo travaso del contenuto di tale supporto nel medesimo portale da parte dell'operatore individuato. Tuttavia, anche questa fase potrebbe essere adeguatamente disciplinata per ribadire e specificare le modalità necessarie per il rispetto delle garanzie di tutela previste dei dati informatici.

4. Prova digitale ed intelligenza artificiale.

L'argomento dell'informatica applicata al procedimento penale per migliorarne l'efficacia attraverso una più facile acquisizione e consultazione di dati ed una più rapida elaborazione di atti, non può che portare ad interrogarsi sull'eventuale utilizzo dell'intelligenza artificiale in tale ambito.

Quest'ultima, intesa come la capacità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività non rappresenta più un futuro lontano ed eventuale con cui il procedimento penale avrebbe potuto, prima o poi, confrontarsi ma costituisce ormai una realtà ben presente nella vita quotidiana delle persone e dunque, di riflesso, in tutte le situazioni in cui vengono coinvolte[31].

[31] Sul rapporto tra diritto penale ed intelligenza artificiale, in termini generali, si veda *Diritto penale e intelligenza artificiale*, G. BALBI, A. ESPOSITO, SA. MANACORDA (a cura di), Torino, 2023.

Possono quindi immaginarsi diversi ambiti di applicazione dei sistemi di intelligenza artificiale che riguardano le diverse fasi di *formazione*, *acquisizione* ed *analisi* delle prove digitali e, dunque, del procedimento penale. Seguendo questo percorso, in effetti, l'intelligenza artificiale potrebbe di certo innanzitutto costituire *un mezzo di prova* in sé, ad esempio, quando si tratta di *software* che registra dati di comportamento di qualcuno, cioè quando questa forma di elaborazione è inserita in apparecchi o strumenti (anche domestici) utilizzati dall'indagato o dalla persona offesa. I dati registrati, memorizzati ed elaborati dal sistema intelligente in chiave ad esempio di abitudini di vita, di comportamento o altro, possono essere invero scaricati ed utilizzati come documento informatico e prova digitale.

Ancora, gli apparecchi dotati di intelligenza artificiale nel campo della robotica potrebbero formare dei mezzi di prova; le azioni poste in essere dall'apparato sulla base di programmi di intelligenza artificiale possono rivelarsi condotte con valenza probatoria nell'ambito di un procedimento penale. Diverso discorso sarebbe, in questo caso, il problema della riconducibilità delle azioni dello strumento intelligente al soggetto installatore ovvero tenuto al monitoraggio e controllo di tali comportamenti, sotto il profilo del rispetto del dovere di vigilanza ovvero dell'eventuale colpa[32].

Dunque, con riguardo alla rilevanza dell'intelligenza artificiale nell'ambito della formazione di una prova digitale vengono in rilievo soprattutto, per un verso, le ipotesi di registrazioni di dati che un *software* può memorizzare ed elaborare formando a sua volta nuovi dati di secondo livello ovvero sistematici ed affinati e, secondariamente, le ipotesi di azioni (ivi comprese le comunicazioni e le omissioni) poste in essere da un apparato robotico intelligente.

Si aggiunga che i sistemi di intelligenza artificiale possono prestarsi ad essere utilizzati per la commissione di illeciti: le avanzate potenzialità offerte da questa tecnologia sono in grado di amplificare la possibilità di realizzazione di reati, non solo informatici, complicando le modalità di prevenzione, controllo e accertamento. Pertanto, quando le azioni illecite vengono condotte mediante meccanismi intelligenti questi ultimi, ciò che hanno creato per consentire tale realizzazione, vengono a formare prove digitali che andranno acquisite nell'ambito di un procedimento.

Nella seconda fase del percorso immaginato l'intelligenza artificiale senz'altro può costituire uno strumento di miglioramento dei meccanismi di *acquisizione delle prove digitali* allocate altrove[33]. Sistemi di intelligenza artificiale, infatti, con accesso diretto agli apparati informatici ovvero a banche dati e fonti digitali possono essere improntati verso una più rapida ricerca ed esportazione delle informazioni richieste. Ciò può riguardare la ricerca di informazioni semplici come di dati complessi estrapolabili dalla propria

---

[32] Si veda, in proposito, M.E. FLORIO, *Il dibattito sulla responsabilità penale diretta delle ia: "molto rumore per nulla"?* in *questa Rivista*, 8 febbraio 2024. Si veda anche F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in *Diritto penale e intelligenza artificiale, "Nuovi Scenari"*, Torino, 2023, 12 ss.; nello stesso volume A. CAPPELLINI, *Reati colposi e tecnologie dell'intelligenza artificiale*, 19 ss.

[33] Tra gli altri utilizzi dell'intelligenza artificiale come strumento di ricerca della prova deve farsi riferimento, ad esempio, ai software di riconoscimento facciale, sul tema L. ALGERI e M. TORRE, *Aspetti definitori e delimitazione della materia*, in *La decisione penale tra intelligenza emotiva ed intelligenza artificiale*, G.M. BACCARI E P. FELICIONI (a cura di), Milano, 2023, 96 ss.

originaria allocazione digitale solo con passaggi dispendiosi in termini di risorse e tempo.

Evidentemente, questo processo di ricerca ed acquisizione di prove digitali mediante strumenti di intelligenza artificiale deve muoversi all'interno dei binari di cautele e garanzie normativamente fissate, come finora detto, a livello nazionale ed internazionale, anche per il controllo della genuinità dell'acquisizione. Alle capacità operative notevolmente superiori - e sempre progressivamente in crescita – degli apparati dotati di intelligenza artificiale non deve corrispondere un inadeguato sistema di verifica della correttezza dell'utilizzo di tali strumenti, nel rispetto delle garanzie e diritti sanciti anche sul piano costituzionale al contrario, a mezzi più forti ed invasivi di ricerca della prova devono corrispondere griglie giuridiche di salvaguardia efficaci e controllabili. Queste griglie devono riguardare tutti i poteri investigativi che possono essere messi in campo nel corso delle indagini preliminari, ivi compresi quelli della polizia giudiziaria a cui, per esempio, potrebbero essere affidati sistemi di intelligenza relativi alla c.d. polizia predittiva[34]. Il percorso normativo che si sta affrontando, ad esempio, a livello europeo, fino all'adozione di un regolamento *ad hoc* per una "prima" disciplina dell'IA tende proprio a disegnare una rete di principi volti a trattenere le potenzialità lesive e dannose di tali strumenti senza indebolirne le potenzialità[35]. A ben vedere, però, già oggi la disciplina sopra tracciata in sintesi sull'acquisizione delle prove digitali, unitamente alla Carta etica sull'uso dell'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente, adottata il 3 dicembre 2018 dalla Commissione UE per l'efficienza della giustizia (CEPEJ)[36], costituisce una valida piattaforma normativa adattabile anche ai casi di acquisizione probatoria mediante sistemi intelligenti.

Stesso dicasi per il terzo e probabilmente al contempo più preoccupante ed affascinante dei momenti di confronto tra intelligenza artificiale e prova digitale, quello dell'analisi, della *produzione creativa ed interpretativa*. Questo step, invero, riguarda il possibile momento in cui all'intelligenza artificiale viene affidato il compito di analizzare prove digitali già formate altrove e già acquisite altrimenti (o comunque anche acquisite sempre tramite macchine intelligenti). Si tratta di un passaggio estremamente delicato

---

[34] A proposito, F. BASILE, *op. ult. cit.*, 5 ss. e nello stesso volume C. PISTILLI, *L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine: tra prospettive di sviluppo ed esigenze di coordinamento*, 145 ss.

[35] È in via di definitiva adozione da parte del Parlamento europeo e del Consiglio, secondo la procedura legislativa ordinaria, la proposta di regolamento, presentata dalla Commissione europea il 21 aprile 2021, recante un quadro giuridico in materia di intelligenza artificiale (esplicitamente denominato "legge sull'intelligenza artificiale"). Invero, il 9 dicembre 2023 è stato infatti raggiunto un accordo politico provvisorio, con l'obiettivo di approvare in via definitiva la nuova normativa entro la conclusione dell'attuale legislatura europea. L'accordo dovrà ora essere formalmente approvato dal Consiglio (a maggioranza qualificata), e dal Parlamento europeo (a maggioranza dei suoi componenti), al più tardi nella sessione del prossimo aprile. Il 2 febbraio il Comitato dei rappresentanti permanenti degli Stati membri presso l'UE (COREPER), ha approvato all'unanimità il testo dell'accordo del 9 dicembre. Si veda www.consilium.europa.eu. Riferimenti alla normativa eurounitaria *in itinere* anche su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206 e https://www.ceps.eu/wp-content/uploads/2021/04/AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf?

[36] Rinvenibile su https://rm.coe.int

perché se per un verso la capacità di elaborazione analitica dei dati da parte dei sistemi di intelligenza artificiale, anche secondo modalità preimpostate, al fine della produzione di un risultato interpretativo di una o più prove digitali, possono portare a traguardi impensati prima e notevolmente avanzati in termini di sintesi e messa in comune dei medesimi dati, dall'altro lato tale forma innovativa di analisi potrebbe sfuggire ai controlli previsti ovvero, in un momento più estremo, soppiantare l'analisi finora rimessa all'operatore giuridico.

Intanto, vi è da chiedersi come poter qualificare l'elaborato analitico prodotto da un sistema di intelligenza artificiale di elementi probatori acquisiti nel corso del procedimento penale. Il problema, infatti, è se tale elaborato debba inquadrarsi a sua volta nell'ambito di un ulteriore documento informatico ma più avanzato, un dato informatico freddo elaborato da un *software*, oppure come una sorta di relazione tecnica alla stregua di quelle realizzate da un consulente specialista. In quest'ultimo caso, più adattabile al profilo di creatività associato ai meccanismi di intelligenza artificiale, si porrebbe poi, in termini maggiori rispetto alla qualificazione dell'elaborato analitico come mero documento informatico, il problema della falsificazione dell'interpretazione scientifico-informatica. Si porrebbe, in effetti, il problema di un eventuale esame, controesame delle convinzioni espresse dall'apparato intelligente e, quindi, di una sua verifica all'interno dell'agone processuale.

È tutto da esplorare lo spazio di come costruire il vaglio processuale di un elaborato prodotto da un sistema di intelligenza artificiale; non pare potersi mettere in dubbio il profilo della necessaria valutazione alla stregua di una qualunque prova portata in giudizio secondo i dettami dell'art. 192 c.p.p. Viene difficile, però, immaginare oggi quali strumenti e criteri di valutazione possono essere messi in campo dal Giudice in questi casi: confrontare più elaborati formati da sistemi di intelligenza diversi ovvero controdedurre l'elaborato digitalmente prodotto con altri di tipo analogico, ivi compresi documenti e relazioni contenenti analisi svolte da professionisti e specialisti. Di certo, l'eventuale produzione giudiziaria di prodotti tecnologici di tipo intelligente non può costituire la fine del momento processuale, la chiave di lettura conclusiva dell'istruttoria e del dibattito che matura in sede processuale[37].

In altri termini, in questa veste di elaborato analitico, il prodotto dell'intelligenza artificiale costituisce pur sempre una prova digitale, scientifica e come tale la stessa deve essere sottoposta al vaglio di attendibilità sancito per le prove non disciplinate *ex lege* dall'art. 189 c.p.p.; tale prova, quindi, andrà sottoposta al contraddittorio sulle sesse modalità di assunzione oltre che, poi, sul suo contenuto. Il giudice, prima di ammettere tale prova tecnologica, deve sentire le parti ed individuare le corrette modalità di assunzione nel processo, oltre ad aver verificato che la stessa prova sia stata formata in modo corretto, in modo che vengano rispettate tutte le garanzie difensive. Il binario di introduzione nel processo di queste prove, quindi, è già oggi più stretto e rigoroso rispetto alle altre prove la cui ammissione è disciplinata *ex* art 190 c.p.p. Al

[37] Sull'argomento si veda E. NAGNI, *Artificial Intelligence, l'innovativo rapporto di (in)compatibilità fra machina sapiens e processo penale*, in *questa Rivista*, 2 luglio 2021.

contraddittorio anticipato per l'ammissione della prova, dovrà poi seguire il contraddittorio sulla prova, ovvero sul suo contenuto: qui l'evidenza deve essere sottoposta ad esperimenti, falsificazioni, *peer review* di tipo tecnico-scientifico, in linea con le acquisizioni giurisprudenziali prevalenti secondo cui anche in tema di prova scientifica occorre verificare la razionalità e logicità della spiegazione fornita e dell'approccio metodologico *con specifico riguardo all'affidabilità delle informazioni utilizzate ai fini della spiegazione del fatto*[38].

Si può pensare ad un passaggio ancora più estremo (o forse no).

L'estremo confine, non troppo lontano, di questo percorso di inserimento dell'intelligenza artificiale nel processo penale è infatti quello dell'affidamento al sistema intelligente della decisione finale, con affiancamento, o addirittura sostituzione, del momento argomentativo e decisionale riservato al giudice. In effetti, se il sistema di intelligenza artificiale è predisposto per la simulazione del processo cognitivo e decisorio dell'essere umano, al culmine del processo l'insieme dei dati, delle informazioni e cioè del quadro probatorio risultante dall'istruttoria svolta potrebbe essere sottoposto ad una analisi algoritmica, di calcolo matematico in grado di pronunciarsi sulla sintesi conclusiva, sull'esito tecnologicamente derivante da questa analisi. Non un *software* delle parti, cioè, ma un *software* "per il" o "del" giudice (ma non, come si vedrà, "il" Giudice).

Ebbene, questo è il punto più delicato della questione finora trattata perché ragionando su questo tema ci si pone sull'esatto confine tra *modus operandi* tradizionale, fondato sulla decisione giudiziaria innervata dal criterio dell'alta credibilità razionale e logica del paradigma probatorio e sistema di decisione matematico-statistico, dal carattere neutro[39]. Si dica subito che difficilmente la trasformazione potrà essere tanto radicale da poter intravedere nel prossimo futuro l'integrale sostituzione dell'uomo con la macchina per la formazione del *decisum* conclusivo del processo; l'ordinamento costituzionale si fonda infatti sull'essenza razionalistica del giudizio, sull'esigenza della motivazione critica del giudizio in base all'apparato probatorio a disposizione (artt. 101, co.2, Cost. e art. 11, co.6, Cost., unitamente all'art. 65 dell'ordinamento giudiziario ed agli artt. 187, 192, 546, lett. e, e 606, lett. e, c.p.p.), che legittima la giurisdizione gestita dai giudici[40]. Tuttavia, l'impianto ordinamentale tradizionale, disegnato dalla

---

[38] Cfr. Cass., sez. IV, sent. n. 10394 del 07/02/2023, Rv. 284240 secondo cui: "*In tema di prova scientifica del nesso causale nei delitti colposi, il controllo di legittimità non riguarda la maggiore o minore attendibilità scientifica delle acquisizioni esaminate dal giudice di merito e, quindi, se la tesi accolta sia esatta, ma solo se la spiegazione fornita e l'approccio metodologico siano razionali e logici, con specifico riguardo all'affidabilità delle informazioni utilizzate ai fini della spiegazione del fatto*." Si veda, ancora, Cass. sez. V, sent. n. 1801 del 16/11/2021, Rv. 282545, secondo cui: "*In tema di prova scientifica, il giudizio di attendibilità di una teoria deve tener conto degli studi che la sorreggono e delle basi fattuali sui quali sono condotti, dell'ampiezza, della rigorosità e dell'oggettività della ricerca, del grado di sostegno che i fatti accordano alla tesi, della discussione critica che ha accompagnato l'elaborazione dello studio e delle opinioni dissonanti che si siano eventualmente formate, dell'attitudine esplicativa dell'elaborazione teorica, del grado di consenso che la tesi raccoglie nella comunità scientifica, nonché dell'autorità e dell'indipendenza di chi ha effettuato la ricerca*".

[39] Sul *software* ChatGPT si veda D. FRANKLIN, *The Chatbot Revolution; ChatGPT: An In-Depth Exploration*, 2022.

[40] Cfr. G. CANZIO, *Intelligenza artificiale, algoritmi e giustizia*, in *questa Rivista*, 8 gennaio 2021; si vedano anche ID., *Intelligenza artificiale e processo penale*, in *Prova scientifica e processo penale*, cit., 903 ss. e, nello stesso volume,

Costituzione, è basato sulla consapevolezza dei limiti delle capacità computazionali della mente umana, e dunque della suscettibilità all'errore dei ragionamenti razionali[41]; per questo l'ordinamento ha messo al centro dei valori per una decisione il più possibile giusta quello dell'obbligo di motivazione. Ecco che su questo punto, su questo esatto crinale entra in gioco l'argomento dell'intelligenza artificiale: il sistema algoritmico si candida ad essere - anziché un sostituto - un capace ed efficiente strumento di supporto, sostegno all'insopprimibile scelta interpretativa del giudice.

Quando si fa riferimento allora alla giustizia predittiva, ovvero alla possibilità offerta dai sistemi di intelligenza artificiale di prevedere l'esito di un giudizio tramite calcoli algoritmici, deve immaginarsi uno strumento scientifico che funge da ausilio alla decisione del giudicante[42]: come se l'esito dell'istruttoria processuale venisse messo a sistema per produrre una sintesi decisionale scientifica che il Giudice può utilizzare da modello, da spunto ovvero da autentico fondamento della propria convinzione che andrà ad essere poi motivata nel provvedimento conclusivo. Il momento interpretativo del giudice, quindi, può essere sostenuto dalla predizione matematico-statistica, creata dal meccanismo dell'intelligenza artificiale ma è sempre sul momento interpretativo che poi deve fondarsi la decisione finale. Ogni assoluto ed impersonale affidamento al prodotto scientifico come base della scelta giurisdizionale rischia di convalidare meccanismi di pre-giudizio e pre-comprensione che violano i principi costituzionali dell'obbligo di motivazione (ed interpretazione) critica e razionale per ogni provvedimento giurisdizionale[43]; dall'altro lato, però, l'aggancio a valutazioni statistiche elaborate analizzando i dati dell'istruttoria processuale potrebbe senza dubbio favorire un miglioramento del canone ermeneutico della prevedibilità della decisione. Dunque, il sistema di intelligenza artificiale può contribuire in concreto a formulare delle prognosi di decisione che, qualora valorizzate e sfruttate dal giudice, offrono alla diagnosi contenuta nel provvedimento giudiziario un connotato di prevedibilità maggiore perché rafforzato dall'analisi statistico-matematica. Una funzione di guida euristica dell'IA, di preparazione alla strada della decisione, che l'operatore può essere chiamato a convalidare e confermare nella soluzione interpretativa scelta, in modo da integrare, limitandola, la componente emozionale e più prettamente umana della decisione[44]. I limiti computazionali della mente umana (con i conseguenti errori nelle valutazioni)[45] potrebbero in altri termini essere ridimensionati laddove l'analisi del

---

L. LUPARIA, *Intelligenza artificiale e libero convincimento del giudice*, 943 ss. Si veda anche M. LUCIANI, *La decisione giudiziaria robotica*, in *Riv. Associazione italiana dei costituzionalisti*, n. 3, 2018, § 1.

[41] Sull'argomento si veda R. BLAIOTTA, *Giustizia, errore, intelligenza artificiale*, in *questa Rivista*, 23 ottobre 2023.

[42] In tema G. UBERTIS, *Intelligenza artificiale e giustizia predittiva*, in *questa Rivista*, 16 ottobre 2023. Si veda anche L. VIOLA (a cura di), *Giustizia predittiva e interpretazione della legge con modelli matematici*, Milano, 2019.

[43] Cfr. N. IRTI, *Per un dialogo sulla calcolabilità giuridica*, 23, in A. CARLEO, a cura di, *Calcolabilità giuridica*, Bologna, 2017. Sul tema per il diritto penale V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 547 ss.

[44] Sull'argomento si veda E. NAGNI, *op. ult. cit.*, 51.

[45] Sul punto, tra gli altri, G. INSOLERA, *Legge, ragione ed emozione nella giustizia penale*, in *disCrimen*, 14 febbraio 2020.

materiale di prova emergente dal processo venisse anche calcolato scientificamente; l'esito di questo calcolo andrebbe a favorire le scelte interpretative che il giudicante deve maturare sempre nell'ambito della neutralità del ragionamento inferenziale. Questo percorso, infatti, deve pur sempre avvenire nel rispetto dei metavalori dell'ordinamento, con le garanzie in esso previste; esattamente a tal proposito sono state predisposte le prime normative di disciplina dell'intelligenza artificiale (come la Carta etica sopra indicata), in attesa, tra l'altro, del regolamento europeo.

Evidentemente, però, la maggiore efficienza del *decisum* dal punto di vista del supporto motivazionale offerto dal calcolo statistico basato sul materiale probatorio acquisito nel corso del processo non conduce verso la frontiera della giustizia esatta, perché il substrato computazionale è sempre limitato dalla qualità e quantità delle evidenze raccolte nell'istruttoria, che non può mai essere del tutto completo. Allora, il miglioramento della decisione giudiziaria sotto questo profilo può invece portare il formante giurisprudenziale verso una giustizia più giusta e prevedibile[46]; in definitiva, il paradigma probabilistico-razionale della soluzione decisoria si rafforza acquisendo connotati di maggiore calcolabilità (e quindi, in prospettiva, uniformità).

Resta da osservare come potranno avvenire le prossime trasformazioni tecnologiche su questo campo, che di certo saranno progressivamente sempre più rapide e rivoluzionarie[47]; una sfida per l'individuazione delle discipline più adattabili a questa frontiera della digitalizzazione e per la conseguente applicazione, cui tutti gli operatori saranno chiamati a confrontarsi.

---

[46] Sulla prevedibilità della decisione giudiziaria, *ex multis*, di recente, G. COCCO, *L'interpretazione giudiziale deve guardare oltre la soluzione del caso concreto. Alcune vicende esemplari*, in *questa Rivista*, 25 gennaio 2024.

[47] Sulla progressione sempre maggiore di crescita delle capacità dell'intelligenza artificiale si veda R. MANZOTTI E S. ROSSI, *IO&IA, mente, cervello e GPT*, Catanzaro, 2023.