

## SEQUESTRO INFORMATICO E INTELLIGENZA ARTIFICIALE: UN POSSIBILE CONNUBIO?

di Matteo Feltrin

(*Dottorando di ricerca in Diritto processuale penale,  
Università degli Studi di Udine*)

Il presente contributo si incentra sull'analisi della disciplina del sequestro di dispositivi informatici, muovendo dal fermo monito della giurisprudenza di legittimità avverso il ricorso a forme di apprensione indiscriminata e soffermandosi, al contempo, sulle persistenti aporie e lacune che connotano l'attuale disciplina positiva. Lungo una seconda direttrice, il contributo si apre a una riflessione prospettica, interrogandosi sul ruolo che l'intelligenza artificiale potrebbe avere nelle operazioni di selezione del materiale informatico sequestrato.

The present contribution focuses on the analysis of the legal framework governing the seizure of digital evidences, moving from the firm warning issued by case against the use of indiscriminate forms of acquisition and, at the same time, examining the persistent shortcomings and gaps the characterize the current regulation system. Along a second line, the study adopts a forward-looking process of seized digital material.

sequestro, prova digitale, intelligenza artificiale  
seizure, digital evidence, artificial intelligence

Sommario: 1. Le ricadute applicative del sequestro informatico – 2. Un monito della giurisprudenza di legittimità contro il sequestro informatico *omnibus* – 2.1 L'imprescindibilità di una riforma: verso l'art. 254 *ter* Cpp? – 3. L'influenza dell'intelligenza artificiale sul volto del sequestro informatico.

1. Vi è un momento, nella storia del diritto processuale penale, in cui le categorie tradizionali mostrano la loro cedevolezza dinanzi al mutamento della realtà<sup>1</sup>. L'emersione dell'informatica, quale infrastruttura ordinaria delle relazioni sociali, segna un mutamento profondo nell'orizzonte del processo penale. L'elemento di prova si sedimenta in flussi binari, si frammenta in ecosistemi di reti transnazionali e si

---

<sup>1</sup> Volgere lo sguardo al domani del processo penale, «significa soprattutto parlare della progressiva adozione di modelli scientifici nell'indagine sui fatti», in quanto un numero sempre più elevato di eventi può essere dimostrato attraverso l'utilizzo di «strumenti tecnici sofisticati». Sul punto, M. Damaska, *Il diritto delle prove alla deriva*, Bologna 2003, 205.

crystallizza in vestigia digitali<sup>2</sup>. In tale contesto, il sequestro informatico si impone non già come mero adattamento tecnico di un istituto consolidato, bensì come luogo in cui si ridefiniscono i confini stessi dell'apprensione probatoria<sup>3</sup>.

La svolta normativa trova il suo baricentro nella Convenzione di Budapest che ha per la prima volta sistematizzato, in una prospettiva sovranazionale, l'esigenza di dotare gli ordinamenti di strumenti processuali adeguati alla specificità dell'evidenza digitale<sup>4</sup>. L'obiettivo non era solo soltanto quello di reprimere nuove forme di criminalità<sup>5</sup>, ma anche di predisporre un sistema di strumenti processuali idonei a garantire l'acquisizione e la conservazione della prova informatica nel rispetto dei diritti fondamentali. L'ordinamento italiano ha dato attuazione a tali principi con la legge 18 marzo 2008 n. 48, ridefinendo le modalità di perquisizione e sequestro dei dati e introducendo cautele volte a preservarne integrità e genuinità<sup>6</sup>.

Dunque, è nel sequestro informatico che si misura la capacità del processo penale

---

<sup>2</sup> Cfr., S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018, 218 ove si precisa che «di fronte alla mancanza di una corporeità visibile degli elementi di prova digitali, la dottrina processualpenalistica aveva inizialmente avvertito un certo disagio nel configurare elementi probatori o prove disgiunte dal requisito della fisicità. Di qui l'equivoco di fondo, che in passato aveva portato a identificare gli elementi di prova digitali con il supporto nel quale essi si erano memorizzati. [...] Solo in un secondo momento, quindi, è maturata la consapevolezza che i dati, le informazioni, i programmi, possono di per sé integrare i concetti di "corpo del reato o di "cose pertinenti al reato" e che, ai fini del sequestro, è spesso sufficiente disporre dei dati e non anche del *computer* o del sistema informatico che li contiene».

<sup>3</sup> Per una disamina sull'oggetto del sequestro probatorio, si veda S. Montone, *Sequestro penale*, in *DigDPen*, XIII, 1997, 254 ss.

<sup>4</sup> Per un maggior approfondimento sia consentito il rimando a S. Aterno, *La Convenzione di Budapest del 2001 e la l. 48/2008*, in *Cybercrime*, diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Torino 2023, 1551 ss., ove si precisa che «la Convenzione di Budapest del 2001 nacque in sordina. In quegli anni non si poteva ancora apprezzare la bontà di alcune norme utili alla lotta al *cybercrime* ma soprattutto utili ad acquisire in modo integro e genuino le prove digitali di qualsiasi scena del crimine. Quelle norme furono pensate e scritte con grande attenzione e con una previsione di quelle che sarebbero state le possibili sfide del futuro investigativo e tecnologico. L'obiettivo principale enunciato era quello di perseguire una politica penale comune per la protezione della società contro la *cybercriminalità*, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale. In questi anni le istituzioni relative alla cooperazione investigativa, la giurisprudenza di merito e di legittimità hanno fatto propri quei principi e li hanno utilizzati per contemperare da una parte le esigenze di indagine e dall'altra le giuste garanzie difensive». Altresì, F.M. Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *CP* 2012, 703 ss.

<sup>5</sup> Una analisi delle modifiche introdotte nell'ambito del diritto penale sostanziale si scorge in L. Picotti, *Ratifica della convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *DI* 2008, 437.

<sup>6</sup> In tema, L. Lùparia, *Le problematiche transnazionali*, in L. Lùparia – G. Ziccardi, *Investigazione penale e tecnologia informatica*, Milano 2007, 205 ss.

di rimanere fedele alla propria matrice garantista pur confrontandosi con l'inedita morfologia della prova digitale. Le esigenze di effettività dell'accertamento non possono tradursi in un'espansione incontrollata del potere di apprensione, né la peculiare struttura del dato<sup>7</sup> può legittimare compressioni indiscriminate della sfera individuale<sup>8</sup>. Invero, quando l'acquisizione probatoria investe universi informativi che racchiudono segmenti essenziali della vita privata<sup>9</sup>, una logica meramente funzionalistica dell'indagine rischia di sacrificare, sull'altare dell'efficienza investigativa, il nucleo irriducibile delle garanzie poste a tutela dell'individuo<sup>10</sup>.

In questa prospettiva, problematico è stato misurarsi con talune questioni applicative e interpretative, scaturite dalla difficoltà di adattare le tradizionali categorie codicistiche a un fenomeno che presenta indubbi caratteri di novità.

Sotto un primo profilo, si è posto il problema dell'effettività dei rimedi azionabili avverso l'illegittima applicazione della misura, avuto riguardo alla fisiologica riproducibilità del dato informatico<sup>11</sup>, nonché all'iniziale consolidarsi di un orientamento nella giurisprudenza di legittimità<sup>12</sup>, incline a escludere la permanenza dell'interesse a impugnare il decreto di sequestro nei casi di previa estrazione di copia forense seguita dalla restituzione dei supporti originari<sup>13</sup>.

---

<sup>7</sup> L. Marafioti, *Digital evidence e processo penale*, in *CP 2011*, 4509, ove si precisa che i dati informatici «consistono in zero and ones of electricity».

<sup>8</sup> Il bagaglio di informazioni ricavabile dai dispositivi informatici costituisce quella che è stata definita una sorta di «corpo elettronico» – *pendant* del «corpo fisico» – che ciascuno possiede e che lascia tracce ovunque. Un corpo dotato di sconfinata capienza, idoneo ad accogliere una massa sterminata d'informazioni capace di rilevare il contenuto d'interesse esistente e adatta a sedare anche la più bulimica istanza di conoscenza. Così, F. Siracusanò, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *PPG 2017*, 179.

<sup>9</sup> Il contenuto del dispositivo informatico è così ampio da contenere l'«intera nuda vita» della persona «con una portata totalitaria che avrebbe forse sorpreso anche la fantasia di George Orwell». Così, M. Olivetti, *Diritti fondamentali e nuove tecnologie. Una mappa nel dibattito italiano*, in *Revista Estudos Institucionais 2020*, 400.

<sup>10</sup> Per una ricostruzione, in senso critico, della prassi antecedente alla riforma del 2008, si veda A. Monti, *No ai sequestri indiscriminati di computer*, in *DI 2007*, 264 ss.

<sup>11</sup> Sul punto, S. Aterno, *Acquisizione e analisi della prova informatica*, in *DPP 2008*, 62 ss.

<sup>12</sup> Si veda, ad esempio, Cass. 8.4.2019, 15113, in *GI 2019*, 1437.

<sup>13</sup> M. Torre, *Il riesame del sequestro probatorio di documenti informatici*, in *GI 2019*, 1438 ove si precisa che «secondo la Suprema corte, il sequestro probatorio di documenti informatici differirebbe concettualmente dalla propedeutica attività di estrazione di copia dei dati medesimi, attività quest'ultima non «riesaminabile» in ragione del principio di tassatività delle impugnazioni di cui all'art. 568 Cpp e rispetto alla quale, peraltro, non sussisterebbe automaticamente un concreto ed attuale interesse ad impugnare da parte del ricorrente. Tale decisione si espone ad un duplice profilo critico: da un lato, si deve sottolineare l'erronea premessa tecnica, in quanto il sequestro probatorio di documenti informatici («ove possibile») si deve tradurre proprio nell'attività di copia dei dati dal supporto che li contiene, mediante una tecnica che assicuri la conformità della copia rispetto

Sotto un secondo profilo, di maggior interesse ai fini della presente trattazione, la semplicità e la velocità con cui, mediante un sequestro informatico, è possibile acquisire ingenti quantità di dati potenzialmente rilevanti ai fini probatori favoriscono il ricorso a vere e proprie “pesche a strascico” nei sistemi informatici di uso quotidiano<sup>14</sup>. Solo in un momento successivo si procede, infatti, all’analisi dei contenuti e alla verifica dell’effettiva utilità probatoria degli elementi raccolti, con evidenti ricadute sul diritto alla riservatezza del titolare dei dati così acquisiti<sup>15</sup>. Le connotazioni strutturali del sequestro informatico impediscono di «operare una convincente *reductio ad unum* dello strumento in questione con il tradizionale istituto del sequestro probatorio»<sup>16</sup>. Proprio tale irriducibilità consente di comprendere il costante richiamo, operato *ex cathedra* dalla giurisprudenza di legittimità<sup>17</sup>, al principio di proporzionalità quale criterio di governo della misura<sup>18</sup>. Esso si attegga a criterio di conformazione dell’esercizio del potere ablativo volto a scongiurare applicazioni *ultra vires* che, mediante l’apprensione indiscriminata dell’intero contenuto di un sistema informatico, si risolvano in una indebita compressione del diritto fondamentale alla riservatezza del titolare dei dati<sup>19</sup>. Diversamente opinando, il rischio è quello di avallare pratiche investigative connotate da finalità meramente esplorative, in aperta frizione con il canone di stretta pertinenza tra *res* sequestrata e *thema probandum*<sup>20</sup>.

Il principio di proporzionalità si configura, in tal modo, non già come mera formula di stile, bensì quale parametro di conformazione del potere ablativo, chiamato a presidiare l’equilibrio tra effettività dell’accertamento e tutela dei diritti

---

all’originale e la non alterabilità dei dati; dall’altro, si deve stigmatizzare l’omessa considerazione del diritto alla “esclusiva disponibilità del patrimonio informatico” come bene giuridico in grado di rilevare ai fini della sussistenza dell’interesse ad impugnare del ricorrente».

<sup>14</sup> G. Cascone, *Il sequestro informatico nel prisma del principio di proporzionalità*, in *DPP* 2022, 125.

<sup>15</sup> S. Signorato, *Le indagini digitali*, cit., 219.

<sup>16</sup> G. Cascone, *Il sequestro informatico*, cit., 179.

<sup>17</sup> Tra le tante, si veda Cass. 3.10.2022, n. 37349.

<sup>18</sup> Ribadisce il rilievo fondamentale che il principio di proporzionalità assume nel bilanciamento tra l’interesse processuale all’accertamento del reato, sotteso al sequestro probatorio, e le istanze private di tutela di quei beni fondamentali che i mezzi di ricerca della prova sono in grado di comprimere, M. Niccolini, *Proporzionalità e adeguatezza in tema di sequestro probatorio anche informatico*, in *DPP* 2023, 536 ss.

<sup>19</sup> In tema, Cass. 11.1.2022, n. 12507.

<sup>20</sup> Sul rapporto di pertinenza tra cose da sequestrare e il tipo di reato oggetto delle indagini, cfr. G. Tranchina, *Sequestro penale II*, in *EG*, XXVIII, 1991, 2.

fondamentali<sup>21</sup>.

2. Nel contesto fin qui tratteggiato, il sequestro di dati informatici rappresenta il luogo di tensione tra l'effettività dell'accertamento penale e la tutela dei diritti fondamentali. La questione assume un rilievo tutt'altro che marginale, ove si consideri come l'acquisizione della *digital evidence*<sup>22</sup> rappresenti, nella prassi investigativa contemporanea, uno snodo particolarmente sensibile dell'attività di ricerca della prova, giacché proprio in tale fase si concentrano i più rilevanti rischi di alterazione del dato<sup>23</sup> e di indebita compressione delle prerogative individuali<sup>24</sup>.

---

<sup>21</sup> Il principio di proporzionalità «reincanala nell'alveo della ragione», se mai ce ne fosse stato bisogno, «il percorso che l'interprete, nonché, prima ancora, il legislatore, sono tenuti a seguire, quando pretendano di ingerirsi legittimamente nella sfera dell'individuo». In questi termini, M. Caianiello, *Il principio di proporzionalità nel procedimento penale*, in *DPenCont* 2014, 143. Sul ruolo del principio di proporzionalità nell'ambito delle indagini digitali, si vedano le osservazioni di E. De Paolis, *La proporzionalità ha fatto carriera (anche tra le misure ablativo)*, in [www.archiviopenale.it](http://www.archiviopenale.it), 23.9.2024, 15, a mente delle quali si osserva che «il principio di proporzionalità tutela, dunque, in tali ipotesi, non solo e non tanto la libertà economia dell'individuo, ma soprattutto la pretesa alla disponibilità dei dati digitali oggetto di apprensione da parte degli inquirenti. L'acquisizione onnicomprensiva di materiale informatico è, infatti, consentita soltanto se giustificata, nella richiesta del pubblico ministero con il dovuto riferimento ai criteri di selezione, ricadendo su quest'ultimo la responsabilità di illustrare le difficoltà connesse all'identificazione *ex ante* dell'oggetto del sequestro. In tal senso, al fine di scongiurare intrusioni arbitrarie nella *privacy* dell'interessato, la ricerca deve essere svolta segnalando i percorsi utili alla selezione dei dati».

<sup>22</sup> Alcune osservazioni sullo sfondo del mito della *digital evidence* quale prova perfetta si rinvencono in L. Lùparia, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in L. Lùparia – G. Ziccardi, *Investigazione penale e tecnologia informatica*, Milano 2007, 141 ove si sottolinea che «non va dimenticato come la ricerca della prova digitale incida profondamente sui valori ascritti nella nostra Carta fondamentale, specie oggi che il *computer* è divenuto, per ognuno di noi, lo strumento più utilizzato per la gestione dei propri interessi, oltre che un veicolo essenziale per la comunicazione e l'interazione col prossimo. Tali metodologie d'indagine, quindi, esigono un ambito di corretta e ristretta operatività per evitare connotazioni di spropositata afflittività e di offesa a beni costituzionalmente protetti».

<sup>23</sup> Sulle modalità di acquisizione del dato digitale, O. Murro, *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Milano 2024, 66, evidenzia che «individuazione ed acquisizione del dato digitale deve avvenire con le metodologie indicate dalla *computer forensics* o, nella sua più ampia declinazione, dalla *digital forensics*, scienza che consente, tra le altre cose, anche di recuperare i dati cancellati, di identificare l'intestatario di una linea dati o di un sito *web*, di ricercare informazioni anche all'interno di grandi masse di dati».

<sup>24</sup> Su questa linea, S. Rodotà, *Persona, libertà, tecnologia, Note per una discussione*, in *D&QP* 2005, 25, il quale osserva che «il nostro modo di vivere è divenuto un flusso continuo di informazioni, inarrestabile, che noi stessi alimentiamo per avere accesso a beni e servizi. La trasparenza sociale ci avvolge. Le tecnologie dell'informazione non solo si impadroniscono della nostra vita, ma costruiscono un corpo elettronico, l'insieme delle nostre informazioni personali custodite in infinite banche dati, che vive accanto al corpo fisico».

L'applicazione delle categorie tradizionali del sequestro probatorio, si rivelerebbe inadeguata alla luce della natura immateriale del dato digitale; il loro impiego comporta, infatti, il rischio di trasfigurare l'istituto in uno strumento di acquisizione di carattere meramente esplorativo, consentendo l'apprensione indiscriminata dell'intero contenuto dei dispositivi informatici. In questo contesto, la selezione del materiale pertinente con l'impalcatura accusatoria viene differito a un momento successivo all'ablazione, determinando una sostanziale inversione del rapporto perquisizione-sequestro. Ne deriva un sacrificio non necessario dei diritti dell'indagato, tanto più ove si consideri che qui vengono quasi sempre in gioco anche i diritti di soggetti terzi estranei al procedimento penale in corso. Non pare configurabile, dunque, una prevalenza delle esigenze di efficienza investigativa su quelle inerenti «all'ortodossia probatoria»<sup>25</sup>, soprattutto quando posta a presidio delle garanzie individuali.

È noto come la legge n. 48 del 2008 non abbia inteso canonizzare all'interno di norme giuridiche procedure tecniche di matrice informatica, poiché ciò avrebbe portato alla lunga a effetti contrari e distorsivi causati dalla costante evoluzione tecnologica<sup>26</sup>. Detto diversamente, il riformatore ha preferito «focalizzare l'attenzione più sul risultato che sul metodo»<sup>27</sup>.

In questa prospettiva, la riforma in parola non ha dettato specifiche regole operative per l'acquisizione della *digital evidence*<sup>28</sup>, limitandosi a disseminare nel tessuto codicistico taluni canoni, variamente riconducibili ai caratteri di genuinità e immutabilità, che devono tradursi in vincoli operativi concreti nell'attività di

---

<sup>25</sup> F. R. Dinacci, *Sequestro di dispositivi informatici: imposizioni tecnologiche e scelte interpretative. Alla ricerca di un recupero della legalità probatoria*, in [www.archiviopenale.it](http://www.archiviopenale.it), 14.2.2025, 13.

<sup>26</sup> Più ampiamente, A. Testaguzza, *Il sequestro di dati e sistemi*, in *Cybercrime*, diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Torino 2023, 1646.

<sup>27</sup> Così, A. Testaguzza, *op. cit.*, 1646.

<sup>28</sup> Ancora, A. Testaguzza, *op. cit.*, 1648 ove si precisa che «il legislatore del 2008 non ha esplicitato le garanzie che dovrebbero connotare attività particolari come quelle compiute in sede di analisi forense dei dati raccolti; vi ha provveduto la riflessione più attenta della dottrina secondo la quale, agli operatori del settore sarebbero imposte ben cinque prescrizioni, concernenti in particolare: 1. l'obbligo di conservare inalterato il dato informatico originale nella sua genuinità; 2. il dovere di impedire l'alterazione successiva del dato originale, previsto per le ispezioni, le perquisizioni (artt. 244 co. 2 e 247 co. 1 bis Cpp); 3. il dovere di formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale; 4. il dovere di assicurare la non modificabilità della copia del documento informatico; 5. l'obbligo di installazione di sigilli informatici sui documenti acquisiti, prevista come meramente facoltativa in relazione al sequestro (art. 266 Cpp)».

acquisizione della prova digitale<sup>29</sup>.

Muovendo da tali premesse, assume rilievo il ruolo del pubblico ministero quale autorità titolare del potere di disporre il sequestro ai sensi dell'art. 253 Cpp. Tale investitura porta con sé taluni interrogativi sulla necessità di una riflessione della materia. Sul punto intervengono le indicazioni provenienti dalla giurisprudenza della Corte di Giustizia dell'UE. Le affermazioni del Giudice di Lussemburgo hanno evidenziato con particolare chiarezza che l'accesso ai dati esterni delle comunicazioni e a quelli di localizzazione detenuti dai gestori dei servizi di comunicazione deve essere subordinato a un controllo preventivo di un organo amministrativo purché diverso dalle parti<sup>30</sup>. Le implicazioni di tale indirizzo giurisprudenziale appaiono difficilmente eludibili. Se l'accesso ai soli dati esterni delle comunicazioni richiede un vaglio preventivo del giudice, quale entità in grado di assicurare una conciliazione dei diversi interessi e diritti in gioco, appare legittimo interrogarsi sulla compatibilità costituzionale e unionale di un sistema che consenta al pubblico ministero di sottoporre a sequestro strumenti di comunicazione contenenti non solo tali dati, ma anche i contenuti integrali delle comunicazioni stesse<sup>31</sup>.

Solo a questo punto si pone il problema del *quomodo* dell'acquisizione. In questo quadro, si è progressivamente valorizzato il ricorso a tecniche di duplicazione forense del dato digitale, concepite proprio allo scopo di realizzare una copia perfettamente

---

<sup>29</sup> M. Pittiruti, *Dalla Corte di cassazione un vademecum sulle acquisizioni informatiche e un monito contro i sequestri digitali omnibus*, in [www.sistemapenale.it](http://www.sistemapenale.it), 14.1.2021.

<sup>30</sup> Il riferimento va a C.G.U.E., 2.3.2021, *Prokuratuur*, C-746/18. La sentenza ha formato oggetto di vari contributi in dottrina, tra i quali possono richiamarsi: F. Resta, *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna*, in [www.giustiziainsieme.it](http://www.giustiziainsieme.it), 6.3.2021; G. Spangher, *Data retention: le questioni aperte*, in [www.giustiziainsieme.it](http://www.giustiziainsieme.it), 9.10.2021; P. Di Stefano, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale: solo un obbligo per il legislatore o una nuova regola processuale?*, in *CP 2021*, 2556 ss.

<sup>31</sup> Pone l'interrogativo A. Chelo, *Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma*, in *DPP 2022*, 1583. In particolare, «la giurisprudenza della Corte di Giustizia dell'UE, che negli ultimi anni ha iniziato a occuparsi sempre più concretamente delle problematiche incontrate dai giudizi nazionali nel coniugare le esigenze investigative e probatorie con il rispetto dei diritti individuali, induce a una riflessione. Le affermazioni del Giudice di Lussemburgo che, in termini estremamente categorici, ha escluso il potere del pubblico ministero di acquisire, con proprio provvedimento, i dati esterni delle comunicazioni e quelli di localizzazione temporaneamente conservati presso i gestori rappresentano lo spunto per porsi un interrogativo: può dirsi legittimo – e rispettoso della Costituzione e del diritto dell'Unione – continuare ad affidare alla pubblica accusa il potere di sottoporre a sequestro strumenti di comunicazione che contengono, oltre i dati esterni delle comunicazioni, i contenuti delle comunicazioni stesse?».

corrispondente all'originale senza incidere sul supporto sorgente<sup>32</sup>. Attraverso siffatte operazioni si mira a coniugare le esigenze dell'accertamento penale con la necessità di preservare l'integrità del dato e la tracciabilità delle operazioni compiute<sup>33</sup>, così da garantire *ex post* la verificabilità dell'attività di acquisizione e la piena affidabilità della prova nel contraddittorio dibattimentale<sup>34</sup>. Il ricorso a tecniche di duplicazione integrale mediante *bit-stream image* non può tuttavia tradursi in un mero automatismo, dovendo essere sorretta da una motivazione puntuale che espliciti il nesso di pertinenzialità tra la massa informativa acquisita e l'oggetto dell'accertamento<sup>35</sup>.

Sotto questo profilo, la giurisprudenza di legittimità ha enfatizzato la centralità del principio di proporzionalità, quale criterio regolatore della misura in parola<sup>36</sup>. Il canone di proporzionalità non si risolve in una mera formula di stile, bensì opera come

---

<sup>32</sup> L. Algeri, *Principio di proporzionalità e sequestro probatorio di sistemi informatici*, in *DPP* 2020, 851, il quale evidenzia che «la procedura più adeguata a garantire l'integrità dei dati consiste nella creazione di una copia-clone dell'*hard disk* conforme all'originale, che viene resa non modificabile mediante appositi strumenti. In concreto, salvo i casi in cui risulti necessario eseguire l'analisi immediata (*live data forensic*) in sede di sopralluogo, il sequestro del dispositivo informatico può precedere l'attività inquirente, che si svolgerà successivamente in laboratorio e sarà diretta ad effettuare l'acquisizione dei dati digitali e a formare la c.d. copia-forense. Una volta creata, la c.d. *bit-stream image* non consiste in una copia, ma in un clone dell'originale. Ne consegue che rileva come cosa pertinente al reato e costituisce, pertanto, l'oggetto del sequestro. In particolare, il dato informatico, in quanto elemento dematerializzato e indipendente dal supporto, può essere sottoposto a sequestro a prescindere dal supporto stesso dove è incorporato».

<sup>33</sup> O. Murro, *Lo smartphone come fonte di prova*, cit., 97 precisa che «in tale contesto appare, dunque, opportuno parlare di "tracciamento" delle operazioni tecniche compiute sullo *smartphone* al fine di consentire una corretta verifica, *ex post*, dell'integrità e genuinità del dato digitale».

<sup>34</sup> Sulla mancata adozione delle *best practices* e divieti probatori, si vedano le osservazioni di F. Cajani, *Il vaglio dibattimentale della digital evidence*, in *AP* 2023, 837 ss.

<sup>35</sup> C. Fontani, *Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi*, in *DPP* 2022, 240. Di qui, «posto che il computer deve essere visto come una "sfera di esplicazione della libertà della persona di cui esso ne è la proiezione spaziale, il provvedimento di sequestro informatico dovrà connotarsi per la presenza di una motivazione più dettagliata e puntuale, rispetto ad un sequestro tradizionale, in punto di modalità di selezione dei dati. Non si può ritenere più accettabile l'adozione di provvedimenti finalizzati genericamente all'esplorazione di tutti i dati digitali contenuti all'interno dell'*hard disk*, attraverso l'apertura (e quindi la lettura) di tutti i *files*, con riserva di selezionare soltanto successivamente quelli "utili" alle indagini».

<sup>36</sup> I riferimenti al principio di proporzionalità sono molteplici. A titolo di esempio possono richiamarsi, Cass. 11.1.2022, n. 12507, in *De Jure*, con nota di A. Schillaci, *Limiti del sequestro probatorio esteso a tutti i dati contenuti negli apparecchi telefonici o in altri sistemi informatici*, in *www.iuspenale.it*, 22.6.2022; Cass. 23.9.2020, n. 37941, in *De Jure*, con nota di C. Parodi, *Perquisizioni e sequestri informatici e sequestri esplorativi: la s.c. delinea gli ambiti operativi*, in *www.ius penale.it*, 10.3.2021; Cass. 2.7.2019, n. 31593, in *DI* 2019, 775 ss.

parametro di delimitazione del potere ablativo, in tal modo impedendo che il sequestro si presti a meccaniche esplorative. La principale criticità dell'attuale assetto codicistico, su cui si tornerà meglio *infra*, risiede nell'assenza di una puntuale disciplina volta a fornire una regolamentazione normativa circa le modalità di conduzione del sequestro informatico. E in questo quadro, si valorizza l'onere motivazionale in ordine alla strumentalità della *res* informatica rispetto all'accertamento penale<sup>37</sup>.

In questa direzione, la giurisprudenza di legittimità ha individuato tre profili - «quantitativo, qualitativo e temporale»<sup>38</sup> - che devono essere oggetto di specifica motivazione da parte del pubblico ministero, pena l'illegittimità del decreto di sequestro. In particolare, affinché il sequestro sia legittimo, occorre che il provvedimento sia specificamente motivato *a)* in ordine al nesso di pertinenza tra bene appreso e ipotesi investigativa, *b)* in relazione alla tipologia di operazioni tecniche da svolgere sul dato e *c)* con riguardo alla durata temporale del vincolo<sup>39</sup>.

Anche volgendo lo sguardo alla giurisprudenza europea, il panorama non muta in modo significativo: l'ago della bilancia tra le esigenze dell'attività investigativa e la tutela dei diritti fondamentali è individuato nell'ammissione di ingerenze solo nei casi previsti dalla legge, purché sia rispettato il principio di proporzionalità<sup>40</sup>.

In definitiva, proprio nella motivazione del provvedimento di sequestro si condensa la principale garanzia contro il rischio di indebite dilatazioni del potere investigativo. È proprio in tale spazio argomentativo che l'autorità procedente è chiamata a rendere conto delle ragioni che giustificano l'ablazione della *res*, rendendo così effettivo il controllo di legalità sulla misura e preservando il necessario equilibrio tra esigenze di accertamento e tutela dei diritti fondamentali.

2.1. Quanto finora detto proietta un vivido fascio di luce su un'evidente aporia: in una congiuntura storica in cui l'ontologia della *res* risulta radicalmente mutata, il dato normativo persiste in un silenzio eloquente.<sup>41</sup> Ponendo uno sguardo attento agli

---

<sup>37</sup> F. R. Dinacci, *op. cit.*, 8.

<sup>38</sup> Cass., 22.9.2020, n. 34265 cit.

<sup>39</sup> In questi termini, M. Pittiruti, *op. cit.* Si vedano altresì le osservazioni di S. Signorato, *Electronic investigation in Italian criminal proceedings*, in *Analele Universității de Vest din Timișoara - Seria Drept* 2014, *passim*.

<sup>40</sup> Si veda, *ex multis*, C. eur., 16.2.2000, *Amann c. Svizzera*. Altresì cfr., F.M. Molinari, *op. cit.*, 19 ss.

<sup>41</sup> O. Murro, *Sequestro dei dispositivi informatici: verso l'art. 254 ter c.p.p.? Brevi note a margine del d.d.l. a.s. n. 806*, in *www.penaledp.it*, 12.3.2024, 1. L'Autrice sottolinea che «la disinvolta disciplina codicistica con la quale -

odierni dispositivi informatici – quali strumenti ormai inseparabili dall’esperienza quotidiana degli individui – non possono essere più considerati meri supporti materiali o semplici contenitori di informazioni. Essi costituiscono, piuttosto, autentici scrigni della persona, capaci di ricostruire la trama stessa dell’esistenza individuale<sup>42</sup>. Si è così sostenuto che, anche nel luogo virtuale, assumono rilievo sia l’art. 13 Cost., nonché gli artt. 14 e 15 Cost.<sup>43</sup>.

Come è noto, il Giudice delle Leggi ha statuito che la messaggistica e la posta elettronica archiviate su un supporto digitale rifuggono dalla qualificazione di mero materiale documentale, preservando l’ontologica natura di corrispondenza<sup>44</sup>. Trattasi di affermazioni gravide di conseguenze sul piano ermeneutico. Il sequestro di un dispositivo informatico, che per l’uso per il quale è stato concepito, è vettore ma anche deposito di corrispondenza<sup>45</sup>.

Ebbene, l’approdo ermeneutico che riconduce le comunicazioni digitali nell’alveo protettivo dell’art. 15 Cost., riverbera effetti dirimpenti sullo statuto delle garanzie procedurali. La citata disposizione, nell’istituire la nota duplice riserva di legge e di giurisdizione<sup>46</sup>, non si limita a postulare il vaglio dell’autorità giudiziaria – requisito sino ad ora assolto dal decreto di sequestro del pubblico ministero –, ma esige che ogni compressione della libertà di corrispondenza avvenga con le garanzie stabilite dalla legge<sup>47</sup>.

Ne discende che l’attuale assetto normativo palesi una significativa lacuna: se la limitazione della libertà e segretezza della corrispondenza può avvenire solo nei limiti

---

sinora – si sono legittimate le operazioni investigative nei dispositivi informatici (*smartphone, computer, tablet, etc.*) è apparsa non solo inadeguata, ma anche inidonea a limitare le attività di indagine che impattano sui diritti fondamentali, nonché su quelli di c.d. di seconda e terza generazione».

<sup>42</sup> O. Murro, *Sequestro dei dispositivi informatici*, cit. 1. Si precisa che «tali dispositivi dischiudono al loro interno un vero e proprio mondo virtuale, idoneo a descrivere l’intera esistenza digitale delle persone. Più precisamente, in riferimento allo *smartphone*, non è apparso peregrino sostenere che esso mediato dalla connessione alla Rete, diventi una vera e propria proiezione informatica dell’individuo che abbraccia l’intera esistenza dell’uomo. Questi, infatti, attraverso il dispositivo elettronico svolge la sua vita digitale (lavora, effettua ricerche, comunica, socializza, etc.), esercitando così i suoi diritti fondamentali». Esamina l’impatto degli strumenti di indagine sui diritti individuali, R. Orlandi, *Una giustizia penale a misura di nemici?*, in *RIDPP* 2020, 735 s.

<sup>43</sup> Si veda, più ampiamente, G. Ubertis, *Sistema di procedura penale*, I, *Principi generali*, Milano 2023, 203 ss.; A. Camon, *La disciplina costituzionale*, in *AA.VV., Fondamenti di procedura penale*, Milano 2023, 99 ss.

<sup>44</sup> Il riferimento naturalmente va a C. cost., 27.7.2023, n. 170.

<sup>45</sup> A. Chelo, *op. cit.*, 2.

<sup>46</sup> Più ampiamente L. Filippi, *Il cellulare “contenitore” di corrispondenza anche se già letta dal destinatario*, in *www.penaledp.it*, 6.9.2023, 2.

<sup>47</sup> A. Chelo, *Tanto tuonò che piove: il nuovo sequestro di dispositivi informatici*, in *www.penaledp.it*, 29.2.2024, 3.

indicati dalla legge quanto ai casi, modi e garanzie, non appare più sostenibile l'assenza di una norma *ad hoc* che regoli le forme dell'ingerenza statale sui messaggi archiviati. Tale vuoto non può essere colmato mediante il ricorso al paradigma del sequestro probatorio "ordinario" ex art. 253 Cpp. Sebbene sia ormai acquisito che il baricentro dell'atto d'imperio si sia spostato dal "contenitore" al "contenuto", la formula generale del sequestro di cose pertinenti al reato si rivela strutturalmente inidonea a soddisfare le esigenze richieste dall'art. 15 Cost.<sup>48</sup>.

Per colmare siffatte lacune, i d.d.l. 690<sup>49</sup> e 860<sup>50</sup> mirano a introdurre nell'alveo del

---

<sup>48</sup> A. Chelo, *op. cit.*, 3.

<sup>49</sup> Si tratta del disegno di legge d'iniziativa dei Senatori P. Zanettin e G. Bongiorno comunicato alla presidenza il 19 luglio 2024, recante "modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali". In tal senso, K. La Regina, *Il sequestro dei dispositivi di archiviazione digitale*, in *www.penaledp.it*, 12.10.2023, 5, sottolinea che «diversa, anche dal punto di vista dei valori sottostanti, è la prospettiva che viene riversata nella seconda proposta di legge, la n. 690, presentata dal Senatore R. Scarpinato, la quale – e nonostante conduca la copia forense nell'archivio riservato delle intercettazioni – appare, invece, molto più attenta alle esigenze dell'accertamento piuttosto che ai diritti individuali. Qui lo schema è presentato come una sorte di ibrido tra il procedimento di sequestro, le disposizioni relative all'acquisizione dei dati del traffico telefonico e le intercettazioni. In sintesi: al p.m. serve l'autorizzazione del giudice per procedere al sequestro ma nei casi di urgenza può provvedere di propria iniziativa, salvo successiva convalida; sia nel caso di azione autorizzata che nell'ipotesi di atto compiuto d'iniziativa non è prevista la sottoposizione al giudice del fascicolo o comunque di materiale ulteriore rispetto al provvedimento del p.m. Come nel d.l. n. 806, anche in questa proposta manca l'indicazione di un catalogo di reati anche se, a differenza della prima, nella n. 690 si è seguita la strada delle intercettazioni e si istituisce un doppio regime: servono gravi indizi di reato per la generalità dei reati e sufficienti indizi per quelli attinenti alla criminalità organizzata. Nel progetto dell'On. Scarpinato, inoltre, non c'è contraddittorio con gli interessati: qui è il pubblico ministero che, in solitaria, stabilisce l'area di ciò che è rilevante e di ciò che non lo è. Lo dimostra anche il fatto che, a conclusione delle operazioni e comunque non oltre settantadue ore (termine peraltro non presidiato da sanzione), si restituisce solo il dispositivo e non la copia forense, la quale però viene indirizzata nell'archivio riservato. Gli interessati appaiono sulla scena solo una volta concluse le operazioni di selezione dei dati rilevanti, perché possono richiedere – non è chiarito in che modo in che tempi e con quali possibili sviluppi procedurali nel caso di disaccordo con il p.m. – la distruzione di quanto non rilevante per le indagini».

<sup>50</sup> Si fa riferimento al disegno di legge d'iniziativa del Senatore R. Scarpinato, comunicato alla presidenza il 9 maggio 2023, relativo "all'introduzione dell'art. 254 *ter* Cpp recante norme in materia di sequestro di strumenti informatici". Di qui, K. La Regina, *op. cit.*, 3, precisa che «si prevedono, particolare, i profili che devono essere oggetto di specifica motivazione da parte del p.m., sia sotto il profilo del nesso di pertinenza tra il bene appreso e l'oggetto delle indagini, sia in relazione alla tipologia di operazioni tecniche da svolgere per eseguire la selezione dei dati; si prevede, inoltre, che questa selezione sia circoscritta ai soli dati effettivamente necessari per il prosieguo delle indagini. In questo contesto, l'analisi e l'esame dei dati viene impedita fino all'espletamento delle operazioni di selezione; queste ultime, infatti, devono essere svolte in contraddittorio con gli interessati e i difensori. Lo schema prescelto è quello degli accertamenti tecnici irripetibili, con la conseguenza anche di risolvere l'annosa questione circa la doverosità per l'acquisizione della *digital evidence*, della attivazione del

nostro codice di rito l'art. 254 *ter* Cpp: la norma dovrebbe riprendere la disciplina delle intercettazioni, ponendosi l'obiettivo di giungere a un punto di equilibrio tra la tutela della *privacy* e la salvaguardia delle esigenze investigative<sup>51</sup>.

Vero che l'art. 253 Cpp è anodino e che l'art. 254 *bis* Cpp non riguarda specificamente il tema del sequestro di dispositivi informatici, ma è altrettanto vero che la recente attenzione del legislatore ha trovato innesco in quella giurisprudenza di legittimità<sup>52</sup> che ha fissato dei limiti ai c.d. "sequestri a strascico" stabilendo le condizioni necessarie affinché un vincolo esteso possa dirsi proporzionato e quindi legittimo – condizioni essenzialmente collocate sul piano dell'onere motivazionale incombente sul pubblico ministero.

Nel solco così tracciato, si deve negare albergo a un preventivo e indefinito monitoraggio del *device* in attesa di una futuribile captazione dei dati d'interesse; non meno illegittimo appare il sequestro di dati che non rechino l'impronta di una stretta pertinenza con l'ipotesi accusatoria<sup>53</sup>. Ne discende che il provvedimento di sequestro informatico dovrà avere una motivazione articolata e dettagliata in ordine alla modalità di selezione dei dati, al fine di evitare che il sequestro si trasformi in una sorta

---

congegno di cui all'art. 360 Cpp. Questo meccanismo, pertanto, diviene funzionale alla selezione dei dati rilevanti e correlativamente alla duplicazione dei soli dati selezionati. Nonostante, nelle sue linee complessive, si tratti di una proposta da cui certamente non resta estraneo il tema del necessario equilibrio tra le esigenze difensive e quelle di accertamento, restano diverse zone d'ombra. In primo luogo, si assiste ad una marginalizzazione del ruolo del g.i.p., la quale si scorge, peraltro, dallo sbarramento alla possibilità di sollevare riserva di pro di promuovere incidente probatorio perché, nel richiamare la disciplina di cui all'art. 360 Cpp, si fa espressa esclusione del comma 4. Che al g.i.p. venga ritagliato un ruolo di secondo piano, del resto, emerge anche dalla scelta di affidare al p.p.m. la decisione sulle questioni concernenti il rispetto dei principi di necessità e proporzione nella selezione dei dati: in questo contesto, infatti, è il *dominus* che decide entro quarantotto ore e il g.i.p. deve esprimersi sulla convalida del provvedimento entro le successive quarantotto ore. Tuttavia, non c'è traccia di messa a disposizione del giudice di elementi di valutazione diversi dal provvedimento decisorio del p.m.; di conseguenza, l'impressione è che, nella traduzione operativa, possa agevolmente prendere vita quello stesso simulacro di controllo che caratterizza la verifica di una intercettazione urgente, rispetto alla quale è ben noto che la convalida non rappresenti affatto il controllo di legittimità di un atto compiuto in sostituzione ma, piuttosto, la sanatoria di un illegittimo. In questa proposta, infine, non si fa riferimento all'archivio e ciò in quanto, una volta eseguita la copia dei dati di interesse, il dispositivo e l'eventuale copia integrale – che può essere disposta, ai sensi del comma 2 del progetto di norma, prima e senza contraddittorio, quanto vi è un pericolo che il contenuto dei dispositivi possa essere cancellato, alterato o modificato – sono immediatamente restituiti all'avente diritto».

<sup>51</sup> A. Chelo, *op. cit.*, 1.

<sup>52</sup> *Ex plurimis* Cass. 29.1.2025, n. 17677; Cass. 13.10.2025, n. 33657; Cass. 4.3.2025, n. 9797; Cass. 3.1.2024, n. 222; Cass. 20.11.2024, n. 1286; Cass. 3.2.2022, n. 17878; Cass. 19.3. 2021, n. 10815.

<sup>53</sup> A. Testaguzza, *op. cit.*, 1662.

di pesca a strascico nel *mare magnum* dei dati personali.

Invero, lo schema concettuale del sequestro probatorio appare costruito su un paradigma di apparente linearità: individuata una cosa utile all'indagine, essa viene appresa e assicurata al processo<sup>54</sup>. Chi ha patito l'atto potrà poi invocare il controllo giudiziale, così da impedire compressioni indebite del diritto di proprietà<sup>55</sup>. Questo schema si è però incrinato aprendo scenari inaspettati. L'antecedente cornice dogmatica, incardinata sulla rigida dicotomia tra l'apprensione del supporto fisico ex art. 253 Cpp e la successiva estrazione di copia ex art. 258 Cpp, determinava una significativa aporia nel sistema delle tutele endoprocedimentali. In virtù del principio di tassatività dei mezzi di gravame, l'ordine di estrazione di copia, quale atto ulteriore e distinto rispetto al decreto di sequestro<sup>56</sup>, risultava insuscettibile di autonoma impugnazione<sup>57</sup>, relegando il sindacato difensivo al solo vaglio di utilizzabilità in fase dibattimentale.

L'approdo ermeneutico segnato dalla Convenzione di Budapest ha determinato un profondo mutamento del panorama appena disegnato<sup>58</sup>. Sotto questo profilo,

---

<sup>54</sup> L. Bartoli, *Sequestro di dati ai fini probatori: soluzioni provvisorie a incomprendimenti durature*, in [www.archiviopenale.it](http://www.archiviopenale.it), 5.3.2018, 1. Si precisa che «per com'è descritto dal libro terzo del codice il sequestro sembra una faccenda semplice: cercata e trovata una cosa utile all'indagine, la si prende e la si porta via, così da assicurarla al processo». Risuonano quanto mai attuali gli insegnamenti di F. Carnelutti, *Principi del processo penale*, Napoli 1960, 174, il quale evidenzia che «andare alla ricerca della prova somiglia assai spesso, per quanto il paragone possa sembrare bizzarro, ad andare a caccia di farfalle: quando si sono afferrate, bisogna conservarle, ed è un'operazione difficile per il pericolo di guastare a loro le ali».

<sup>55</sup> A. Camon, *Le prove*, in AA.VV., *Fondamenti di procedura penale*, Milano 2023, 418. Difatti, «il sequestro è menzionato nella Carta fondamentale nell'art. 14, sulla libertà di domicilio; ma può incidere anche su altri interessi costituzionalmente rilevanti, quali il diritto di proprietà e la libertà di iniziativa economica». Altresi, G. Cascone, *op. cit.*, 124.

<sup>56</sup> «La conclusione trova fondamento nell'idea per cui l'attività di estrazione della copia e l'istituto del sequestro sarebbero tra loro perfettamente autonomi, non costituendo il secondo presupposto indefettibile della prima. Perciò, posto che l'art. 568 Cpp sancisce il principio della tassatività delle impugnazioni, il riesame – ossia il mezzo espressamente previsto per il provvedimento di sequestro, non può costituire lo strumento per sindacare la legittimità dell'estrazione della copia». Così, M. Niccolini, *op. cit.*, 542, nota 51.

<sup>57</sup> Cass. 24.4.2008, n. 18253 con osservazioni di E. Aprile, *Carenza di interesse al riesame del sequestro probatorio di bene già restituito previa estrazione di copia*, in CP 2008, 4031 ss.

<sup>58</sup> La rivoluzione copernicana in materia è rappresentata, come si è detto, dalla Convenzione di Budapest, di poco successiva al *dictum* delle Sezioni Unite Tchmil. In particolare, G. Todaro, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*, in *DPenCont* 2017, 164, chiarisce che con il punto 197 del rapporto esplicativo alla Convenzione di Budapest, adottato dal Comitato dei Ministri del Consiglio d'Europa, è stato evidenziato che “sequestrare” significa “prendere il supporto fisico sul quale i dati o le informazioni sono registrati oppure fare e trattenere una copia di tali dati o informazioni”.

l'estrazione di copia dei dati sequestrati ha smesso di configurarsi quale attività istruttoria dotata di autonoma alterità rispetto al sequestro, assurgendo piuttosto a modalità esecutiva del vincolo ablatorio di cui all'art. 253 Cpp. Le ricadute sistematiche di tale approdo assumono una portata dirompente: la restituzione del dispositivo digitale, lungi dal determinare la caducazione della misura, non ne segna la perdita di efficacia<sup>59</sup>. In altri termini, lo svincolo del contenitore, non estingue la coazione sul contenuto, che permane cristallizzato nella copia forense<sup>60</sup>. Ne discende che l'interesse di gravame, sì da poter ottenere la restituzione dei dati estratti in copia, sopravvive pure allo svincolo dell'apparecchio elettronico.

In trepida attesa che il legislatore, «folgorato sulla via di Damasco»<sup>61</sup>, sia illuminato da una rinnovata coscienza e colga appieno la portata cruciale della materia, l'esigenza di una riflessione della disciplina è imposta anche dalla trasformazione che permea l'odierno ecosistema comunicativo. L'universo telematico «rappresenta sempre di più un'agorà globale, dove soggetti lontani possono tessere rapporti attraverso piattaforme comunicative che proliferano costantemente»<sup>62</sup>.

In questo spazio, si pone lo *smartphone*, il quale ha progressivamente abbandonato la sua caratteristica di mero strumento comunicativo per assurgere a dispositivo con il quale la persona svolge le più disparate attività<sup>63</sup>. Risulta pertanto evidente la ragione che elegge lo *smartphone* a principale bersaglio dell'attività investigativa: il patrimonio informativo racchiuso nell'alveo del *device* offre «un raffinato spaccato della vita

---

<sup>59</sup> G. Todaro, *op. cit.*, 165.

<sup>60</sup> Cass. 14.2.2019, n. 41974. In particolare, la Suprema corte ha precisato che laddove venga trattenuta una copia integrale dei dati presenti su un dispositivo sequestrato, nonostante quest'ultimo venga restituito al proprietario, ciò comunque determina la sottrazione all'interessato dell'esclusiva disponibilità delle informazioni: pertanto, anche in tal caso permane il sequestro probatorio, avente ad oggetto la copia informatica o la riproduzione su supporto cartaceo dei dati contenuti nell'archivio del dispositivo. In altri termini, la restituzione, previo trattenimento di copia del supporto fisico, non comporta il venire meno del sequestro, in quanto permane, sul piano del diritto sostanziale, una perdita per il titolare del dato.

<sup>61</sup> A. Chelo, *op. cit.*, 1588.

<sup>62</sup> O. Murro, *Lo smartphone come fonte di prova*, cit., 17.

<sup>63</sup> «Lo smartphone non è più solo un mezzo di comunicazione, ma è diventato "lo" strumento per eccellenza con il quale la persona lavora, si relaziona, effettua ricerche e, più ampiamente, produce dati: chat, e-mail, archivi multimediali, agende elettroniche, documenti, geolocalizzazione, cronologia internet. Tutte informazioni che, racchiuse nel dispositivo elettronico, permettono di mappare le abitudini di vita dell'individuo, sino a delineare le caratteristiche descrittive della persona». In questi termini, O. Murro, *Prospettive in tema di sequestro dello smartphone: le novità approvate dal Senato*, in *DPP* 2024, 1619.

quotidiana dell'individuo»<sup>64</sup>.

Posto che il sequestro del dispositivo trascini con sé il compendio delle comunicazioni ivi custodite, non vi è ragione alcuna per cui tale atto resti privo di presidi procedurali commisurati alla sacralità dei diritti coinvolti. In tale ottica, il ricorso al sequestro del vettore telematico deve essere sorretto da un onere motivazionale di peculiare rigore, al fine di comprovare, nel rispetto del principio di proporzionalità, che la misura è indispensabile per la prosecuzione delle indagini.

In definitiva, appare, dunque, necessario l'innesto di un segmento di controllo affidato al giudice per le indagini preliminari, potenziandone l'effettività e l'orizzonte conoscitivo, cercando così di compiere quel passo necessario al fine di superare il perimetro della suggestiva immagine consegnataci da Massimo Nobili: in questo quadro, occorrerebbe un organo giurisdizionale investito di poteri ben più incisivi rispetto a quelli in dote al giudice delle indagini preliminari; un giudice, per l'appunto, "senza occhi e senza braccia"<sup>65</sup>. Ancora, considerata la natura dei dati coinvolti, si impone il ricorso allo strumento degli accertamenti tecnici irripetibili, a garanzia di una selezione pertinente e di un immediato contraddittorio. Infine, la previsione di termini perentori per lo svolgimento delle operazioni di selezione dei dati e restituzione del *device*, prescritti a pena di inammissibilità, costituisce l'unico argine contro possibili derive autoritarie<sup>66</sup>.

3. Giunti a questo punto, l'ormai pervasiva influenza dell'informatica nell'ambito del procedimento penale<sup>67</sup> per migliorarne l'efficacia attraverso una più facile acquisizione

---

<sup>64</sup> O. Murro, *Lo smartphone come fonte di prova*, cit., 19.

<sup>65</sup> M. Nobili, *La nuova procedura penale. Lezione agli studenti*, Bologna 1989. Si veda ad esempio 139 s.; 142 s.; 357 s.; 369 s.

<sup>66</sup> Nell'ottica di una compiuta ricognizione dei possibili interventi del legislatore nella materia *de qua*, sia consentito ancora il rimando a O. Murro, *Lo smartphone come fonte di prova*, cit., 293 ss.

<sup>67</sup> L. Romanò, *Intelligenza artificiale come prova scientifica del processo penale: una sfida tra machine generated evidence e equo processo*, in *Prova scientifica e processo penale*, a cura di G. Canzio e L. Lùparia, Milano 2022, 914. «Nell'era dei *Big Data*, gli algoritmi e l'intelligenza artificiale [...] hanno ormai pervaso molto ambienti del vivere sociale e sono già utilizzati nei processi decisionali: sofisticati *software* e modelli di "apprendimento automatico" (*machine learning*) sono in grado di elaborare un'enorme quantità di informazioni, interpretarle, stabilire correlazioni e utilizzare gli *output* per formulare previsioni e per prendere decisioni. I mutamenti antropologici prodotti dall'era digitale non hanno certo lasciato indifferente il mondo del diritto, che, facendosi recettore delle nuove istanze di riconoscimento e tutela legate al progresso tecnico scientifico, è già da tempo chiamato a confrontarsi con le sfide della "società algoritmica". Sul rapporto problematico tra intelligenza artificiale e processo penale, si veda G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in

e consultazione dei dati, non può che portare a interrogarsi, con rinnovata consapevolezza delle trasformazioni in atto, sull'eventuale utilizzo dell'intelligenza artificiale nella selezione del materiale informatico sequestrato. L'alba di una nuova era, dai contorni ancora nebulosi, che suscita reazioni diametralmente opposte: da un lato, un atteggiamento protettivo e un timore reverenziale; dall'altro, viene osannata come un «Eden ritrovato»<sup>68</sup>.

L'impiego di algoritmi, in grado di operare su grandi moli di dati, potrebbe, almeno in linea teorica, consentire di superare quelle prassi investigative caratterizzate da una indistinta apprensione dell'intero contenuto dei dispositivi informatici, orientando invece l'attività di ricerca verso una selezione più mirata e coerente con le esigenze probatorie del caso concreto<sup>69</sup>. Detto altrimenti, l'intelligenza artificiale potrebbe assurgere a filtro preliminare nell'individuazione delle informazioni pertinenti all'indagine in corso.

Tuttavia, tale prospettiva, lungi dal risolversi in una soluzione priva di criticità, impone una riflessione ben di più ampio respiro. L'affidamento, sia pure parziale, a sistemi algoritmici del compito di selezionare il materiale sequestrato rilevante, solleva questioni di non poco momento, che investono tanto il piano delle garanzie processuali quanto quello della trasparenza e della controllabilità delle operazioni compiute<sup>70</sup>. Il rischio, invero, è che il criterio selettivo venga traslato da una valutazione umana a un processo decisionale opaco, il cui funzionamento risulti difficilmente decifrabile secondo il paradigma della c.d. *black box*<sup>71</sup>.

---

[www.archiviopenale.it](http://www.archiviopenale.it), 12.11.2019, 5 ss.

<sup>68</sup> S. Lorusso, *La sfida dell'intelligenza artificiale al processo penale nell'era digitale*, in [www.sistemapenale.it](http://www.sistemapenale.it), 28.3.2024, 1.

<sup>69</sup> Si vedano le osservazioni di P. Dal Checco, *IA a supporto di perquisizione, sequestro e la conseguente analisi forense*, in *Intelligenza artificiale e indagini penali*, a cura di C. Parodi e T. Rizzo, Piacenza 2025, 189. In particolare, «chi si occupa di investigazioni digitali sa bene che ogni operazione – dalla perquisizione al sequestro, fino all'analisi dei dati – genera una mole enorme di informazioni. Dischi rigidi, smartphone, servizi cloud, messaggistica istantanea, e-mail, backup: tutto può contenere prove rilevanti, ma il problema è trovarle spesso in mezzo a milioni di dati e farlo nel rispetto delle regole. Qui l'intelligenza artificiale può offrire un aiuto reale: non si tratta di sostituire l'uomo, ma di affiancarlo, gestire le parti di lavoro ripetitive, quelle che richiedono conoscenze enciclopediche, incrocio dei dati, ragionamenti comparativi e logici su moli di dati difficilmente gestibili da un singolo essere umano».

<sup>70</sup> Pone taluni interrogativi, P. Dal Checco, *op. cit.*, 190, «Come facciamo ad esempio a fidarci di un algoritmo se non possiamo capire davvero come ragiona, su quali dati si basa, quali principi ha seguito nel "ragionamento" che lo ha portato alla conclusione?».

<sup>71</sup> L. Romanò, *op. cit.*, 922, ove si precisa che «un altro problema in ormai "classico" in materia di IA è quello della

Ne deriva l'esigenza di delineare un sistema di garanzie capace di evitare che l'innovazione tecnologica si traduca in una surrettizia elusione dei presidi che devono governare l'esercizio del potere investigativo<sup>72</sup>.

In particolare, l'eventuale utilizzo dei sistemi di intelligenza artificiale nelle operazioni di selezioni dei dati sequestrati dovrebbe essere sorretto da taluni protocolli operativi rigorosi e previamente determinati, idonei a esplicitare i criteri di funzionamento dell'algoritmo, le categorie di dati oggetto di accertamento e i parametri di rilevanza adottati<sup>73</sup>. Solo in tal modo sarebbe possibile assicurare la verificabilità *ex post* delle operazioni compiute e, con essa, il vaglio processuale secondo i dettami dell'art. 192 Cpp.

Rimanendo nel solco fin qui tratteggiato, occorre altresì evidenziare l'impiego dell'intelligenza artificiale nel contesto della copia forense. Non si tratta di una questione di lana caprina, né un vacuo esercizio di stile. Al contrario, «tale tecnologia interviene sia nella configurazione automatica degli strumenti di acquisizione, ottimizzando parametri come il tipo di copia, sia nel monitoraggio della qualità della duplicazione». Invero, il *punctum pruriens* risiede nella capacità di questi sistemi di analizzare «in tempo reale i log di acquisizione per individuare anomalie come settori

---

*black box*, che allude all'impossibilità pratica di spiegare con esattezza il risultato prodotto dalla macchina. Da un lato entrano dati (*input*) e dall'altro vengono fuori conclusioni (*output*). Nel mezzo, "una scatola nera" la cui opacità è normalmente inaccessibile perfino ai programmatori stessi. Sicché il funzionamento dell'IA viene icasticamente paragonato da taluni a quello di un moderno "oracolo" che, contrariamente ai suoi antichi predecessori, opera con altissima precisione statistica».

<sup>72</sup> Più ampiamente, G. Canzio, *Processo penale e intelligenza artificiale: sfide e prospettive*, in *Intelligenza artificiale e indagini penali*, a cura di C. Parodi e T. Rizzo, Piacenza 2025, 7 s.

<sup>73</sup> Si vedano sull'argomento le osservazioni di S. De Flammineis, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in [www.sistemapenale.it](http://www.sistemapenale.it), 8.3.2024, 20. Si osserva che «questo processo di ricerca ed acquisizione di prove digitali mediante strumenti di intelligenza artificiale deve muoversi all'interno di binari di cautele e garanzie normativamente fissate, [...], 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 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 artificiale relativi alla c.d. polizia predittiva. 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».

danneggiati, errori di lettura, discrepanze nei valori *hash*»<sup>74</sup> suggerendo al tecnico le necessarie azioni correttive.

È imperativo, tuttavia, che l'intelligenza artificiale operi come ausilio tecnico, e non come surrogato dell'autorità giudiziaria <sup>75</sup>. Siffatto strumento è, dunque, un acceleratore necessario, ma il suo impiego *de iure condendo* richiede un rigoroso inquadramento normativo che bilanci l'efficacia con le garanzie fondamentali del giusto processo<sup>76</sup>.

In definitiva, l'irruzione dell'intelligenza artificiale nell'alveo del sequestro informatico non può essere letta né in termini salvifici né, per converso, come una minaccia alle garanzie individuali. Essa rappresenta, piuttosto, una sfida per il giurista contemporaneo, il quale ha l'onere di mantenere come stella polare il monito secondo cui «la tecnica è chiamata, alla stregua di ogni altra prova, a piegarsi alle regole e ai valori a cui si ispira il procedimento penale»<sup>77</sup>.

---

<sup>74</sup> In questi termini, P. Dal Checco, *op. cit.*, 192, da cui è tratta anche la citazione precedente.

<sup>75</sup> Ancora, P. Dal Checco, *op. cit.*, 194. In particolare, «tutto ciò [...] non può sostituire l'attività umana ma la supporta in maniera strategica: la responsabilità delle decisioni, delle valutazioni e della correttezza delle operazioni compiute rimane saldamente in capo al personale della polizia giudiziaria o al consulente tecnico. L'adozione di tecnologie basate su intelligenza artificiale, soprattutto se ben integrate nei protocolli operativi e correttamente documentate, può certamente aumentare l'affidabilità delle operazioni e ridurre il rischio di nullità, inutilizzabilità o contestazioni giuridiche e tecniche delle prove digitali».

<sup>76</sup> Sui rapporti tra intelligenza artificiale e giusto processo, si veda G. Canzio, *op. cit.*, 1 ss.

<sup>77</sup> Così, O. Murro, *Sequestro dei dispositivi informatici*, cit., 9.