PARITÀ DELLE ARMI E *DISCOVERY* DIGITALE: QUALCHE INDICAZIONE DA STRASBURGO[1]

di Laura Bartoli
(Assegnista di ricerca presso l'Università degli studi di Torino)

SOMMARIO: 1. Introduzione. – 2. Cause ed effetti di una torsione. – 3. Diritto d'accedere a cosa? Perimetro della *discovery* digitale. – 4. *Segue.* Cooperazione e controllo. – 5. Quali facilitazioni? – 6. Conclusioni.

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

Oggi la prova digitale appartiene al quotidiano; la «nuova procedura penale», invece, si sta ancora facendo attendere. Le modifiche normative si sono limitate a prendere atto dell'esistenza dei dati trattandoli perlopiù come una sorta di appendice delle tradizionali prove fisiche e la profezia si è avverata: le potenzialità dell'indagine informatica hanno travolto gli equilibri del sistema; di conseguenza, il compromesso tra pubblico potere e garanzie appare, se non più precario, meno collaudato[3]. Gli snodi che ne risentono non sono pochi: perfetti in altri contesti, risultano sghembi o comunque mal strutturati dinanzi alle geometrie che l'informatizzazione ha tracciato. Uno dei più vistosi riguarda la *discovery*: si tratta senza dubbio di uno degl'ingredienti fondamentali del diritto a godere del «tempo e delle facilitazioni necessarie a preparare

[1] Una prima versione del contributo è in corso di pubblicazione nel volume *Nuove questioni di Informatica forense*, Roma 2022. Si ringraziano i curatori per aver acconsentito alla pubblicazione su questa rivista.
[2] O.S. Kerr, *Digital Evidence and the New Criminal Procedure,* in *Columbia Law Rev.*, 2005, 279 ss.
[3] Il discorso potrebbe essere esteso anche ad altri sviluppi tecnologici recenti. Per un affascinante panorama, v. F. Caprioli, *Tecnologia e prove penali: nuovi diritti e nuove garanzie*, in *Dimensione tecnologica e prova penale*, a cura di L. Luparia-L. Marafioti-G. Paolozzi, Torino 2019, 45 ss.

la [propria] difesa» garantito dall'art. 6 § 3 *b* Conv. e.d.u.[4]. Senza un'adeguata conoscenza del caso, l'imputato non potrebbe valutare realisticamente le proprie opzioni né mettere a punto una strategia processuale informata. L'accertamento, insomma, si torcerebbe in agguato e del contraddittorio, come diritto e come metodo, resterebbero soltanto le apparenze[5]. Ma che fare se l'accusa, nel corso delle indagini, ha prelevato milioni e milioni di documenti? Quale e quanto materiale dev'essere sottoposto alla controparte? Con quanto anticipo? In quale formato? Insomma, come si deve strutturare la *discovery* perché rimanga compatibile con il principio di parità delle armi e, più in generale, con i canoni del 'giusto' processo?

Dopo una breve disamina dei fattori che complicano il segmento, passeremo in rassegna i principali temi emersi di fronte alla Corte europea dei diritti dell'uomo, analizzando di volta in volta i correttivi che i giudici di Strasburgo hanno individuato.

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

Da un lato, infatti, il semplice ammontare di informazioni riguardo a un fatto o a una persona è aumentato esponenzialmente, e non solo a causa dell'ubiquità ormai familiare di telefoni e computer. I congegni con cui una singola persona interagisce sono sempre più vari, numerosi e impercettibili, tanto integrati nella quotidianità da diventare praticamente trasparenti. Non sono rari i casi risolti grazie anche al contributo di sensori e assistenti domestici[6], tracker[7], pacemaker cardiaci[8]: tutti apparecchi capaci di consegnare agl'investigatori qualche ragguaglio su come una certa

[4] Per un'analisi della disciplina italiana della *disclosure*, specie in relazione ai diritti garantiti dalla Convenzione e.d.u. v. S. Allegrezza, *La conoscenza degli atti nel processo penale fra ordinamento interno e Convenzione europea*, in *Giurisprudenza europea e processo penale italiano*, a cura di A. Balsamo-R. Kostoris, Torino 2008, 143 ss.

[5] G. Giostra, voce *Contraddittorio*, in *EG* 2001, 1: «due pareri su un argomento non costituiscono contraddittorio, quando entrambi, o anche uno soltanto di essi, sono espressi senza conoscere preventivamente le argomentazioni della controparte [...]. Non lo costituiscono, per la semplice e decisiva ragione che due monologhi non fanno un dialogo».
Per la *discovery* come presupposto essenziale del contraddittorio "come metodo", v., nella letteratura anglofona, W.J. Brennan Jr., *The Criminal Prosecution: Sporting Event or Quest for Truth?*, in *Washington University Law Rev.* 1963, 287; M. Moore, *Criminal Discovery*, in *Hastings Law Journal*, 1968, 871.

[6] Sul punto, v. A. Bianchini, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, in *George Washigton Law Review*, 2018, 1 ss.

[7] N. Chauriye, *Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie*, in *Catholic University Journal of Law and Technology*, 2016, 495 ss.

[8] D. Paul, *Your Own Pacemaker Can Now Testify Against You in Court*, in *www.weired.com*, 29.8.2017. Per un esame approfondito delle ordinanze d'ammissione v. M.H. Maras-A.S. Wandt, *State of Ohio v. Ross Compton: Internet-enabled medical device data introduced as evidence of arson and insurance fraud*, in *The International Journal of Evidence & Proof* 2020, 1 ss.

vicenda possa essersi svolta[9]. L'accertamento penale, almeno in potenza, è in grado di mappare con precisione fatti della vita che, solo un paio di decadi fa, non sarebbe nemmeno riuscito a lambire.

D'altro canto, la quantità non è l'unico aspetto che merita attenzione. La qualità del materiale ha forzato un adeguamento delle tecniche, in modo da rendere le ricerche il più possibile affidabili e accurate: i dati, infatti, sono elementi preziosi ma effimeri, che possono essere danneggiati o persi se li si maneggia con imperizia; inoltre, è raro che il materiale rilevante sia nettamente separato da tutto il resto, facile da individuare e interpretare senza analisi più raffinate sull'archivio dal quale proviene. Per queste ragioni, molte linee guida di settore raccomandano prudenza: almeno per i casi più delicati, quando si ha a che fare con uno o più computer, è bene clonare l'intera memoria informatica con metodi che garantiscano la conformità della copia all'originale[10]. Anziché prelevare solo quel che serve, si preferisce talvolta raccogliere tutto: le porzioni interessanti saranno individuate in un secondo momento, in un ambiente protetto, magari con l'aiuto di strumenti appositi e personale specializzato[11].

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

[9] Lasceremo qui da parte i profili legati all'affidabilità e alla verificabilità dei dati generati da tali dispositivi; per un'accorta disamina dei problemi inerenti ai dati generati automaticamente, «senza alcun intervento umano nella loro rilevazione», v. S. Quattrocolo, *Qualcosa di meglio del diritto (e del processo) penale?*, in *www.discrimen.it*, 26.6.2020, 5 ss.; Id., *Equità processuale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Ítalo-Española de Derecho Procesal* 2019, 17 ss.

[10] Una eco di tali cautele si rintraccia nell'art. 19 della Convenzione di Budapest sulla criminalità informatica, laddove impone alle parti di adottare misure tali da «mantenere l'integrità dei dati rilevanti»; la disposizione è stata recepita dall'ordinamento italiano con la l. 18 marzo 2008, n. 48, che ha interpolato la disciplina delle ispezioni (art. 244 c.p.p.), delle perquisizioni (art. 247 e 352 c.p.p.), del sequestro probatorio (artt. 254 e 254-*bis* c.p.p.), dei doveri d'esibizione (art. 256), della custodia (art. 259 c.p.p.) e del sopralluogo (art. 354 c.p.p.).

[11] Sul tema si veda almeno M. Daniele, *La prova digitale nel processo penale*, in *RDP* 2011, 287 s.; G. Di Paolo, voce *Prova informatica (diritto processuale penale)*, in *ED, VI*, Milano 2013, 756 s.

Per una ricognizione degli standard tecnici e, soprattutto, per una proposta metodologica più selettiva, ma non meno affidabile, v. R. Brighi-M. Ferrazzano, *Digital Forensics: Best Practices and Perspectives*, in *Digital Forensic Evidence*, a cura di M. Caianiello-A. Camon, Padova 2020, 43 ss.

comunque delle risorse per assumere professionisti dedicati. L'accusa, inoltre, muove per prima: ha l'onere di ricostruire l'accaduto e di dimostrare la correttezza della propria versione ma, almeno inizialmente, può lavorare nel segreto e con relativa calma. Non appena si indossano i panni del difensore, invece, l'orizzonte cambia. È difficile immaginare un avvocato che, per quanto competente e avviato, disponga di una struttura tale da rivaleggiare con un ufficio di procura: non potrà contare su unità di investigatori formati e l'aggiunta di consulenti esterni al collegio difensivo dipende in maniera cruciale dalle possibilità economiche dell'assistito; i tempi della preparazione, infine, non sono indefiniti, ma dettati dell'incedere di un procedimento cui altri hanno dato impulso[12].

Dinanzi a questa realtà, ci si è chiesti innanzi tutto quanto materiale debba essere condiviso con la controparte e, in seconda battuta, se e come sia opportuno aggiornare la nozione di "facilitazioni" utili a predisporre efficacemente la difesa; l'interrogativo è stato posto ormai varie volte all'organo meglio piazzato per dare risposte innovative: la Corte europea dei diritti dell'uomo. Non essendo vincolata dagli ordinamenti nazionali, essa non deve marciare al passo dei legislatori; è giudice ultimo dell'equità del processo ai sensi della Convenzione e.d.u.: poco importa che le autorità abbiano seguito fedelmente leggi vigenti o prassi consolidate; se il risultato appare sbilanciato, la Corte di Strasburgo può censurarlo.

3. Le cautele che abbiamo appena tratteggiato fanno sì che il materiale a disposizione degl'inquirenti sia troppo; i frammenti utili devono così essere individuati e isolati da tutto ciò che non serve. Se in un'indagine tradizionale si cerca per sequestrare, nell'indagine digitale si sequestra per cercare, e l'inversione fa sì che coesistano, nell'ambito di un solo procedimento, diverse collezioni di dati: quella più vasta conterrà le informazioni "grezze", così come sono state raccolte; quello più ristretto includerà solo quelle rilevanti, che l'accusa ha intenzione di utilizzare nel corso del processo.

Per comprendere meglio il procedimento, converrà prendere ad esempio i fatti alla base di una delle pronunce più emblematiche della Corte europea in materia di *disclosure* digitale: *Sigurður Einarsson* contro Islanda[13]. Il caso riguardava un'indagine eccezionalmente ampia e complessa, che mirava ad accertare eventuali responsabilità penali nel collasso del sistema bancario islandese a seguito della crisi a seguito della crisi finanziaria del 2008. Il procuratore *ad hoc* a capo del procedimento aveva disposto il sequestro dei dati di tre istituti di credito, oltre a diversi dischi rigidi esterni di proprietà dei dipendenti. La mole d'informazioni, insomma, aveva del monumentale e

[12] Per considerazioni simili, ma riferite al campo delle indagini digitali difensive, v. M. Pittiruti, Digital evidence *e procedimento penale*, Torino 2017, 137.
[13] C. eur., 4.6.2019, *Sigurður Einarsson c. Islanda*.

chiedere a una squadra d'agenti di esaminare ciascun documento alla ricerca di elementi utili sarebbe stato irragionevolmente dispendioso in termini di tempo e di risorse; la raccolta grezza, quindi, è stata analizzata con un software in grado di eseguire ricerche per parole chiave.

Il metodo, ormai diffuso, merita una breve digressione. Esso è sempre più apprezzato non solo perché consente di separare velocemente il grano dal loglio, ma anche perché aiuta a proteggere meglio alcuni interessi rilevanti sul piano giuridico. Se il materiale fosse filtrato da un programma informatico, i dati pertinenti sarebbero evidenziati senza che nessun essere umano debba rovistare in ogni cartella o ispezionare ogni file[14]. A guadagnare terreno sarebbe innanzi tutto il diritto al rispetto della vita privata dei soggetti coinvolti, ma anche l'integrità metodologica dell'indagine: per esaminare utilmente l'archivio, gl'investigatori dovrebbero aver già tracciato una pista; il rischio di sequestri esplorativi potrebbe essere almeno attenuato[15].

Dalla massa indistinta di informazioni, ad ogni modo, viene estratto un corredo più selezionato: nel caso islandese, per esempio, una serie di ricerche a maglie sempre più strette ha permesso di restringere progressivamente il campo, fino a isolare gli elementi utili, ovvero: il materiale che l'accusa aveva ritenuto rilevante per il giudizio. Dall'angolo visuale degl'investigatori, l'operazione è del tutto fisiologica; per quanto riguarda la difesa, invece, la situazione pone quesiti delicati: i confini del diritto alla *discovery*, in particolare, si fanno sfumati. Indubbiamente, l'imputato ha diritto quantomeno a consultare il materiale che verrà usato contro di lui a processo: negargli l'accesso a quelle informazioni equivarrebbe senza dubbio a un diniego delle facilitazioni necessarie a preparare la propria difesa, incompatibile con l'art. 6 della

[14] In generale, non si tratta di un obbligo: gli inquirenti, in genere, conservano un buon grado di discrezionalità per quanto riguarda la scelta delle tecniche d'analisi. Tuttavia, gli evidenti vantaggi pratici fanno sì che si tratti di una prassi ormai piuttosto diffusa. Le linee guida emesse dal *Attorney General Office* britannico, per esempio, spiegano che, se il materiale fosse troppo, sarebbe impossibile esaminare manualmente ciascun documento elettronico, «dunque non ci si deve aspettare che ciò accada». Anzi, «è perfettamente accettabile la ricerca a campione o per parole chiave [...]. Le tecnologie di ricerca che fanno uso di calcoli inequivoci per risolvere problemi determinati, come algoritmi o *predictive coding*, costituiscono metodi accettabili per esaminare e selezionare il materiale»: *Attorney General's Guidelines on Disclosure. For investigators, prosecutors and defence practitioners*, 18.12.2020, disponibili al sito www.*gov.uk*, 32.

[15] La Corte di cassazione, in un caso, ha ritenuto violati i principi di proporzionalità e adeguatezza e, di conseguenza, ha annullato il sequestro di diversi dispositivi anche perché la polizia giudiziaria aveva iniziato lo spoglio manuale dei dati anziché attendere che il consulente tecnico del pubblico individuasse le informazioni rilevanti in base a una lista di termini di ricerca: Cass., 22.9.2020 n. 34265, in *SentenzeWeb*.
Il setaccio delle parole chiave è tanto più efficace e protettivo quanto più lo si prende sul serio: se i lemmi individuati fossero eccessivamente generici, molti dei vantaggi sfumerebbero; la privacy sarebbe maggiormente compromessa e il pericolo di manovre volte a cercare notizie di reato anziché indizi su un'ipotesi pre-esistente assumerebbe una nuova concretezza. Il profilo, di tanto in tanto, fa capolino: v., per esempio, Cass., 22.9.2020 n. 34265, cit., che non si è direttamente espressa sul punto. In Lussemburgo, invece, si è affermata l'autonomia degl'investigatori nella determinazione dei criteri: K. Ligeti-G. Robinson, *The Handling of Digital Evidence in Luxembourg,* in *Digital Forensic Evidence*, a cura di M. Caianiello-A. Camon, cit., 149.

Convenzione. Riguardo all'intero archivio informatico, però, il discorso si fa più sfumato: la maggior parte dei dati che contiene avrà probabilmente poco o niente a che vedere con il caso. Esso serve a garantire l'autenticità delle informazioni e la correttezza epistemologica dell'indagine; sul piano del contenuto, però, potrebbe non aver nulla da offrire. Qual è, quindi, l'estensione del diritto alla *discovery*? La difesa può accedere incondizionatamente anche alla raccolta "grezza" o deve accontentarsi della selezione operata dall'organo d'accusa?

Si tratta dell'interrogativo centrale di *Sigurður Einarsson* contro Islanda: gli imputati avevano avuto regolare accesso al fascicolo che conteneva il materiale rilevante ma, nonostante le ripetute richieste, veniva loro negata la possibilità di consultare l'intera raccolta di dati. Gli imputati – incassata la condanna – hanno quindi lamentato davanti alla Corte europea la violazione dell'art. 6 c. 1 e 3 lett. *b* della Convenzione: secondo i ricorrenti, l'accusa aveva potuto esaminare tutte le informazioni a suo piacimento, avvalendosi di strumenti all'avanguardia per scegliere cosa presentare in tribunale e cosa lasciar fuori; la difesa, invece, non si era potuta avvicinare: non aveva potuto svolgere ricerche autonome né individuare altri criteri di selezione. Il monopolio di fatto che la parte pubblica deteneva sulla collezione "integrale" si sarebbe risolto in una plateale e ingiustificata violazione del principio della parità delle armi: se l'accusa avesse voluto trattenere dati riservati o di cui non avesse ritenuto opportuna la diffusione, avrebbe dovuto individuarli e sottrarli dall'insieme, non sbarrare l'accesso a tutto il compendio.

Per comune ammissione delle parti, il materiale utilizzato per discutere la causa era stato messo a disposizione degli imputati e, nel corso del processo, l'accusa non aveva mai fatto riferimento ad altro. La controversia, insomma, non riguardava il diritto a conoscere ed esprimersi sulle prove presentate al giudice ma l'eventuale diritto a cercarne, estraendole da una miniera di materiale indeterminato. La Corte europea dei diritti dell'uomo, quindi, ha innanzi tutto escluso che il caso potesse essere deciso secondo gli stretti standard che giustificano l'uso di una prova deliberatamente sottratta all'esame della difesa[16], anzi: essa ha preso atto dei bisogni operativi degl'investigatori e si è soffermata sul loro metodo di lavoro. Nell'ambito di un'indagine digitale così complessa, è inevitabile che la massa di dati grezza, così come raccolta, contenga elementi che nulla hanno a che vedere con il caso: è dunque normale che gli agenti cerchino di scartare ciò che non serve, riducendo il fascicolo a dimensioni almeno gestibili. In questa fase, ha affermato la Corte, sarebbe opportuno, almeno in linea di massima, coinvolgere anche la difesa, in modo che almeno i criteri di selezione dei dati siano condivisi. L'affermazione è importante; vedremo che sarà

[16] C. eur., 23.5.2017, *Van Wesenbeeck c. Belgio*. Per una disamina della giurisprudenza precedente v. S. Allegrezza, *La conoscenza degli atti nel processo penale*, cit., 149 ss.

smorzata, ma vale la pena guardarla subito più da vicino. Il collegio non si è spinto fino a postulare un diritto d'accesso a tutto il materiale raccolto dall'accusa, ma sembra aver proiettato il principio della parità delle armi su una dimensione nuova. Normalmente, infatti, la nozione è riferita alla possibilità di presentare i propri argomenti davanti al tribunale, in condizioni che non mettano una parte in conclamato svantaggio rispetto all'altra: non si tratta di stabilire precisi equilibri durante le indagini, ma della pari opportunità di convincere il giudice che pronuncerà sentenza. Qui, invece, la Corte sembra collocare la necessità anche "a monte": se la cernita fosse fatta unilateralmente, senza controlli e senza dare alla controparte occasione di partecipare, l'articolo 6 § 1 Conv. e.d.u. sarebbe leso.

La Corte europea, però, non ha portato il principio alle sue estreme conseguenze, anzi: lo ha moderato con due considerazioni. Innanzi tutto, precisa la sentenza, si può chiedere alla difesa di motivare la propria richiesta, e si può far sì che le ragioni addotte siano vagliate dalle corti nazionali. Una generica richiesta d'accesso all'intero archivio si tradurrebbe infatti una "spedizione aleatoria" che non dovrebbe essere legittimata in ogni caso. Inoltre, una risposta negativa non comprometterebbe automaticamente la parità delle armi: nel caso concreto, il pubblico ministero non aveva perfetta cognizione di tutto il materiale; gli era noto il contenuto degli stessi documenti sottoposti alla difesa e, quindi, di fatto, non si trovava in una posizione di vantaggio. I dati non prodotti, secondo la motivazione, erano più affini a oggetti mai sequestrati che non a elementi sottratti alla *discovery* «in senso tradizionale».

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

Nel dare sue soluzioni, la Corte sembra aver complicato il problema anziché chiarirlo: è il pubblico ministero che deve aprire la conversazione con i difensori o, al contrario, sono questi ultimi a dover sollecitare approfondimenti specifici? Quando dovrebbero avvenire gli scambi? Dinanzi a quale organo? Sono temi delicati su cui la

Corte ha preferito non prendere posizione, perdendo un'eccellente opportunità per orientare legislatori e interpreti nazionali.

4. Eppure, dalla pronuncia possono scaturire spunti interessanti a patto di riordinare il quadro e precisarne meglio la premessa maggiore. La decisione, infatti, ha dato per implicito un punto fondamentale, ovvero: nulla vieta agli investigatori di fornire alla difesa tutto il materiale prelevato, rilevante e irrilevante. Anzi, la strategia della massima trasparenza da parte degli organi investigativi è stata più volte incoraggiata dalla stessa Corte europea.: in casi non dissimili, i giudici di Strasburgo non hanno esitato a riconoscere un vero e proprio diritto d'accesso alla globalità delle informazioni raccolte. Il dovere di *discovery* coprirebbe anche gli elementi privi di valore probatorio «in senso stretto, in quanto non può essere limitato a ciò che la sola accusa considera rilevante. La nozione copre piuttosto tutto il materiale che è nel possesso delle autorità e che sia dotato di rilevanza potenziale, anche se non esaminato o non ritenuto pertinente» [17]. L'accesso completo, insomma, dovrebbe essere la modalità da preferire, tanto che l'imposizione di barriere del tutto arbitrarie costituirebbe un rifiuto delle facilitazioni necessarie alla preparazione del processo e, quindi, una violazione dell'art. 6 § 3 lett. *b* Conv. e.d.u.[18].

La deviazione da questo standard può essere accettabile: si tratta allora di capire a quali condizioni sia possibile imboccare una strada alternativa senza infrangere i canoni del giusto processo. Su questo punto, il collegio di *Sigurður Einarsson* contro Islanda si è spaccato: l'opinione dissenziente parteggiava per l'applicazione di un test ben più severo, cioè quello utilizzato dalla Corte per stabilire se un processo possa essere equo quando determinate prove siano state scientemente sottratte alla difesa[19]. Stando a tale schema, ogni restrizione dovrebbe essere motivata dal bisogno di salvaguardare un diritto fondamentale altrui o un importante interesse pubblico – per esempio: l'incolumità di un testimone o la sicurezza nazionale – e sarebbe legittima solo in quanto strettamente necessaria. Se si applicasse la stessa misura alla *discovery* digitale, quindi, dovrebbe essere consegnato alla difesa ogni byte che non fosse assolutamente indispensabile sottrarle. La maggioranza dei giudici, invece, ha abbandonato maglie così strette e la posizione, tutto sommato, pare equilibrata: un conto è nascondere alla difesa prove presentate al giudice del dibattimento e utilizzate ai fini della decisione; altro è limitare l'accesso a un compendio che, per la maggior parte, è destinato comunque a rivelarsi inutile. Applicare lo stesso metro alle due

[17] C. eur., 31.8.2019, *Rook c. Germania*, § 58.
[18] In questo senso v. C. eur., 31.8.2019, *Rook c. Germania*, § 58; C. eur., 8.12.2009, *Janatuinen c. Finalndia*, § 45; C. eur., 31.3.2009, *Natunen c. Finlandia*, § 42-43, che riguarda conversazioni intercettate scelte unilateralmente dagl'inquirenti che, poi, avevano distrutto i nastri originali così come previsto dalla legge finlandese. In entrambe le occorrenze, la Corte aveva riconosciuto la violazione dell'art. 6 § 1 e 6 § 3 lett. *b* Conv. e.d.u.
[19] Opinione dissenziente del giudice Pavli a C. eur., 4.6. 2019, *Sigurður Einarsson c. Islanda*, § 4.

situazioni sarebbe probabilmente esagerato, poco pratico e a tratti addirittura controproducente: gl'inquirenti dovrebbero vagliare l'intera memoria informatica al solo scopo di individuare il materiale che è necessario escludere; i dati irrilevanti dovrebbero essere studiati nonostante non abbiano nessuna pertinenza con il fatto da accertare e i benefici portati dalla ricerca per parole chiave sfumerebbero.

Sembra insomma più saggio lasciare agl'investigatori un certo margine di manovra, accettando limitazioni d'accesso alla raccolta integrale anche sulla base di una generica quanto condivisibile preoccupazione per la riservatezza altrui. In definitiva, quindi, il perimetro della *discovery* digitale dipende in prima battuta dalla leale collaborazione tra accusa e difesa: se la natura del materiale e le circostanze del caso permettessero la serena condivisione dei dati, la procura dovrebbe consentire alla difesa d'accedere senza ulteriori mediazioni; se, al contrario, la situazione imponesse determinate cautele, gl'investigatori potrebbero a buon diritto mostrarsi più circospetti.

Perché le precauzioni degl'inquirenti non si risolvano in una problematica selezione unilaterale – o peggio: in un mero esercizio d'arbitrio – dovrebbero essere predisposti contrappesi adeguati. A questo punto, le soluzioni della sentenza *Sigurður Einarsson* offrono suggerimenti preziosi. Innanzi tutto, se l'accusa decidesse di non condividere tutti i dati con la difesa, dovrebbe quantomeno dialogare con la controparte per stabilire criteri di ricerca condivisi. La discrezionalità nella scelta del metodo resterebbe in mano agl'investigatori, senza implicare però una totale mancanza di trasparenza: i termini di ricerca potrebbero essere stabiliti in maniera condivisa o, se non altro, l'indagato saprebbe dall'inizio dell'opzione strategica della controparte e potrebbe organizzarsi di conseguenza[20]. L'incontro tra contendenti sarebbe valorizzato al meglio se fosse sfruttato per accordarsi anche su altri aspetti: per esempio, le parti potrebbero stabilire un calendario condiviso, dandosi scadenze di massima per la consegna del materiale rilevante; esse potrebbero poi stabilire un formato in cui preferiscono lavorare, disinnescando fin dal principio un buon numero di potenziali complicazioni.

Accusa e difesa potrebbero quindi cooperare e gestire la *discovery* in maniera autonoma. Se la concordia non fosse totale, però, sarebbe auspicabile l'intervento di

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

un giudice: se l'attività di spoglio degl'inquirenti fosse insoddisfacente; se i tempi previsti non fossero rispettati; se l'indagato volesse chiedere l'accesso all'intero archivio a dispetto delle scelte iniziali degl'investigatori, dovrebbe esserci un soggetto terzo e imparziale da investire delle questioni. L'interessato, a quel punto, avrebbe l'onere di spiegare perché le scelte della controparte stiano ingiustamente comprimendo il suo diritto a preparare la propria difesa. Idealmente, un controllo simile dovrebbe collocarsi prima dell'inizio del processo, in modo da affrontare le questioni in tempo utile ed evitando, per quanto possibile, intoppi nelle fasi successive. La Corte europea, ad ogni modo, non si è mostrata rigida sul limite temporale: l'art. 6 § 3 lett. *b* tollera anche soluzioni posticipate, purché la parte possa ragionevolmente familiarizzare col materiale in tempo utile per la decisione[21].

5. Poniamo che la difesa riesca a ottenere una copia integrale dei dati raccolti. Le difficoltà che abbiamo appena descritto sarebbero superate, ma il tema della parità delle armi tornerebbe ad affacciarsi seguendo percorsi diversi, quasi rovesciati rispetto a quelli di cui ci siamo occupati fin qui. Se la selezione unilaterale del materiale rilevante limita eccessivamente gli orizzonti della difesa, la condivisione dell'intero archivio potrebbe allargarli troppo: esplorare tutto con scrupolo sarebbe difficile, specie per un professionista che non è necessariamente organizzato per quel tipo di lavoro[22]. Se non si gli fornisse alcun aiuto, l'accesso al compendio integrale si rivelerebbe perfino svantaggioso rispetto a una cernita unilaterale "garantita": su grossi volumi, incappare rapidamente in dati utili sarebbe improbabile; trovare anche solo la cartella in cui potrebbe celarsi qualche elemento interessante potrebbe richiedere settimane di lavoro. Di fatto, la selezione finirebbe per essere parziale quanto prima, troncando per di più sul nascere ogni possibile lamentela della difesa, cui è stato riconosciuto il massimo accesso possibile.

Da una considerazione simile muove gran parte del dibattito statunitense, più preoccupato dalla sistematica *disclosure* dell'intero archivio che non da dinieghi ingiustificati. In quell'ordinamento, del resto, la legge non chiede all'accusa di mostrare tutte le carte, anzi: la regola del "fascicolo aperto", pur applicata in qualche ordinamento statale, è del tutto recessiva. Il dovere di rivelazione degli atti d'indagine si estende soltanto a ciò che si intende presentare al giudice, nonché agli elementi che

[21] C. eur., 31.8.2019, *Rook c. Germania*, § 73.

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

possono essere considerati favorevoli all'imputato[23]: normalmente, quindi, la difesa accede a un compendio altamente selezionato, che svela la strategia dell'avversario e le permette di lavorare di conseguenza[24]. Il digitale, però, ha complicato lo scenario: realisticamente, il procuratore non riuscirebbe a trovare, nel pagliaio, l'ago che anche solo per ipotesi potrebbe essere utile alla difesa; per non incorrere nella violazione dei suoi doveri istituzionali, allora, rivela tutto, lasciando all'imputato il compito di sbrogliare la matassa e trovare ciò che può essere rilevante. Più che essere percepita come un diritto, la possibilità di rovistare in tutte le memorie informatiche sequestrate è quindi vissuta come un passo indietro, se non proprio come una strategia elusiva o una «trappola»[25]. Alcuni autori, in quel contesto, hanno quindi provato a riaffermare la necessità di una selezione attenta: la tecnologia è mutata, ma i doveri costituzionali che gravano sull'accusa no. Gli investigatori avrebbero dunque l'onere di setacciare tutto il materiale, in modo da poter sottoporre alla controparte gli elementi potenzialmente rilevanti[26]: aiutare la difesa significherebbe studiare il contenuto di ogni file.

Per rendere equo il processo, stando a queste opinioni, occorre che tutti i dati siano sondati e, singolarmente, siano trattenuti o scartati; il peso dell'operazione non potrebbe che cadere sulla parte meglio strutturata per condurre un lavoro di questo tipo, ovvero la pubblica accusa. La linea, comprensibilmente, ha incontrato una ferma opposizione: il carico di lavoro sarebbe enorme, e non è detto porterebbe a risultati soddisfacenti; per presentare una sintesi utile o per rinvenire elementi a discarico, gli agenti dovrebbero saper valorizzare le sfumature più favorevoli alla strategia che la difesa intende adottare, forte anche delle conoscenze e delle indicazioni confidenziali del diretto interessato. Per questo, gli standard delle autorità investigative[27], diverse

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

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

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

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

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

decisioni[28] e non pochi studiosi[29] hanno respinto l'opinione.

Una strada più proficua, forse, potrebbe passare da una riflessione sugli strumenti più che sull'attività: se la difesa avesse modo di svolgere analisi autonome, agevolata da programmi informatici paragonabili a quelli del pubblico ministero, le difficoltà d'orientamento si diraderebbero. La giurisprudenza statunitense procede spedita in quella direzione: per soddisfare i propri doveri, secondo diversi arresti, il pubblico ministero non può limitarsi ad aprire il fascicolo e lasciare che l'imputato trovi da solo gli elementi che più gl'interessano; deve condividere dati navigabili, su cui sia tecnicamente possibile svolgere ricerche rapide e mirate[30]. Sul fronte europeo, la Corte di Strasburgo ha avuto modo di dare qualche direttiva nella pronuncia *Rook* contro Germania, di cui gioverà occuparsi brevemente.

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

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

[29] V. J.I. Turner, *Managing Digital Discovery in Criminal Cases*, in *Journal of Criminal Law and Criminology*, vol. 109 (2017), f. 2, 301.

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

in un formato leggibile tramite programmi a licenza gratuita.

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

6. Dalle vicende che abbiamo riassunto emerge un tratto comune: quando il volume d'informazioni è umanamente inaffrontabile, le dinamiche della *discovery* meritano di essere riconsiderate. L'impersonale deposito del fascicolo, in quelle condizioni di lavoro, non basta ad assicurare le "facilitazioni" necessarie alla preparazione della difesa: se esso contenesse tutto, rischierebbe di paralizzare la difesa dell'imputato, specie se non facoltoso; se esso includesse solo i frammenti scelti dal pubblico ministero, la difesa potrebbe avere difficoltà a proporre al giudice una ricostruzione alternativa convincente e documentata.

Da questo paradosso, la prassi tende a uscire innanzi tutto tramite il dialogo tra le parti: la leale collaborazione, almeno potenzialmente, potrebbe sciogliere parecchi nodi di metodo, di calendario e di formato. Ciò però non significa che accusa e difesa, debbano essere lasciate sole, anzi: i loro accordi guadagnerebbero in equità e trasparenza se la conversazione partisse da presupposti chiari e si sviluppasse in sedi e in tempi stabiliti, con la possibilità di chiamare in causa garanti imparziali[31].

[31] Pur cercando soluzioni a un problema parzialmente diverso, la dottrina di lingua italiana ha avanzato varie proposte, come quella di svolgere lo scrutinio del materiale in incidente probatorio (F. Iovene, *Perquisizione e sequestro di computer: un'analisi comparatistica*, in *RDP*, 2012, 1616) o di istituire un'apposita udienza di selezione (L. Bartoli, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *AP* 2018, rivista *web*, 1, 18; S. Carnevale, *Copia e restituzione di documenti informatici sequestrati*, in *DPP* 2008, 481; L. Luparia, Computer crimes *e procedimento penale*, in *Modelli differenziati d'accertamento*, a cura di G. Garuti, in *Trattato di procedura penale*, diretto da G. Spangher, vol. VII, t. 1, Torino 2011, 375; G. Schena, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*, in *CP* 2016, 306).

Le corti statunitensi, pur muovendo da diverse premesse, hanno già avuto modo di dettare regole più avanzate; sull'onda di quell'evoluzione, anche i testi normativi sono stati aggiornati[32]. Gli ordinamenti europei sembrano presentare tempi di reazione più lenti, ma questo non vuol dire che gli stessi temi non siano già emersi: a maggior ragione, la Corte di Strasburgo avrebbe potuto fare da apripista e spronare legislatori e interpreti. Essa, però, non ha sfruttato fino in fondo le occasioni che le sono finora state offerte: non ha mai tentato di dettare uno statuto completo della *discovery* digitale pienamente compatibile con i diritti garantiti dalla Convenzione; si è limitata a giocare di rimessa, ratificando gli atteggiamenti virtuosi e censurando, ma solo a parole, le prassi meno trasparenti. Anche le dichiarazioni più utili e coraggiose sono state stemperate in passaggi motivazionali imprecisi, poco chiari quanto a oggetto e scopi e, infine, neutralizzate dalla valutazione dell'equità del procedimento "nel suo complesso", ormai consueta quanto criticata[33]. La vicenda della *discovery* digitale, insomma, sembra confermare una diagnosi già formulata in termini più generali[34]: anche in questo settore, pare che la Corte europea abbia deciso di abdicare al ruolo di avanguardia che un tempo rivendicava; se si esaspera l'approccio caso per caso e se si ammettono fattori compensativi capaci di rimediare a (quasi) qualsiasi violazione[35], la giurisprudenza nel suo insieme non potrà che risultare ambivalente, incapace d'esprimere equilibri univoci. L'opera di razionalizzazione degli interpreti, dunque, appare più che mai preziosa sia per suggerire soluzioni operative immediatamente utilizzabili, sia per avanzare, in prospettiva, innesti normativi capaci di riconciliare il progresso tecnologico con le scelte di valore alla base del sistema processuale.

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

[33] Per un recente consuntivo, v. A. Boldrin, *Approccio compensativo e* overall fairness *nella giurisprudenza della Corte EDU, tra relativismo delle garanzie e altre derive*, in *www.lalegislazionepenale.eu*, 26.10.2021. L'opinione dissenziente del giudice Pavli a C. eur., 4.6.2019, *Sigurður Einarsson c. Islanda*, § 28 ha fortemente criticato tanto gli argomenti, incluso l'impiego indiscriminato del criterio della equità del caso nel suo complesso, tanto il generale atteggiamento elusivo a suo avviso adottato dalla maggioranza del collegio.

[34] M. Caianiello, *You Can't Always Counterbalance What You Want*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2017, 283 ss.

[35] Fanno eccezione soltanto le violazioni all'art. 3 Conv. e.d.u., costantemente e severamente riconosciute inaccettabili e, quindi, non bilanciabili: C. eur., 5.11.2020, *Ćwik c. Polonia*. Per una lettura ordinata del fenomeno v. A. Cabiale, *I limiti alla prova nella procedura penale europea*, Padova 2019, 133 ss.