QUESTIONI APERTE

Mezzi di ricerca della prova - Sequestri

La decisione

Dati informatici - Estrazione copia dati contenuti nel computer in sequestro - Richiesta di riesame - Conferma del decreto di sequestro - Restituzione del computer all'avente diritto - Ricorso per cassazione - Ammissibilità – Condizioni (C.E.D.U. art. 8 e 10; c.p.p. artt. 252-258, 324, 325, 352, 354, 355, 568, 591; L. 18 marzo 2008, n. 48).

È ammissibile il ricorso per cassazione avverso l'ordinanza del tribunale del riesame di conferma del sequestro probatorio di un computer o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati ivi contenuti, sempre che sia dedotto l'interesse, concreto e attuale, alla esclusiva disponibilità dei dati.

CASSAZIONE PENALE, SEZIONI UNITE, 7 settembre 2017 (ud. 20 luglio 2017), – CANZIO, *Presidente* – RAMACCI, *Relatore* – CARDIA, *P.G.* (conf.) – Andreucci, *ricorrente*.

Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature

Il commento si sofferma sui principali passaggi della sentenza Cass., Sez. un, 20 luglio 2017, n. 40963, Andreucci, che torna a occuparsi del rapporto tra sequestro probatorio, copia d'informazioni e interesse a impugnare.

The essay points out the principal traits of the decision Cass. s. u., July 20th 2017, n. 40963, Andreucci, that deals with the intricate relationship between seizure, the copy of information and the right to a judicial review.

1. Una decennale ambiguità.

Con questa sentenza, le Sezioni unite tentano di ricucire i labbri di una questione aperta da più di vent'anni, sospesa tra progresso tecnologico e regole sbiadite. In mezzo, il sequestro. Per com'è descritto dal libro terzo del codice, 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. Chi ha patito l'atto potrà poi invocarne il controllo giudiziale tramite il riesame, così da impedire

compressioni indebite del diritto di proprietà[1]. Questo schema, impeccabile per linearità, s'è però incrinato: l'affinarsi della tecnica ci ha consegnato apparecchi capaci di riprodurre documenti in maniera economica, veloce e affidabile, aprendo scenari inaspettati. Perché trattenere in originale il materiale sequestrato, quando si può duplicare e restituire? Tutte le informazioni resterebbero salve agli atti, mentre la cosa potrebbe essere riconsegnata ben prima della fine del processo. La copia potrebbe persino esser prodotta sul posto, raggiungendo lo scopo senza sottrarre nemmeno un foglio di carta. L'informatica ha poi ampliato le possibilità d'uso dello stratagemma: clonata la memoria, il dispositivo potrebbe essere tranquillamente svincolato[2].

Il metodo è semplice e poco invasivo: in fondo, concilia bene gl'interessi della proprietà con quelli dell'accertamento, giocando sulla separazione tra il documento e il suo contenuto; proprio per questa ragione s'è promosso il suo impiego, anche in ossequio al principio di proporzionalità: a parità di risultato, dovrebbe essere scelto l'atto che meno incide sulle libertà di chi lo patisce[3].

Si crea tuttavia una situazione difficile da afferrare. Da un lato c'è un oggetto restituito o addirittura mai sottratto; dall'altro la sua essenza resta nelle mani degl'inquirenti, e secondo una forma che non corrisponde esattamente alla sagoma di un sequestro[4]. Che nome dare, quindi, a questo atto? A quale re-

---

[1] SELVAGGI, *Commento all'art. 257 c.p.p.*, in *Commento al nuovo codice di procedura penale*, a cura di Chiavario, vol. II, Torino, 750 s., secondo il quale «la previsione del riesame del provvedimento disposto a fini probatori [...] intende soddisfare all'esigenza di predisporre un sistema di controllo su qualsiasi provvedimento che si presenti astrattamente idoneo a incidere su diritti garantiti a livello costituzionale (diritto di proprietà e libertà di iniziativa economica)»; TRANCHINA (voce), *Sequestro penale*, in *Enc. giur.*, vol. XXVIII, 6. Per un'impostazione differente, v. MONTONE (voce), *Sequestro penale*, in *Nov. dig. disc. pen.,* vol. XIII, Torino, 1997, 260: l'Autore sostiene che il riesame possa avere come scopo quello di escludere una determinata *res* dal compendio probatorio.

[2] Senza dimenticare di prendere precauzioni a tutela dell'indagine: in mancanza di direttive precise, il proprietario potrebbe anche decidere di divulgare tutto ciò che gl'inquirenti avevano carpito; v. Cass. sez. VI, 16 febbraio 2011, n. 20105, p.m. in Spirolazzi, in *Mass. Uff.,* n. 250493.

[3] Sulle potenzialità della copia, specie in ambito informatico: v. CHELO MANCHIA, *Sequestro probatorio di* computers*: un provvedimento superato dalla tecnologia?*, in *Cass. pen.*, 2005, 1634 s.; MONTI, *No ai sequestri indiscriminati di* computer, in *Dir. dell'Internet*, 2007, 268 s.; ID., *La nuova disciplina del sequestro informatico*, in *Sistema penale e criminalità informatica*, a cura di Lupária, Milano, 198-199; VENTURINI, *Il sequestro probatorio e fornitori di servizi informatici*, in Lupária *Internet provider e giustizia penale*, a cura di Lupária, Milano, 2012, 116 s.
Per il principio di proporzionalità rispetto agli atti d'indagine v. CAMON, *La prova genetica tra prassi investigative e regole processuali*, in *Proc. pen. giust.*, 167; per uno sguardo più generale e un diverso approccio al tema, v. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale,* in *Dir. pen. cont.*, 2014, f. 3-4, 144.

[4] Sottolineava l'ambiguità BONSIGNORE, *L'acquisizione di copie in luogo del sequestro: un atto atipico elusivo delle garanzie difensive*, in *Cass. pen.*, 1998, 1515 s.

gime giuridico si può ricondurre? Si può sempre adire un giudice, anche quando la cosa è stata restituita?
La Corte di cassazione è tornata sul punto, scontando un quadro normativo scarno e una scia di precedenti contraddittori che esamineremo subito, prima di passare all'analisi del nuovo approdo.

2. Panorama normativo e giurisprudenziale.

A dire il vero, un punto di partenza dovrebbe esserci: l'art. 258 c.p.p. disciplina infatti la copia dei documenti sequestrati, ma non sembra nemmeno cosciente del problema. D'altronde il testo è la reincarnazione dell'art. 343 del codice previgente: contempla solo quanto aveva senso disciplinare negli anni '30, quando le tecniche di copia si limitavano alla carta carbone; non si confronta certo con le potenzialità di strumenti che sarebbero apparsi soltanto decenni più tardi[5].
Alla giurisprudenza è così toccato il compito di ricondurre situazioni ambigue a categorie note, in uno sforzo interpretativo che ha prodotto risultati oscillanti. Nella maggior parte dei casi, l'estrazione di copia era considerata un provvedimento a sé, del tutto separato dal vincolo precedente[6]; quando poi era eseguita "sul posto", duplicando subito quanto rinvenuto nel corso di una perquisizione, le veniva semplicemente negata la qualifica di 'sequestro'[7].
Al singolo era di conseguenza sbarrato l'accesso al riesame: la lesione della proprietà, se mai esistita, non era più attuale; il risultato tipico dell'impugnazione – il dissequestro – era già stato raggiunto, cosa che faceva venir meno l'interesse a proporre il gravame. Del resto, ogni questione su eventuali invalidità poteva essere deferita al giudice del dibattimento, senza attivare per questo un procedimento incidentale[8].

---

[5] La disposizione, infatti, si limita a chiarire che l'autorità giudiziaria può estrarre copia di atti e documenti sequestrati, attribuendo il diritto di chi li deteneva legittimamente a farsene rilasciare copia autentica. Sulla tradizione testuale della norma tra vecchio e nuovo codice v. SELVAGGI, *Commento all'art. 258 c.p.p.*, in *Commento al nuovo codice di procedura penale*, a cura di Chiavario, vol. II, Torino, 753.

[6] Cass. sez. VI, 3 giugno 1994, n. 2682, Marini, in *Mass. Uff.*, n. 199141.; Cass. sez. VI, 10 aprile 1998, n. 1331, Pomenti, *ivi*, n. 211590; Cass. sez. VI, 3 giugno 1998, n. 2073, p.m. in Colasante, *ivi*, n. 212219; Cass. sez. II, 23 marzo 1999, n. 1480, Ferrari, *ivi*, n. 213306; Cass. sez. IV, 13 dicembre 2001, n. 26506, p.m. in Mattei, in *DeJure*; Cass. sez. II, 20 dicembre 2005, n. 3598, Canzano, in *Mass. Uff.*, n. 233335; Cass. sez. II, 14 giugno 2007, n. 24958, Cal, *ivi*, n. 236759; Cass. sez. II, 5 luglio 2007, n. 32881, Sandalj, *ivi*, n. 237763.

[7] Cass. sez. III, 26 gennaio 2000, n. 384, Motta, in *Mass. Uff.*, n. 217687; Cass. sez. VI, 23 maggio 2003, n. 35087, Bonaduce, *ivi,* n. 226753.

[8] Le decisioni sono le stesse già citate alla nota n. 6.

Qualche decisione ragionava però diversamente, postulando l'interdipendenza tra sequestro e copia; senza aver vincolato il materiale, non lo si sarebbe nemmeno potuto riprodurre: i vizi del primo atto finivano così per propagarsi anche al secondo[9]. Altre volte s'intravedeva un interesse ulteriore alla restituzione della cosa: quello al rispetto delle disposizioni di legge che presiedono alla raccolta degli elementi di prova[10]. In entrambi i casi, comunque, s'affermava il diritto al controllo giurisdizionale.

A partire dal 2008, tuttavia, le coordinate del discorso si sono spostate tanto sul piano legislativo quanto su quello giurisprudenziale.

Il codice di procedura penale ha infatti subito numerose modifiche perché fosse attuata la Convenzione di Budapest sulla criminalità informatica: la serie d'interventi ha sottolineato in più punti la differenza tra dati e sistemi in cui sono ospitati[11]. Quella più interessante ai nostri fini è l'art. 254-*bis* c.p.p. che, proprio nel descrivere un'ipotesi di sequestro, slega l'atto dalla corporeità della cosa. Stando a questa previsione, infatti, i dati in quanto tali possono essere prelevati a prescindere da ciò che accade al dispositivo; s'individua anche una tecnica specifica d'apprensione: la copia, che assurge ufficialmente al rango di vincolo. La lettera della norma, però, è particolarmente limitata: essa si riferisce soltanto ai fornitori di servizi telematici, con il dichiarato intento di garantire la continuità delle loro prestazioni.

Se la legge sembrava affermare l'autonomia del dato, la giurisprudenza s'è mossa rapidamente nella direzione opposta: una sentenza resa a sezioni unite ha infatti consacrato gli orientamenti più restrittivi, e non senza ostentare una

---

[9] Cass. sez. II, ordinanza del 22 febbraio 1995, n. 1143, p.m. in Magliuolo, in *Mass. Uff.*, n. 201586; Tribunale di Brescia, sez. riesame, ordinanza del 9 ottobre 2006, in *Diritto dell'Internet*, 2007, 264, con commento di MONTI, *No ai sequestri indiscriminati di* computer; anche in *Giur. di merito*, 2007, 1110, con nota di GABRIELLI, *Il sequestro probatorio non supera il riesame: la copia dell'hard-disk ritorna al giornalista, sia pure con qualche "scorciatoia" argomentativa.*

[10] Cass. sez. V, 19 giugno 1990, n. 3308, Menci, in *Mass. Uff.*, n. 185304; Cass. sez. VI, 1 luglio 2003, n. 36775, Ronco, in *Cass. pen.*, 2005, 914, con nota di CANTONE, *Sulla riesaminabilità del decreto di sequestro di cose già restituite*; Cass. sez. VI, 31 maggio 2007, n. 40380, Sarzanini, in *Dir. pen. proc.*, 2008, 1417, con nota di MACRILLÒ, *Segreto* ex *art. 200 c.p.p. e sequestro del* computer *in uso al giornalista*; in *Giur. it.*, 2008, 732, con osservazioni di GABRIELLI, *Quando il sequestro probatorio ha per oggetto l'*hard disk *del* computer *di un giornalista*; in *Il diritto dell'informazione e dell'informatica*, 2008, 743, con commento di BACCHINI, *Il sequestro probatorio nei confronti del giornalista non indagato: il problema del bilanciamento di interessi costituzionalmente garantiti ed il rischio di elusione delle tutele.*

[11] La legge con cui s'è adeguato il codice alla Convenzione è la l. 18 marzo 2008, n. 48; per un commento v. PICOTTI-LUPÁRIA, *La ratifica della convenzione* cybercrime *del Consiglio d'Europa*, in *Dir. pen. proc.*, 2008, 696 s.; LUPÁRIA, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(L. 18 marzo 2008, n. 48)*, Milano, 2009.

certa mancanza di tatto; nell'affrontare la questione, la Corte s'ispirava a un precedente[12] che trattava del diritto al riesame per il sequestro di un'automobile poi restituita, suggerendo un accostamento tra informazioni e vetture di per sé eloquente. S'è così ribadito che, restituita la cosa, l'effetto tipico dell'impugnazione è già raggiunto e dunque non c'è interesse a impugnare, anche se i dati sono rimasti agli investigatori[13].

La barra è rimasta sostanzialmente ferma – pur con qualche occasionale sbandamento[14] – fino al 2015, quando la novella del 2008 è tornata in scena. Valorizzando a dovere tutte le interpolazioni, la Corte ha finalmente ribaltato la premessa: ai dati è stata riconosciuta autonomia rispetto al supporto e, dunque, la capacità d'esser sequestrati. Se contenitore e contenuto sono chiaramente distinti, la restituzione del bene, di per sé, non basta a metter fine alla partita. Sulla chiusura del ragionamento, tuttavia, i sentieri della giurisprudenza si sono ancora biforcati.

Secondo una prima tesi, la permanenza del vincolo non renderebbe ammissibile ogni richiesta di riesame[15]. Per accedere a una verifica giurisdizionale, bisognerebbe infatti dimostrare che il valore dell'informazione risiede nell'esclusività del suo controllo. Solo allora il pregiudizio sopravvivrebbe alla restituzione del bene, poiché il monopolio sarebbe comunque rotto

---

[12] Si tratta di Cass. sez. un., 20 dicembre 2007, n. 230, Normanno, in *Mass. Uff.*, n. 237861.

[13] Cass. sez. un., 24 aprile 2008, n. 18253, Tchmil, in *Dir. pen. proc.*, 2009, 469, con nota di CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*; in *Cass. pen.,* 2008, 4031, con osservazioni di APRILE.

[14] Aderiscono alla linea delle sezioni unite: Cass. sez. VI, 24 aprile 2012, n. 29846, Addona, in *Mass. Uff.*, n. 253251; Cass. sez. III, 30 maggio 2014, n. 27503, Peselli, *ivi*, n. 259197. La duplicazione di materiale non vincolato restava un non-sequestro: Cass. sez. II, 30 giugno 2010, n. 29019, Fontana, *ivi*, n. 248143. In aperta contraddizione si poneva invece Cass. sez. VI, 28 maggio 2013, n. 26291, Antonini, *ivi*, n. 256813, riconoscendo un legame tra provvedimento di sequestro ed estrazione di copia tale da consentire la propagazione dei vizi del primo.

Qualche confusione era destata anche dall'ipotesi in cui ad impugnare fosse il pubblico ministero, obbligato dal riesame a restituire gli originali avendo già estratto copia del materiale: in un caso, il ricorso è stato dichiarato inammissibile per carenza d'interesse poiché i duplicati erano rimasti agli atti: Cass. sez. V, 10 febbraio 2010, n. 14897, p.m. in Pieri, *ivi*, n. 246869. *Contra*, Cass. sez. VI, 26 giugno 2009, n. 26699, p.g. in Genchi, *ivi*, n. 244395.

[15] Cass. sez. VI, 24 febbraio 2015, n. 24617, Rizzo, in *Giur. it.*, 2015, 1503 s., con nota di LORUSSO, *Sequestro probatorio e tutela del segreto giornalistico*; in *www.penalecontemporaneo.it*, 25 luglio 2015, con commento di CERQUA, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza* elettronica; in *Arch. n. proc. pen.,* 2016, 269 s., con osservazioni di COSTANZI, *Perquisizione e sequestro informatico. L'interesse al riesame nel caso di estrazione di copie e restituzione dell'originale*; in *Cass. pen.,* 2016, 286 s., con nota di SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*. Lo stesso afferma Cass. sez. II, 9 settembre 2016, n. 40831, Iona, in *Mass. Uff.*, n. 267610.

dall'esistenza di un duplicato. L'interesse a impugnare mancherebbe invece «laddove non permanga una perdita valutabile per il titolare del bene»[16].
S'è però imboccata anche un'altra strada, assai più generosa: stando a una seconda interpretazione, infatti, l'attualità di un vincolo implicherebbe di per sé il diritto a rivolgersi a un giudice[17]; si tratterebbe di una garanzia procedurale minima, persino necessaria.
La questione è così tornata alle sezioni unite meglio scandita, analizzata in ogni passaggio dall'ordinanza di rimessione[18]. Preso atto del contrasto, la sezione semplice ha sottolineato come lo scollamento tra dati e supporto – che accomuna carta stampata e informazioni digitali[19] – metta lo strumento del riesame di fronte a un bivio: se dovesse tutelare solamente il diritto di proprietà e restaurare il rapporto con la cosa, non sarebbe necessario estendere la tutela. Se invece dovesse proteggere anche altri diritti della persona come la riservatezza, il diritto al segreto o all'informazione, il concetto d'interesse scolpito nel 2008 sarebbe insufficiente: al singolo spetterebbe infatti il diritto d'agire non soltanto per tornare nel possesso della cosa, ma per riguadagnare l'esclusiva disponibilità del proprio patrimonio informativo.

3. La consistenza autonoma dell'informazione.

Le sezioni unite non hanno affrontato la questione per come era stata loro sottoposta: ogni accenno alla duplicazione di documenti cartacei è stato tagliato via. La rinuncia a coltivare parallelismi con la carta stampata, però, rende il prodotto incompleto, asimmetrico: le conclusioni, di conseguenza, appariranno traballanti, poggiate su un legno storto[20].
Ad ogni modo, la Corte s'è trovata a un punto di partenza quasi obbligato: per prima cosa, infatti, occorre saggiare la consistenza del dato per stabilire se sia possibile sottoporlo a sequestro prescindendo dal supporto.
Sul tema, la legge è disseminata d'indicazioni che le sezioni unite hanno pazientemente spigolato, rintracciando nei singoli frammenti una direzione tal-

[16] Cass. sez. VI, 24 febbraio 2015, n. 24617, Rizzo, cit.
[17] Cass. sez III, 21 settembre 2015, n. 38148, Cellino, in *Dir. pen. proc.*, 2016, 508 ss., con nota di ZAMPERINI, *Impugnabilità del sequestro probatorio di dati informatici*.
[18] Cass. sez. VI, ordinanza del 29 maggio 2017, n. 21121, in *www.penalecontemporaneo.it*, 21 luglio 2017.
[19] Si osserva appunto che il dilemma del digitale «è certamente assimilabile alla estrazione di copie di documenti cartacei mediante una fotocopia o una scansione che sia tale da realizzare una riproduzione perfettamente fedele ed "indistinguibile" dall'originale restituito all'avente diritto. [...] Il contrasto fra gli opposti orientamenti va dunque oltre la peculiarità del dato informatico».
[20] Sul rapporto tra la decisione e la carta stampata si tornerà più ampiamente al § 7.

mente univoca da concludere che le informazioni sono «pacificamente» autonome dal dispositivo in cui alloggiano[21].
Informazione e supporto sono dunque entità distinte, che possono essere indipendentemente vincolate dagl'inquirenti e c'è da esser grati alle sezioni unite per averlo affermato in modo così chiaro; in realtà era necessario raschiar via dalla mentalità giurisprudenziale i vari strati di vernice che l'avevano resa a lungo impermeabile – quantomeno su questo versante – alle novità legislative del 2008.
La concezione esclusivamente "corporea" del sequestro sembrava ormai stare stretta anche alla Corte: prova ne è il fatto che la prima sentenza dissonante non è più stata smentita su questo punto; nessuna pronuncia successiva è tornata alla tesi opposta, che pure aveva dominato per oltre un lustro. Questa decisione ratifica quindi il cambio di temperatura: il piglio con cui si è guardato al patrimonio informativo appare svecchiato e ben più in linea non solo con le norme di legge che lo riguardano, ma anche con il dibattito pubblico sulla sua tutela. In filigrana, infatti, s'intravede anche un fattore di contesto: i dati giocano ormai un ruolo chiave nella nostra vita quotidiana e del loro valore si è sempre più consapevoli; sono ormai riconosciuti come la risorsa più preziosa al mondo[22], senza contare che ciascuno attribuisce loro un'importanza persino superiore a quello del dispositivo, come gli attacchi *ransomware* dimostrano con efferata chiarezza[23].
L'informazione è dunque un oggetto a sé, e questo elemento costituisce il primo anello della catena: resta da precisare quando e come lo si vincola, tracciando i contorni di un sequestro immateriale.

---

[21] A quanto risulta, l'unica voce contraria all'assunto è quella di ZAMPERINI, *Impugnabilità del sequestro probatorio di dati informatici*, cit., 515, ad avviso della quale il materiale digitale può essere vincolato soltanto attraverso il supporto; ritenere diversamente significherebbe, secondo l'autrice, «ammettere la sequestrabilità di un'idea o di un pensiero».
[22] Secondo il settimanale *The Economist*, i dati hanno ormai scavalcato il petrolio nella classifica delle materie prime di valore: v. *The world's most valuable resource is no longer oil, but data,* 6 maggio 2017, in *www.economist.com*; nei paesi del G7, il 70% del prodotto interno lordo è legato a informazioni, non a beni materiali: FLORIDI, *Information: a very short introduction*, Oxford, 2010, 9.
[23] Si tratta di operazioni criminali svolte infettando il computer con un *software* malevolo che critta tutti i dati, rendendoli così illeggibili. Per tornare ad averli in chiaro è necessaria una chiave di cifratura che gli hacker s'impegnano a comunicare dietro pagamento di una somma di denaro. Versando il riscatto e ammesso d'avere a che fare con estorsori onesti, gli *hard disk* saranno sbloccati. Il supporto fisico, naturalmente, è intatto e una formattazione basterebbe a eliminare il virus; ciò nonostante, un numero impressionante di persone è disposto a pagare un prezzo più caro del dispositivo stesso, pur di poter riavere in chiaro le proprie informazioni. Sebbene gli esperti di sicurezza informatica suggeriscano di non versare denaro, il successo di questi ricatti ha fatto sì che la cifra sia progressivamente aumentata: v. HOWELL O' NEIL, *Ransomware demands now average about $1,000 because so many victims decide to pay up*, 26 aprile 2017, *www.cyberscoop.com*.

4. Intermezzo: di cosa parliamo quando parliamo di copia.

A questo punto, la Corte allarga il discorso a un altro tema, legato solo in parte a quello principale e destinato a non avere riflessi diretti sul dispositivo; se fin qui s'era parlato di duplicazione come vincolo, se ne sottolinea adesso il ruolo nell'assicurare l'autenticità del materiale acquisito. La decisione s'addentra così nel terreno dell'indagine informatica, offrendo spunti su cui è il caso di soffermarsi.

Le sezioni unite notano che la legge si limita a fissare un obiettivo, lasciando agli operatori un certo grado di libertà sulla scelta delle tecniche: l'importante è che si adottino precauzioni tali da garantire la tutela dell'originale e la conformità della replica. Del resto, è bene che il legislatore non si sia improvvisato meccanico: la tecnologia corre veloce e le situazioni che possono presentarsi nella prassi sono pressoché infinite; intervenire con il giusto grado di precisione, elasticità e aggiornamento sarebbe probabilmente impossibile. Non si è corso il rischio di irrigidire la disciplina, ma si è caduti nella tentazione opposta: gli scopi fissati dal codice non sono presidiati da invalidità di sorta, né la legge rinvia a linee guida capaci di orientare tanto le parti nel loro lavoro quanto il giudice nella sua valutazione. La norma, in sostanza, s'affida al buon senso di chi agisce; ogni elemento acquisito in violazione delle regole tecniche sarà liberamente valutabile: potrà tutt'al più perdere d'efficacia persuasiva.

Le migliori pratiche di settore forniscono pur sempre un buon punto di riferimento operativo, individuando i modi di procedere più sicuri: uno di questi, la *bit stream image*, ha raggiunto una certa notorietà e anche la decisione in commento le ha dedicato parecchio spazio. Si tratta della clonazione di una memoria che avviene duplicando integralmente ogni *bit* secondo l'ordine in cui si trova nell'originale; se l'operazione è correttamente eseguita, la copia sarà identica alla matrice, e la loro corrispondenza potrà essere verificata[24]. Ogni modifica postuma lascerebbe quindi una traccia: la mancanza di conformità emergerebbe, ipotecando seriamente la credibilità dell'elemento.

La Corte ripercorre i pregi della tecnica, sottolineando che la sua adozione è facoltativa, da calibrare a seconda della complessità del caso: la legge 48/2008

[24] Per svolgere questo controllo, si utilizzano generalmente una o più funzioni di *hash*: per una compiuta descrizione della tecnica v. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. Pen. Proc. – Dossier: La prova scientifica nel processo penale*, 2008, 62 s.; CASEY, *Digital Evidence and Computer Crime*, III ed., Waltham, 2011, 22 s.; BARTOLI, *La catena di custodia del materiale informatico: soluzioni a confronto*, in *Anales de la Facultad de Derecho – Universidad de La Laguna*, 2016, vol. 33, 153 s.

aveva in mente uno strumento tanto raffinato perché si dirigeva contro un tipo di criminalità – quella informatica – che richiede queste scaltrezze per carpire tutti gli elementi utili. Le stesse precauzioni non sarebbero invece necessarie per operazioni più semplici: se si tratta di acquisire un testo – insiste la motivazione – non serve andar tanto per il sottile; una procedura meno sofisticata potrà bastare.

Di per sé, la conclusione regge: come s'accennava, nulla obbliga gl'investigatori a prediligere un metodo operativo; l'immagine forense, in più, non è sempre un'opzione accessibile: richiede tempo e su grossi volumi è talmente antieconomica da essere addirittura impraticabile[25].

Il discorso della Corte, tuttavia, sembra non tenere conto di un elemento. Gli innesti normativi del 2008 hanno un raggio ampio; il codice di procedura non distingue le precauzioni operative per tipo di reato o per complessità dell'indagine[26] e per una buona ragione: l'obiettivo non è quello di agevolare gli operatori, ma di dare una cornice epistemologica agli accertamenti informatici. Del resto, non c'è inchiesta che non passi per il sequestro dei dispositivi del sospettato, si tratti di concussione[27], strage[28], spaccio[29]: tutti reati in cui l'apporto della tecnologia non è esattamente preponderante. È quindi necessario fissare dei requisiti minimi d'affidabilità che superino lo steccato del

[25] V. BARILI, *Accertamenti informatici*, in *Le indagini scientifiche nel procedimento penale*, a cura di Valli, Milano, 2013, 593 s.

[26] Su questo punto, la dottrina è compatta: v. LUPÁRIA, *La ratifica della convenzione* cybercrime *del Consiglio d'Europa – I profili processuali*, in *Dir. pen. proc.*, 2008, 719; TONINI, *Nuovi profili processuali del documento informatico*, in *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, a cura di De Cataldo Neuburger, Padova, 2010, 427, 431; NOVARIO, *Prove penali informatiche*, Torino, 2011, 15 s.; LUPÁRIA, Computer crimes *e procedimento penale*, in *Modelli differenziati d'accertamento*, a cura di Garuti, in *Trattato di procedura penale*, diretto da Spangher, vol. VII, t. 1, Torino, 2011, 370; DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 283 s.; BARILI, *Accertamenti informatici*, cit., 589; DI PAOLO (voce), *Prova informatica (diritto processuale penale)*, in *Enc. Dir. – Annali VI*, Milano, 2013, 737; TESTAGUZZA, Digital forensics, Padova, 2015, 35; CUOMO-GIORDANO, *Informatica e processo penale*, in *Proc. pen. giust.*, 2017, 716.

[27] Per un esempio tratto dalla cronaca recente v. *Sindaco di Mantova indagato, la procura: sms a sfondo sessuale per un anno*, in *www.repubblica.it*, 25 novembre 2017. Per accertare l'ipotesi di reato, «quella di cui agli articoli 56, 81 e 317 del codice penale», cellulare, pc e tablet dell'indagato sono stati sequestrati. Per il caso s'è poi richiesta l'archiviazione: a quanto hanno riportato le fonti di stampa, i messaggi su cui si basava l'accusa sarebbero stati manipolati dalla persona offesa.

[28] Noto in tutto il mondo è il caso della sparatoria di S. Bernardino, California: il 2 dicembre 2015 una coppia di coniugi armati di fucili e pistole aprì il fuoco in un centro per disabili uccidendo 14 persone. Sul sequestro del cellulare di uno degli attentatori s'è poi innestata una battaglia legale tra l'azienda produttrice e la polizia federale, che aveva chiesto all'azienda di programmare un grimaldello capace di superare il blocco del dispositivo; per una descrizione degli eventi e del dibattito che hanno suscitato, v. OLIVER, *Encryption*, in *Last Week Tonight*, HBO, 13 marzo 2016, in *www.youtube.com*.

[29] V. Cass. sez. IV, 28 giugno 2016, n. 40903, Grassi, in *Mass. Uff.*, n. 268227.

'crimine informatico' – ed è quello che la legge del 2008 ha cercato di fare, pur con strumenti troppo blandi.
Conservare l'originale e impedire alterazioni costituiscono infatti esigenze trasversali: se il materiale "vergine" andasse perso, non si potrebbero replicare le analisi; il metodo utilizzato e la sua conformità ai canoni tecnico-scientifici di riferimento resterebbero sommersi. Affiorerebbe invece il punto d'arrivo di procedure impossibili da falsificare, mettendo tutti i soggetti processuali di fronte al fatto compiuto; la difesa e gli eventuali periti non potrebbero svolgere daccapo gli opportuni accertamenti; il giudice non potrebbe giovarsi di un vero contraddittorio sul piano tecnico e si vedrebbe a quel punto costretto, più che alla valutazione d'un elemento, a un atto di fede[30]. Le regole dell'informatica vanno qui di pari passo con l'epistemologia del processo: se non si rispettano le prime, s'azzoppa la seconda[31].
L'attenzione alle esigenze investigative sembra invece aver oscurato il problema di metodo: la Corte ha probabilmente ragione nel sostenere che l'acquisizione di un testo è affare facile; non si tratta certo di rintracciare i *server* e gli amministratori di una pagina del *deep web*[32] ed esistono più mezzi con cui appropriarsi del *file*: basterebbe un ordinario copia-incolla o addirittura una stampa[33]. Il dato sarebbe comunque noto agl'inquirenti e versato in atti, indipendentemente dalla tecnica d'apprensione: però, se si procedesse così, fare una verifica successiva sull'autenticità del materiale sarebbe pratica-

[30] Insisteva sul punto, prima della riforma del 2008: LUPÁRIA, *La disciplina processuale e le garanzie investigative*, in Lupária-Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, 2007, 128; ripropone il pensiero PITTIRUTI, *Profili processuali della prova informatica*, in *'Incontri ravvicinati' con la prova penale*, a cura di Marafioti-Paolozzi, Torino, 2014, 50; dopo la riforma, v. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, 405 s.; LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in *Sistema penale e criminalità informatica*, a cura di Lupária, cit., 136.
Lo stesso discorso vale poi anche in altri frangenti: per una declinazione in materia di videoriprese, v. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove «incostituzionali»*, in *Cass. pen.*, 1999, 1193.
[31] Sulle interazioni e le tensioni tra le regole della scienza e quelle del processo, v. almeno: CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, 3530; DOMINIONI, *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in *Prova scientifica, ragionamento probatorio e decisione giudiziale*, a cura di Bertolino-Ubertis, Napoli, 2015, 37 s.; RENZETTI, *Prova scientifica nel processo penale: problemi e prospettive*, in *Riv. dir. proc.*, 2015, 399 s.; CATALANO, *Il metodo del controesame sul letto di Procuste. Le insidie e le sfide della prova scientifica*, in *Le erosioni silenziose del contraddittorio*, a cura di Negri-Orlandi, Torino, 2017, 151.
[32] Sulle complicazioni che questo genere d'accertamento può comportare, v. il documentario scritto e diretto da WINTER, *Deep web*, 2015, nel quale si ripercorrono le indagini e il processo che hanno portato alla condanna di Ross William Ulbricht, accusato d'essere il gestore di *Silk Road*, una pagina dalla quale era possibile acquistare ogni tipo di sostanza stupefacente.
[33] V. ad esempio Cass. sez. VI, 24 febbraio 2015, n. 24617, Rizzo, cit.

mente impossibile. Chi assicura che la "stampata" riproduca fedelmente il dato? Cosa garantisce che quel testo copiato non abbia subito variazioni? E se le ha subite, com'è possibile dimostrarlo?
Da un lato, quindi, bene hanno fatto le sezioni unite a ribadire che non c'è vincolo di legge sulle tecniche di copia: gli operatori hanno a disposizione un ventaglio che è bene dosare in base alle necessità; dall'altro, avrebbero fatto meglio a sottolineare che il contraddittorio sul piano tecnico resta un valore da garantire, qualunque sia lo strumento impiegato. Se si volesse fare a meno dell'immagine forense, si dovrebbe chiedere agli investigatori di documentare le operazioni in maniera meticolosa, tramite videoripresa o sistemi di *auditing*[34]. Questi accorgimenti permetterebbero infatti di limitare i rischi rendendo tracciabile ogni passaggio; si potrebbe così valutare il preciso impatto delle manovre compiute sul sistema[35]: la ripetibilità non sarà più assicurata, ma si potrebbe svolgere un controllo successivo sulla sostenibilità scientifica del procedimento seguito[36].

5. Casi e modi del sequestro di dati informatici.

Finita la digressione, si torna sulla strada principale: stabilito che i dati possono essere autonomamente sottoposti a sequestro, resta da capire quando si concreti l'atto e a quali condizioni sia ammissibile il riesame.
Volendo trarre conclusioni a fil di logica, il percorso sarebbe lineare: se il dato in quanto tale può essere appreso e se la copia impone un vincolo, ogni

[34] La tecnica è consigliata in generale per la documentazione delle analisi: v. CASEY, *Digital Evidence and Computer Crimes*, cit., 232; DANIELE, *La prova digitale nel processo penale*, cit., 298.
[35] Per una posizione sostenibile sulla tutela dell'originale, v. CASEY, *What does forensically sound really mean?,* in *Digital investigation*, 2007, vol. 4, 49 s.
[36] Tra l'altro, la ripetibilità o irripetibilità degli accertamenti informatici è questione da tempo dibattuta in dottrina: v. GUALTIERI, *Prova informatica e diritto di difesa*, in *Dir. pen. proc. – Dossier: La prova scientifica nel processo penale*, 2008, 73; RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, 337 s.; FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc.,* 2012, 373; DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche,* in *Cass. pen.,* 2012, 441; ID., *La prova digitale nel processo penale*, cit., 297-298; TESTAGUZZA, Digital forensics, cit., 46.
La giurisprudenza, ad ogni modo, è granitica nel qualificare le operazioni come accertamenti tecnici ripetibili, che saranno quindi effettuati senza che sia necessario l'avvertimento al difensore; v. Cass. sez. I, 25 febbraio 2009, n. 11503, in *Mass. Uff.*, n. 243495; Cass. sez. I, 26 febbraio 2009, n. 11863, Ammutinato, *ivi*, n. 243922; Cass. sez. I, 5 marzo 2009, n. 14511, Stabile Aversano, in *Cass. pen.*, 1520, con nota di LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*; Cass. sez. I, 30 aprile 2009, n. 23035, Corvino, in *Mass. Uff.*, n. 244454; Cass. sez. I, 9 marzo 2011, n. 17244 in *Cass. pen.*, 2012, 440; Cass. sez. II, 19 febbraio 2015, n. 8607, Apicella, in *Mass. Uff.*, n. 263797; Cass. sez. II, 4 giugno 2015, n. 24998, Scanu, *ivi*, n. 264286, *ivi*; Cass. sez. II, 1 luglio 2015, n. 29061, p.c. in Posanzini, *ivi*, n. 264572.

duplicazione dovrebbe costituire un sequestro, che potrebbe di conseguenza essere impugnato[37].

La soluzione della Corte è più sfumata e identifica tre ipotesi. La prima – del tutto pacifica – riguarda il vincolo sul dispositivo, che può essere sottoposto a riesame. Venendo ai dati, la cassazione mette a punto una divisione opaca: distingue infatti «il dato informatico in sé» da quello in cui la traccia informatica è «mero "recipiente" d'informazioni». Il primo tipo si distinguerebbe in quanto «riguarda il dato come cristallizzato nel "clone" identico all'originale e, perciò, da esso indistinguibile. Il dato-recipiente invece è appreso «in quanto rappresentativo di atti o fatti, dunque quale vero e proprio documento».

Alle due categorie si riconnettono trattamenti diversi: per il dato in sé, la riconsegna del supporto non fa venir meno il vincolo sulle informazioni; l'accesso al riesame sarà quindi garantito. Per i dati-documento, al contrario, la Corte ribadisce le conclusioni cui erano giunte le sezioni unite nel 2008: la restituzione della cosa tronca l'interesse a impugnare[38]. S'aggiunge però un passaggio significativo: nel caso in cui il documento «trasferisca il proprio valore anche sulla copia», sopravvive un interesse alla «disponibilità esclusiva del "patrimonio informativo"» capace di tenere aperta la porta del riesame: l'esistenza di un duplicato sarebbe infatti sufficiente a generare un pregiudizio.

Prima di soffermarci sui singoli snodi dell'argomentazione, vale la pena gettare uno sguardo al principio di diritto che la Corte ricava: «è ammissibile il ricorso per cassazione avverso l'ordinanza del tribunale del riesame di conferma del sequestro probatorio di un computer o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati ivi contenuti, sempre che sia dedotto l'interesse, concreto e attuale, alla esclusiva disponibilità dei dati». La massima non contiene che un frammento della sequenza logica che l'ha generata: stando ai motivi, infatti, la regola dovrebbe valere soltanto per ciò che può essere equiparato a un documento; per il resto non dovrebbe esser posto alcun onere rafforzato perché il riesame sia ammissibile[39]. Nella formulazione del principio, tuttavia, la differenza tra dato vero e

---

[37] A questa conclusione era giunta Cass. sez III, 21 settembre 2015, n. 38148, Cellino, cit.; avrebbe preferito un simile epilogo TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare:* revirement *delle sezioni unite*, in *www.penalecontemporaneo.it*, 11/2017, 172.

[38] Sottolinea la continuità RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in *Cass. pen.,* 2018, 132: «sarebbe erroneo affermare che [la pronuncia] opera un radicale *revirement* [...]; l'attuale arresto giurisprudenziale infatti ha preso in esame un aspetto che era stato trascurato in precedenza»; v. anche 142.

[39] La stessa giurisprudenza sembra essersene resa conto: una decisione successiva, infatti, ha accantonato la massima adoperando l'intero apparato argomentativo, v. Cass. sez. II, 31 ottobre 2017, n. 53810, Lo

proprio e dato-documento viene taciuta: del resto, la distinzione appare difficile da afferrare e riassumere. Cosa si ripartisce, poi, con questa differenza? Perché la *bit stream image* permette un accesso immediato al riesame mentre un altro metodo d'apprensione no?
La Corte scrive che, con questa tecnica, originale e copia sarebbero indistinguibili; le altre modalità di duplicazione, invece, non clonano: fanno qualcosa di meno, tanto che matrice e riproduzione conservano una rispettiva identità. Questa distanza qualitativa sembra essere il vero confine tra le due categorie di dato: in un caso si sequestra generando una seconda matrice; nell'altro invece si forma una semplice replica, che non pare in grado di rappresentare un vincolo[40].
L'assunto, tuttavia, è vero solo in parte: tutto è distinguibile sul piano naturalistico e, ai fini di determinati accertamenti, una *bit stream image* non sarà comunque in grado di sostituire l'originale. Alcune operazioni di recupero dati, per esempio, sfruttano la memoria fisica del dispositivo, che permette di risalire a ciò che è stato eliminato sul piano informatico[41]; un'operazione simile non potrebbe certo essere svolta sulla copia *bit* per *bit*, che riproduce di pari passo tutte le tracce digitali che il disco contiene, non quelle che non ospita più. Si tratta insomma di una tecnica molto precisa, ma l'affermazione per produrrebbe un duplicato indistinguibile non sembra essere del tutto accurata.
In verità, due piani distinti sembrano essere qui sovrapposti: il rilievo accordato all'immagine forense è infatti del tutto comprensibile quando si tratta di conservare un elemento ma, rispetto all'ubiquità del materiale informatico, la procedura sembra perdere la sua posizione privilegiata. Anche le altre modalità di replica creeranno una versione in più; cambierà il perimetro di quanto raccolto, i *bit* saranno rimescolati ma la ridondanza dell'informazione c'è comunque.

6. Il riesame: modi d'accesso ed efficacia del controllo.

Ambivalenze interpretative a parte, la pronuncia imprime una svolta: l'impugnazione ne esce indiscutibilmente estesa in ampiezza e fini. Accanto al diritto di proprietà, si accorda tutela anche all'esclusivo godimento del patrimonio informativo.

Castro, in *BancaDati24*.
[40] La Corte esclude infatti che a ogni copia corrisponda un sequestro.
[41] Si tratta delle celle sovrascritte: l'immagine forense copierà il contenuto attuale di quello spazio; per risalire a ciò che c'era in passato occorre tentare una ricostruzione che può essere svolta soltanto sul dispositivo coinvolto.

Ricapitoliamo: la domanda sarà ammessa nel caso sia vincolato il dispositivo, mentre per quanto riguarda i dati la soluzione è spaccata in due. Se è stata formata un'immagine forense, saremo davanti a un vincolo vero e proprio che merita d'essere sottoposto a una verifica; si seguiranno anche qui le regole di un normale riesame. Per le copie formate diversamente, invece, il discorso cambia: il sequestro – se mai eseguito – si considera spirato con la restituzione dei supporti e le sezioni unite hanno modulato di conseguenza il diritto d'impugnativa del privato. Per accedere al controllo del tribunale, occorre un interesse che giustifichi l'avvio di un incidente nonostante la misura sia già cessata[42]: in altre parole, bisognerà provare che il trattenimento della copia arreca comunque un pregiudizio. Se il vincolo fosse ancora in essere, un onere simile non troverebbe fondamento nel testo normativo che, dalla richiesta di riesame, non esige nemmeno i motivi.
Le sezioni unite si mostrano piuttosto rigide: non bastano generiche allegazioni; si dovrà infatti dimostrare la sussistenza di «un interesse concreto ed attuale, specifico ed oggettivamente valutabile sulla base di elementi univocamente indicativi della lesione di interessi primari conseguenti alla indisponibilità delle informazioni contenute nel documento»[43].
Parafrasando: perché l'impugnazione risulti ammissibile, occorre che sia compresso un interesse primario, cioè: la duplicazione deve mettere a rischio un diritto riconosciuto dalla legge. La Corte – attingendo a piene mani dai precedenti – presenta pure qualche esempio: certamente meritevoli di tutela sono il segreto professionale e la riservatezza. La lesione che si desidera rimossa deve poi risultare da elementi univoci grazie ai quali provare un interesse concreto, attuale, specifico e oggettivamente valutabile.

---

[42] Una soluzione analoga, basata su un dovere dimostrativo rafforzato rispetto all'interesse è già consolidata rispetto al riesame delle misure cautelari personali decadute: v. Cass. sez. VI, 24 novembre 2005, n. 14422, Riccardi, in *Mass. Uff.*, n. 234023; Cass. sez. VI, 15 novembre 2006, n. 9943, Campodonico, *ivi*, n. 235886; Cass. sez. VI, 16 aprile 2007, n. 27580, Romano, *ivi*, n. 237418; Cass. sez. VI, 16 ottobre 2007, n. 38855, Russo, *ivi*, n. 237658; Cass. sez. VI, 26 novembre 2007, n. 4222, Reinhaler, *ivi,* n. 238719; Cass. sez. VI, 6 dicembre 2007, n. 2210, Magazzu', *ivi,* n. 238632; Cass. sez. VI, 14 gennaio 2009, n. 3531, Gervasi, *ivi,* n. 242404; Cass. sez. VI, 14 gennaio 2009, n. 3528, Caruso, *ivi*, n. 242662. L'orientamento è poi stato adottato anche dalle sezioni unite, con la sentenza del 16 dicembre 2010, n. 7931, Testini, *ivi*, n. 249002; e ribadito dalle sezioni semplici: v. Cass. sez. I, 12 gennaio 2017, n. 19649, Cei, *ivi*, n. 270009. Lo stesso principio è stato affermato rispetto all'impugnazione dell'ordinanza che convalida l'arresto al quale non segue l'applicazione di una misura cautelare: Cass. sez. VI, 13 febbraio 2009, n. 13522, Calia, *ivi*, n. 244141; Cass. sez. V, 31 gennaio 2017, n. 9167, Fanu, *ivi*, n. 269038. Per le evoluzioni della giurisprudenza, nella cornice del requisito della concretezza dell'interesse, v. CARNEVALE, *L'interesse ad impugnare nel procedimento penale*, Torino, 2012, 214 s.

[43] Là dove la Corte fa riferimento all'indisponibilità del dato, s'intende la non esclusiva disponibilità. La copia, infatti, rende il materiale sempre disponibile a entrambe le parti; ciò che viene meno è il controllo sull'informazione.

Se sgraniamo questo piccolo rosario d'aggettivi, troveremo due grandi classici: la concretezza e l'attualità, a significare rispettivamente che l'impugnazione deve poter rimuovere il pregiudizio lamentato e che il *vulnus* deve sussistere al momento della richiesta: non basta una mera potenzialità[44]. L'interesse deve inoltre essere 'specifico': dovrà saldarsi cioè a un'interferenza ben individuata e non a istanze vaghe.

Qualche dubbio in più suscita l'ultima delle caratteristiche elencate, secondo cui l'interesse deve essere 'oggettivamente valutabile'. Ora, tutto sta a intendersi: se significa che il pregiudizio deve essere riconoscibile dall'esterno, anche al di fuori della prospettiva personalissima di chi ha subito l'atto, si sta dicendo una cosa valida in assoluto. Ciascuno può infatti avere una ragione per dare impulso ulteriore a qualunque procedimento, ma non è detto che l'ordinamento debba farsi carico di ogni desiderio: si pensi alla sentenza d'assoluzione totalmente liberatoria che propone una ricostruzione dei fatti che l'imputato – pur prosciolto – contesta; dal suo punto di vista la correzione di questo o quel dettaglio potrebbe avere un'importanza vitale, ma l'esigenza non basta al sistema per avviare un ulteriore grado di giudizio[45]. Se il parametro che la Corte ha specificato dovesse essere letto in questa accezione, si tratterebbe quasi di una ridondanza: non si designerebbe un interesse particolarmente qualificato; si ribadirebbe soltanto una delle sue caratteristiche strutturali.

Non mancano però suggestioni differenti, assai più restrittive: lo stesso precedente che questa decisione sposa, per esempio, sembrava alludere a requisiti di matrice economica[46]. Il riesame, in quella cornice, era ammesso per le informazioni «il cui valore consiste nella riservatezza del dato», dalla cui duplicazione scaturiva di per sé «una perdita valutabile»; in questa direzione andavano anche gli esempi proposti: un piano industriale, un progetto, un dato segreto, il nome di una fonte[47]. La pronuncia ragionava quasi in termini di diritti di privativa per come intesi nel settore della proprietà intellettuale: la co-

[44] Per una compiuta argomentazione delle definizioni qui accolte, v. CARNEVALE, *L'interesse ad impugnare nel procedimento penale*, cit., 173 e 231.

[45] Per ulteriori esempi e una problematizzazione più ampia, v. CARNEVALE, *L'interesse ad impugnare nel procedimento penale*, cit., 55, 91 e 155 s.

[46] Si tratta di Cass. sez. VI, 24 febbraio 2015, n. 24617, Rizzo, cit.; sul rapporto tra le due decisioni si soffermano MARI, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione dei dati*, in *Cass. pen.*, 2017, 4316; TODARO, *Restituzione di bene sequestrato*, cit., 165; RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, cit., 139.

[47] Sull'aspetto si concentra COSTANZI, *Perquisizione e sequestro informatico*, cit., 281.

pia interrompe l'esclusivo godimento dell'informazione e ne rende impossibile il controllo – quindi, anche lo sfruttamento economico.
La seconda interpretazione sarebbe però troppo severa, specie se si vuole dare alla *privacy* una tutela effettiva: se tra atti di un'indagine per bancarotta si serbassero anche le fotografie dell'indagato con l'amante – magari gelosamente custodite nel computer aziendale e duplicate insieme alla contabilità – la perdita economica per l'impugnante sarebbe pari a zero; l'intrusione nella sua vita privata sarebbe però innegabile e, per di più, non si potrebbe nemmeno giustificare sul piano dell'accertamento: nel nostro esempio, il materiale sembrerebbe del tutto irrilevante.
Quello della riservatezza, più in generale, sembra essere un tasto dolente dell'assetto: da qualunque lato lo si giri, questo pezzo di *puzzle* non sembra proprio volersi incastrare, specie nel caso dell'immagine forense. Il controllo del riesame, infatti, insisterà più che altro sulla legittimità del sequestro: se rispetta i presupposti normativi, verrà confermato; diversamente, il materiale sarà restituito o distrutto.
La tecnica, del resto, sembra difficile da censurare alla luce del principio di proporzionalità come invece vorrebbe la Corte. Con la copia immagine, infatti, si prenderà sempre più materiale di quello che serve: la memoria è duplicata integralmente per essere esaminata in un secondo momento, con tutto il tempo e le precauzioni necessarie alla buona riuscita dell'operazione[48]. Insomma, prima si sequestra tutto e poi si perquisisce, in un rovesciamento che miete vittime illustri, a partire dal principio di pertinenza[49]. A giustificare il prelievo eccessivo, tuttavia, ci pensa la legge: abbiamo visto che la *bit stream image* è la procedura più sicura per quanto riguarda la conservazione dell'originale, e la sua tutela è posta dal codice come una priorità. Si potrà cassare un sequestro perché è stato eseguito seguendo alla lettera il dettato normativo? La necessità della tecnica rispetto al caso concreto potrà essere valutata a indagine in corso, prim'ancora che l'analisi sia terminata? Nei tempi contingentati del riesame, nemmeno gli inquirenti saranno probabilmente riusciti a lavorare su tutto il materiale: potrebbero essere in perfetta buona

[48] V. BARILI, *Accertamenti informatici*, cit., 593: il «prima acquisisci, poi seleziona e analizza» è «un consolidato "mantra" della *computer forensics*»; KERR, *Searches and Seizures in a Digital World,* in *Harward Law Review*, 2005, vol. 119, 547.; ID., *Fourth Amendment Seizures of Computer Data*, in *Yale Law Journal*, 2010, vol. 119, 714; LOGLI, *Sequestro probatorio di un* personal computer*. Misure* ad explorandum *e tutela della corrispondenza elettronica*, in *Cass. pen.,* 2008, 2955.
[49] Sul punto, v. in particolare CAMON, *La fase che "non conta e non pesa": indagini governate dalla legge?*, in *Legge e potere nel processo penale*, Padova, 2017, 111-112.

fede nell'utilizzare uno strumento che, col senno di poi, si rivelerà del tutto eccessivo; si potrà valutare negativamente il loro scrupolo?
Un controllo puntuale a tutela della *privacy*, del pari, sembra impraticabile: i dispositivi sono infatti miniere d'informazioni sempre più capienti; per individuare la vena utile – specie se è stata nascosta[50] – si dovrà scavare tra parecchio materiale di risulta: il tribunale non potrà di certo rovistare tra decine di *gigabyte*; non rispettando le cadenze temporali stabilite.
In più, anche se fosse riconosciuta una violazione, il rimedio della restituzione selettiva del materiale potrebbe non essere il migliore, specie in una fase tanto precoce dell'indagine: l'analisi di quanto raccolto sarà sicuramente ancora incompleta e a estromettere anche un solo file verrebbe meno la corrispondenza del duplicato all'originale.
Consapevole delle difficoltà, la dottrina ha elaborato diverse proposte che mirano direttamente alla selezione del materiale prelevato, in analogia a quanto accade per le intercettazioni telefoniche. Tutte le opinioni si ricollegano infatti al modello dell'udienza stralcio, da svolgere secondo una prima tesi in incidente probatorio; la prova sarebbe acquisita il prima possibile e il materiale irrilevante sarebbe tempestivamente restituito o distrutto[51]. L'opzione, tuttavia, non sembra del tutto funzionale: aprire un incidente probatorio per ogni analisi informatica sarebbe un aggravio notevole e non sempre necessario. L'attività potrebbe poi mettere a repentaglio l'indagine: si rischierebbe d'offrire uno spaccato importante dell'inchiesta ben prima della sua conclusione.
Tutto sommato, sembra preferibile la voce che s'è limitata a suggerire l'estensione dell'udienza stralcio[52], ipotesi che ha peraltro avuto una flebile eco pure in giurisprudenza[53]: si raggiungerebbe così un equilibrio migliore tra

[50] Per esempio, mediante l'uso della steganografia: occulta la presenza stessa di un contenuto (mentre la crittografia punta a renderlo incomprensibile a chiunque non abbia la chiave); è possibile nascondere informazioni dentro un'immagine, o in un *pixel* del fotogramma di un filmato. Lo stratagemma è stato utilizzato da diverse organizzazioni terroristiche per far circolare i propri piani d'azione; sul punto v. CHOUDHARY, *Image Steganography and Global Terrorism*, in *International Journal of Scientific & Engineering Research*, 2012, vol. 3, f. 7, consultabile alla pagina *www.ijser.org*; WANG-WANG, *Cyber warfare: steganography vs. steganalysis*, in *Communications of the ACM*, 2004, vol. 47, f. 10, 76 s., consultabile alla pagina *www.researchgate.net*.

[51] IOVENE, *Perquisizione e sequestro di computer: un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, 1616.

[52] L'idea è espressa da: CARNEVALE, *Copia e restituzione di documenti informatici sequestrati*, cit., 481; LUPÁRIA, Computer crimes *e procedimento penale*, cit., 375; SCHENA, *Ancora sul sequestro di materiale informatico*, cit., 306.

[53] Cass. sez. V, 27 ottobre 2016, n. 25527, in *DeJure*, che richiama addirittura due rimedi diversi: s'invoca per prima «l'applicazione in via analogica del rimedio previsto in caso di intercettazioni telefoniche, circa la selezione delle informazioni irrilevanti»; si cita poi l'art. 254 comma 3 c.p.p., che impone

le esigenze in gioco creando una sede garantita, tale da consentire la scelta del materiale in contraddittorio. In teoria il rimedio calzerebbe a pennello, ma si cadrebbe su un istituto affossato dalla prassi là dove la legge l'aveva previsto[54].
Bisognerebbe insomma mettere a punto un istituto snello, impossibile da liquidare come un appesantimento inutile e che consenta allo stesso tempo una protezione efficace della *privacy*.
Lo stesso accesso alla tutela andrebbe poi ripensato anche alla luce delle modalità d'archiviazione dei dati: i dispositivi sono infatti sincronizzati quasi sempre con un *cloud*; le forze dell'ordine potranno ottenere una copia dei contenuti rivolgendosi direttamente ai *provider*[55].
In tali casi, l'interferenza dell'autorità con il supporto è inesistente: la richiesta è inoltrata al fornitore del servizio di *storage*, non alla singola persona. Eppure dal punto di vista della riservatezza le coordinate del discorso non cambiano di molto: una copia delle informazioni sarebbe versata in atti e, molto probabilmente, agli elementi rilevanti si mescolerebbe una gran quantità di materiale inutile. Il quadro, semmai, si complica: non essendo il destinatario del provvedimento, il soggetto non è nemmeno al corrente del prelievo[56] e,

---

la restituzione delle «carte e [degli] altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile».

[54] Per l'analisi del fenomeno e per un quadro dei contrappesi man mano adottati dagli uffici, v. CABIALE, *Il superamento dell'udienza di stralcio: prassi "deviante" o opportunità teorica?*, in *Dir. pen. proc.*, 2014, 109; GIORDANO, *Il Consiglio Superiore della Magistratura sulle buone prassi in materia di intercettazioni: prime considerazioni*, in *www.penalecontemporaneo.it*, 11 ottobre 2016; CAPRIOLI, *La procedura di selezione e stralcio delle comunicazioni intercettate nelle linee-guida della Procura della Repubblica di Torino*, in *Arch. n. proc. pen.*, 2016, 553 s.; CAMON, *Il diritto alla privacy di fronte alle intercettazioni: le circolari delle Procure ispirano la riforma Orlando*, in *questa Rivista.*, 2017, 646 s. Il fenomeno è pure esaminato nella prospettiva di una sistematica svalutazione del principio di legalità in materia processuale da NEGRI, *Splendori e miserie della legalità processuale*, in *Legge e potere nel processo penale*, Padova, 2017, 78. Sulle modifiche alla procedura di selezione, v. CAMON, *Primi appunti sul nuovo procedimento d'acquisizione dei risultati delle intercettazioni*, in corso di pubblicazione.

[55] Su come il *cloud* stia cambiando i rapporti tra utente e contenuto, v. IRION, *Your digital home is no longer your castle: how cloud computing transforms the (legal) relationship between individuals and their personal records*, in *International Journal of Law and Information Technology*, 2015, vol. 23, 348 s.
Occorre tener conto del fatto che la capacità di collaborazione dei fornitori di servizi dipende anche dalla tecnologia che decidono di adottare: dopo le rivelazioni di Edward Snowden, per esempio, s'è assistito a un generalizzato passaggio alla crittografia *end-to-end*, che consente ai soli membri d'una conversazione di visualizzare un messaggio in chiaro; per il gestore, la comunicazione rimarrà cifrata, e quindi non potrà fornirla alle autorità in un formato intellegibile. Per una descrizione della tecnologia e la sua diffusione dopo lo scandalo NSA, v. ERMOSHINA-MUSIANI-HALPIN, *End-to-End Encrypted Messaging Protocols: An Overview*, in *Internet Science: third international conference, INSCI 2016, Florence, Italy, September 12-14, 2016: proceedings*, a cura di Bagnoli-Satsiou-Stavrakakis-Nesi-Pacini-Welp-Tiropanis-DiFranzo, Cham, 2016, 244 ss.

[56] Alcuni *provider*, come Amazon, Google e Apple, si riservano il diritto d'avvisare l'utente prima della

pure se ne fosse informato e proponesse gravame, sarebbe ancora più difficile ammettere l'impugnazione; nessuno ha mai interrotto il possesso sulla cosa e lo stesso interessato permette di regola al *provider* d'accedere ai dati, affinché possa verificare il rispetto dei termini di servizio; l'utente si trova insomma in uno stato di terzietà rispetto al suo stesso patrimonio informativo.

Inoltre, non si tratta nemmeno di sequestri in piena regola, ma piuttosto di richieste accondiscese dai fornitori del servizio: essi hanno ormai linee guida talmente dettagliate da assomigliare a procedure parallele, tanto da imporre alla prassi determinati standard[57]; se una domanda presenta i requisiti che l'azienda ritiene necessari, verrà soddisfatta e le informazioni saranno consegnate.

Un meccanismo di selezione capace di mediare tra *privacy* ed esigenze d'indagine sarebbe quindi da estendere anche a queste ipotesi, oggi non contemplate. La loro consistenza numerica non è irrilevante, ed è probabilmente destinata a crescere insieme all'uso dei *cloud*[58]: secondo i rapporti sulla trasparenza di Microsoft, Apple, Google e Facebook sono state inoltrate dalle autorità italiane quasi 40.000 richieste per oltre 65.000 *account* e dispositivi nel periodo che va dal 2013 al primo semestre del 2017[59]. Una risposta organica non può non tener conto di questa realtà diffusa, dando anche al proprietario dei dati qualche mezzo d'interlocuzione.

---

eventuale *disclosure*, a meno che non sia vietato da un ordine del tribunale o dalla legge.

[57] Specie dopo lo scandalo NSA, sono molte le aziende che pubblicizzano un atteggiamento ostile verso le richieste degl'inquirenti. Tra le più perentorie c'è Amazon, che dice di lottare affinché il IV Emendamento sia esteso alla privacy in via legislativa; intanto, per cedere le informazioni esige un mandato del giudice e non un semplice ordine del procuratore ritenendo che questo sia lo standard idoneo: «we also advocate in Congress to modernize outdated privacy laws to require law enforcement to obtain a search warrant from a court to get the content of customer communications. That's the appropriate standard, and it's the standard we follow»: SCHIMDT, *Privacy and Data Security*, in *www.aws.amazon.com*. Amazon Web Services è il principale attore nel mercato del *cloud*, totalizzando il 47,1% degl'incassi di settore: v. COLES, *AWS vs Azure vs Google Cloud Market Share 2017. Overview of Cloud Market in 2017 and Beyond*, 13 luglio 2017, in *www.skyhighnetworks.com*.

[58] Sulle dimensioni di mercato del *cloud* e le sue proiezioni di crescita a tre anni, v. *Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017*, 22 febbraio 2017, in *www.gardner.com*.

Il modo di procedere, comunque, non è vincolato: si potrà sempre prediligere il sequestro tradizionale del dispositivo, che contiene i dati presenti nella memoria e costituisce un punto d'accesso agli spazi di *storage* prediletti dall'utente: v. Cass. sez. IV, 28 giugno 2016, n. 40903, Grassi, cit.

[59] Per la precisione: 39.357 richieste per 65.584 *account* e dispositivi. Il rapporto di Microsoft è disponibile presso: *www.microsoft.com*; quello di Apple presso: *www.apple.com*; quello di Google all'indirizzo: *www.transparencyreport.google.com*; quello di Facebook si trova alla pagina: *www.transparency.facebook.com*. I dati forniti da Apple comprendono tanto le richieste sui dati degli *account*, quanto quelle sui dati dei dispositivi (per esempio: il numero di serie) e sui dati di natura finanziaria.

7. Oltre il digitale.

Al termine del percorso, resta una domanda: qualcosa è cambiato anche rispetto alla carta? La decisione s'è infatti concentrata sull'informatica, ma anche il contenuto di un foglioè informazione e può essere duplicato[60]. Che fare, dunque, nel caso in cui sia lui ad essere replicato?

Il regime della *bit stream image*, qui, è fuori gioco: nemmeno la stampa a colori ad alta definizione sembra esserne un equivalente logico; il prelievo d'informazione non sarà quindi considerato alla stregua di un sequestro, né si potrà accedere direttamente al sistema delle impugnazioni.

Al contrario, le conclusioni che la Corte ha raggiunto per tutti gli altri casi sembrano valere anche per l'analogico: troverà infatti applicazione l'art. 258 c.p.p. che si occupa di documenti sequestrati, siano o non siano digitali. Dimostrando la sopravvivenza di un interesse, dunque, si dovrebbe poter accedere al riesame anche se il materiale duplicato non appartiene al dominio dei dati informatici.

A questo punto, però, sarebbe forse stato meglio tenere unite le due categorie: non solo si sarebbero affrontate due incognite al prezzo di una, ma si sarebbe messo a fuoco il tema con maggior chiarezza. Il problema di fondo è infatti rimasto inevaso, anzi, ha guadagnato forza: se si afferma che l'informazione è sequestrabile in quanto tale, si rischia di sdoganare una categoria concettualmente incontenibile. Tutto ciò che si fa nel corso di un procedimento è finalizzato a scoprire e accumulare dati rilevanti: se si ammettesse un'equivalenza secca tra l'acquisizione di informazioni e il sequestro, ogni atto d'indagine potrebbe essere descritto come tale.

Un tentativo di delimitazione più equilibrato arriva dalla dottrina d'oltreoceano, che affronta da tempo problemi analoghi[61]: per circoscrivere l'atto non s'è lavorato attorno agli strumenti coinvolti, ma al significato dell'apprensione. Aiutiamoci con qualche esempio: se la polizia fotografasse

---

[60] Gran parte della giurisprudenza che ha portato all'arresto del 2008 riguardava infatti materiale cartaceo, non informatico; anche in seguito, poi, non s'è perso il riferimento a entrambe le categorie: v. Cass. sez. VI, 24 febbraio 2015, Rizzo, cit.

[61] Del tema si occupa in particolare KERR, *Fourth Amendment Seizures of Computer Data*, cit., 700 s.; l'Autore s'era già espresso sul tema in ID., *Searches and Seizures in a Digital World,* cit., giungendo a conclusioni in parte differenti.

Anche negli Stati Uniti la tecnologia mette in dubbio i confini di categorie già collaudate e in particolare, per quanto qui interessa, del IV Emendamento. Per una panoramica sul tema v. GRAY, *The Fourth Amendment in an age of surveillance*, Cambridge, 2017, in particolare 68 s.; KERR, *The Fourth Amendment and the Global Internet*, in *Stanford Law Review*, 2015, 285 s.; SCHULHOFER, *More essential than ever: the Fourth Amendment in the twenty-first century*, Oxford, 2012.

un poster appeso alla parete, ne starebbe sequestrando il contenuto? E se duplicasse una cartella che contiene decine e decine di *file*? In entrambi i casi, infatti, si finisce per preservare e acquisire agli atti un'informazione, ma con una differenza. Nella prima ipotesi, l'agente aveva già avuto modo di vedere il dato che ha poi appreso; l'aveva innanzi tutto osservato e selezionato, prim'ancora di "congelarlo". La seconda istanza, invece, appare del tutto differente: con ogni probabilità, chi procede alla copia non verifica il contenuto di ogni elemento anzi, di norma la replica servirà proprio a svolgere questa operazione in un secondo momento.

Nel primo scenario, insomma, il contenuto è già noto e la duplicazione non aggiunge nulla di nuovo al patrimonio informativo di cui gl'investigatori dispongono: la riproduzione servirà semplicemente ad aiutare la memoria di chi per primo ha conosciuto il dato. Nel secondo, invece, si preleva materiale senza sapere in anticipo cosa si troverà: non c'è stata osservazione umana preventiva e sarà proprio la replica ad allargare l'insieme delle informazioni disponibili. Se in un caso la conoscenza precede la copia, nell'altro il duplicato è funzionale alla scoperta investigativa: la prima situazione non costituirà quindi un vincolo vero e proprio – la copia del dato varrà come aiuto alla memoria dell'agente – nella seconda, invece, si tratterà di un sequestro a pieno titolo[62].

La tesi ha senz'altro il pregio dell'universalità: sarebbe infatti in grado di offrire un confine omogeneo tanto per la carta quanto per il materiale informatico, indicando una sistemazione tutto sommato univoca. Il discrimine che traccia, tuttavia, sembra facilmente aggirabile: basterebbe infatti guardare prima e copiare dopo per schivare l'ostacolo, trasformando il prelievo in documentazione di quanto visto.

La tesi sembra quindi ancorare i diritti di chi subisce l'atto a un comportamento arbitrario di chi lo compie; per di più, la differenza è appesa a un filo sottilissimo: la soggettiva, personale conoscenza del dato.

Bisognerebbe invece ragionare su un limite oggettivo, che tenga conto di tutti i soggetti coinvolti e che non s'inerpichi in insostenibili definizioni di 'informazione'[63]: l'obiettivo, infatti, non è cingere con la medesima disciplina l'acquisizione di qualunque 'dato', ma regolare una possibilità tecnica – la duplicazione – che consente di sdoppiare un insieme finito di cose. Non tutto è, infatti, replicabile. Pensiamo per esempio al caso di uno stabile abusivo foto-

[62] KERR, *Fourth Amendment Seizures of Computer Data*, cit., 715 s.

[63] La nozione ha suscitato un vivace dibattito filosofico efficacemente riepilogato da FLORIDI, *Information*, in *The Blackwell Guide to the Philosophy of Computing and Information*, a cura di Id., Oxford, 2004, 40 s.

grafato: lo scatto catturerà certamente un dato – per esempio, il luogo in cui si trova la costruzione – ma immortalare l'immobile non significa duplicarlo.
Un primo limite al 'sequestro d'informazione' potrebbe forse stare nello speciale legame tra cosa e dato, limitandone l'ambito a quelle sole ipotesi in cui l'oggetto è significativo in virtù del suo contenuto: in ultima analisi, l'area interessata si potrebbe grossomodo sovrapporre a quella dei documenti.
Probabilmente, ciò non basterebbe a far sorgere un sequestro: se così fosse, la disciplina dell'istituto si dovrebbe applicare alla replica di ogni singolo elemento, anche se disponibile al pubblico o volontariamente consegnato agli investigatori. Sembrerebbe invece più saggio guardare al luogo in cui le informazioni sono conservate: se si trattasse d'uno spazio riservato – fisico o virtuale che sia – la loro duplicazione costituirebbe un vincolo imposto dall'autorità giudiziaria, la cui opportunità dovrebbe poter essere proficuamente messa in discussione[64].

8. Conclusioni.

Tirando le somme, si tratta d'una sentenza tanto autorevole quanto vaga nelle definizioni, che tenta di giostrarsi tra principi dirompenti e governo dei loro effetti. Il risultato non è ottimale, e proprio questo pare essere il tratto più istruttivo: declamazioni tradite, concetti abbozzati, rimedi imperfetti sembrano il sintomo d'un certo malessere. La Corte s'è trovata tra le mani un tema colossale senza disporre di strumenti abbastanza affilati per dominarlo: l'unico appoggio normativo è l'innesto del 2008, che il legislatore ha eseguito allargando a realtà diverse gl'istituti preesistenti[65]. Gli otri vecchi non hanno però retto il vino nuovo: il livello di garanzie non s'è normalizzato, non s'è inciso o quasi su una prassi disordinata ai limiti dell'indecifrabile[66] ma

[64] Non rileverebbe la natura dell'informazione, ma la natura della modalità con cui è conservata. Prendiamo a esempio un articolo di giornale: di per sé non è niente di riservato; se fosse però stato scaricato e fosse custodito in formato digitale nel computer del sospettato, la sua duplicazione implicherebbe comunque un sequestro. Pur a fini diversi, traccia una simile distinzione anche SIGNORATO, *Le indagini penali informatiche*, cit., 84, ad avviso della quale «per verificare se l'investigazione debba o meno conformarsi alla tutela della privacy, non sembra rilevare il carattere riservato dell'informazione, ma il carattere riservato del luogo della rete in cui essa è contenuta».

[65] La scelta ha suscitato parecchie critiche da parte della dottrina: LUPÁRIA, *La ratifica della convenzione* cybercrime *del Consiglio d'Europa*, cit., 719; MONTI, *La nuova disciplina del sequestro informatico*, cit., 202; FASOLIN, *La copia di dati informatici*, cit., 372; MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico,* in *Cass. pen.*, 2012, 704; DI PAOLO (voce), *Prova informatica*, cit., 761.

[66] Pronosticava il risultato sin dall'entrata in vigore della legge MONTI, *La nuova disciplina del sequestro informatico*, cit., 217. Sulla prospettiva che il difensore può avere rispetto a questo dedalo v. MORELLI, *Profili problematici del diritto di partecipazione del difensore nella fase delle indagini preliminari: dalle dichiarazioni dell'indagato alla prova informatica*, in *Nuovi orizzonti del diritto alla difesa tecnica*, a cura

l'identità e la funzione degli strumenti d'indagine s'è fatta ambigua; lo stesso impaccio nel dare un nome alle cose ne è spia inequivoca.
L'identico rischio, speculare, si ripropone sul fronte delle tutele: in fondo si ragiona attorno all'estensione di uno strumento – il riesame – che già sappiamo essere un ripiego, inadatto com'è al ruolo che gli si vuole assegnare. Certo, qualcosa è pur sempre meglio di niente, ma le disposizioni non si possono allargare o restringere come se nulla fosse: sono piuttosto un prodotto di sartoria, cucito addosso a realtà precise. L'abito non vestirà allo stesso modo un manichino diverso: occorrerà prendere le misure daccapo, individuando i diritti da proteggere e chiedendosi fino a che punto s'è disposti a sacrificarli in nome dell'accertamento penale.
Nel nostro caso, tuttavia, proprio questa operazione è complicata da una duplice difficoltà: da un lato la tecnica è in costante evoluzione e, forgiata una categoria, spunta l'arnese che la rende obsoleta; dall'altro, il valore che fa spesso da contrappeso – la riservatezza – non ha forma né colore, è una sorta di gigante ma senza spina dorsale: «si riconosce l'esigenza, si ammette la sociale dignità dell'interesse; non di meno si nega tutela, perché mancherebbe la norma»[67]. Gli appigli più solidi si collocano sull'orizzonte delle Carte sovrannazionali e la dottrina nostrana, per ricavare vincoli stringenti, ha accarezzato sempre la stessa idea – allargare l'esistente a situazioni diverse, pure sul piano costituzionale[68].
Se questa è la diagnosi, occorre una terapia che agisca su più fronti, e non ci si può aspettare che sia la sola giurisprudenza a cercare di metterla a punto, anzi: di tutti i formanti, è quello che più di ogni altro deve lavorare con un testo normativo che, al momento, costringe a incoerenze testarde. Occorrerebbe dunque fare un passo indietro e chiarire bene quali esigenze salvaguardare e come bilanciarle con le altre, assegnando anche alla riservatezza uno statuto tale da proteggerla senza farne un idolo: la normativa di dettaglio e la giuri-

---

di Negri-Renon, Torino, 2017, 27 s.

[67] GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Scritti giuridici in memoria di Piero Calamandrei*, vol. V, Padova, 1958, 438.

[68] Ad esempio, è nato così il 'domicilio informatico' come categoria dottrinale che ha il preciso scopo di estendere la garanzia della doppia riserva – di legge e di giurisdizione – anche a interventi che non coinvolgano un luogo fisico; la categoria, però, non sembra adatta allo scopo: anche se fosse riconosciuta e impiegata con questa intenzione, sarebbe limitata a una manciata di situazioni lasciando tutto il resto allo scoperto. Basti pensare ai dati bancari, o alle informazioni stivate in un *cloud*: sarebbero tutte conservate in *server* difficili da ricondurre alla nozione di domicilio, per quanto la si possa estendere. Per un esempio di questo modo d'argomentare v. VENTURINI, *Il sequestro probatorio e fornitori di servizi informatici*, cit., 114 s.; per una descrizione della categoria e un accenno ai problemi che potrebbe porre, v. SIGNORATO, *Le indagini penali informatiche*, cit., 51 s.

sprudenza troverebbero un binario posato, un principio alla luce del quale intuire regole[69].

Qualunque equilibrio – sia affermato dalla legge in via generale e astratta; sia deciso dal giudice di un singolo caso – non può però che passare da una conoscenza profonda degli elementi fattuali coinvolti, tra cui i mezzi tecnici impiegati. Se così non fosse, anche la soluzione giuridica più elegante risulterebbe goffa non appena toccato il suolo, inadatta alla realtà come gli albatros di Baudelaire.

LAURA BARTOLI

[69] Un esempio in questo senso arriva dalla Germania, dove la Corte costituzionale federale ha coniato il diritto all'autodeterminazione informativa che ha plasmato di conseguenza il sistema processuale: sul tema v. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, 1153 s.; nella dottrina tedesca, v. MAISCH, *Informationelle Selbstbestimmung in Netzwerken*, Berlin, 2015, in particolare 56 s.; BULL-GIESEN-KÜHLING-LEUTHEUSSER-SCHNARRENBERGE-LEWINSKI-ROBRECHT-SCHAAR-SCHRAMM-SCHULZKI-HADDOUTI-SEEMANN-SPIECKER-STINNER-TREPTE, *Zukunft der informationellen Selbstbestimmung*, Berlin, 2016. Sui principi come norme in grado di produrre regole, v. LUZZATI, *Principi e principi. La genericità nel diritto*, Torino, 2012.