I nuovi ambiti dell'inutilizzabilità probatoria nel sistema multilivello dei diritti. Riflessioni a margine del disegno di legge in materia di sequestri di dati informatici

Michela Siracusa
(Tirocinante *ex* art. 73 d.l. n. 69/2013 presso la Suprema Corte di Cassazione)

Abstract
L'impiego delle moderne tecnologie investigative, che consentono di acquisire un'estesa mole di informazioni personali, ha determinato un'inevitabile trasformazione del concetto di *privacy*, oggi consacrato tra le garanzie inviolabili della persona sia dalla *Grund-Norm* che dalle fonti europee. A fronte di attività acquisitive illegittime si impone la riflessione circa la possibilità di ampliare, gli ambiti del divieto di utilizzabilità probatoria, sì da conferire adeguata ed effettiva tutela al diritto alla riservatezza informatica.

The use of modern investigative technologies, which allow the acquisition of a large amount of personal information, has led to an inevitable transformation of the concept of privacy, which is today consecrated, by the Grund-Norm and European sources, among the inviolable guarantees of the person. This leads us to reflect on the possibility of expanding, in the face of illegitimate acquisition activities, the areas of exclusionary rules, to give adequate and effective protection to the right to privacy.

Sommario: **1**. Il "nuovo" art. 254-*ter*: tutto cambia perché nulla cambi! **2**. La tutela della *privacy* sotto l'occhio vigile delle Corti europee **3**. Vecchie e nuove aporie di sistema **4**. Spunti di riflessione in chiave comparatistica **5.** Inutilizzabilità a tutela della *privacy*: quali sviluppi (futuribili)?

1. Il nuovo art. 254-*ter* c.p.p.: tutto cambia perché nulla cambi!

È al vaglio del Legislatore la discussione sulla riforma dei moderni strumenti investigativi. Il tentativo è quello di riequilibrare le indebite intrusioni nella *privacy* dei singoli, provocate da un'attività di indagine che si trasforma in una pesca a strascico di informazioni personali.

Una premessa è d'obbligo: la *data retention*[1], intesa quale agglomerato di tecniche che, sfruttando le nuove tecnologie di rete, consentono di acquisire una grossa mole di dati, non solo tollera, ma esige la predeterminazione di apposite procedure di conservazione, trattamento e accesso[2], corredandole di adeguate sanzioni processuali.

Da qui la prospettiva di riforma avente ad oggetto la materia dei sequestri informatici, attraverso cui è possibile captare ciò che costituisce il "D.N.A." virtuale della persona. Con l'articolo 254-*ter* c.p.p.[3] si è voluto scansionare l'attività di sequestro informatico.

Il procedimento prevede la richiesta, da parte del pubblico ministero al giudice per le indagini preliminari, di essere autorizzato al sequestro, fermo restando, secondo una prassi già consolidata in materia intercettativa, la possibilità di procedere a prescindere dall'autorizzazione nei casi di urgenza, richiedendo la convalida in un momento successivo.

Effettuato il sequestro, disposto dal pubblico ministero o dalla polizia giudiziaria su delega della pubblica accusa, viene disposta la copia su idoneo supporto informatico atto a preservare l'autenticità e l'immodificabilità del dato: si vuole garantire all'indagato una piena

---

[1] S. Marcolini, R. Flor, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale,* Torino, 2022; R. Flor, *Data retention e giustizia penale in Italia, in* C. Parodi, V. Sellaroli (a cura di), *Diritto penale dell'informatica,* Milano, 2020, 683 ss.; G. Formici, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino, 2021.

[2] S. Marcolini, *La disciplina processuale italiana sulla data retention*, in S. Marcolini, R. Flor (a cura di), *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale,* Torino, 2022, 45.

[3] D.D.L. depositato in Senato il 9 maggio 2023. Cfr., A.S. n. 690, in www.senato.it.

corrispondenza tra quanto viene estratto e quanto viene sequestrato al momento dell'attività perquisitiva.
Il trattenimento dei dati informatici può avvenire anche mediante la tecnica c.d. *bit a bit* [4], con cui si consegna all'autorità inquirente la copia conforme dell'originale, sì da preservare la non adulterazione dello stesso[5]. L'esigenza da salvaguardare è la non modificabilità del dato e l'immediatezza dell'acquisizione: invero, a conclusione di tali operazioni, da svolgere in un breve arco temporale e, comunque, non oltre le settantadue ore dal momento in cui il sequestro è convalidato, il contenitore sarà restituito al suo legittimo proprietario.
Permane, tuttavia, la conservazione indistinta di ciò che è all'interno del contenitore, sebbene sia stato prevista – quale *pseudo* garanzia – l'istituzione di un archivio presso le Procure che, alla stregua di quanto disposto per le intercettazioni a norma dell'art. 269 comma 1 c.p.p., consentirà di trattenere le informazioni apprese.
Infine, concluse le operazioni acquisitive, l'interessato potrà chiedere la distruzione di quanto risulti estraneo o irrilevante a fini investigativi[6].
Per quanto concerne i presupposti legittimanti il sequestro dei contenitori e della copia dei contenuti ivi allocati sono necessari i gravi indizi di colpevolezza per la generalità dei reati, a fronte di sufficienti indizi di colpevolezza laddove si tratti di delitti attinenti alla criminalità organizzata. Si ripropone, quindi, la logica del doppio binario, mutuata dall'analoga disciplina in materia di intercettazioni.
Tuttavia, in una nota di indirizzo governativo, divulgata dalla Procura di Trento ai Procuratori della Repubblica, già si rinveniva l'invito a non effettuare un sequestro esplorativo *omnibus*, essendo doveroso selezionare soltanto elementi rilevanti a fini accertativi[7] secondo i criteri di adeguatezza e di proporzionalità, previsti per le misure cautelari personali.
Nella proposta di legge, invero, si è cercato di sedare il dibattito sui nuovi ambiti di tutela della *privacy*, offrendo ai consociati una scansione procedimentale che culmina nell'eventuale, e a richiesta

[4] S. Fasolin, *La copia dei dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc.,* 2012, 372 ss.

[5] G. Costabile, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008,* in *Ciberspazio e dir.*, 2010, 500 ss.

[6] M. Martorana, *Privacy e indagini, presentato un DDL sul sequestro di strumenti elettronici*, 2023, in www.altalex.com.

[7] L. Filippi, *Sequestro dispositivi elettronici: nota della Procura Generale di Trento, in Dir. pen. proc.*, 2021, 2 ss.

di parte, distruzione del materiale non rilevante. Il rimedio individuato è anche peggiore del male, dal momento che si ancora la disciplina del sequestro ad una procedimentalizzazione rigorosa e puntuale, scansionando i passaggi necessari per l'acquisizione dei dati e trascurando l'esigenza di individuare una specifica sanzione processuale a fronte di attività *contra legem* e lesive di garanzie inviolabili.

2. La tutela della privacy sotto l'occhio vigile delle Corti europee

Il discorso muta in ambito europeo dove al centro dell'attenzione vi è proprio la necessità di un rimedio efficace ed effettivo a tutela del diritto alla riservatezza[8].

Ed è stata la Corte europea dei diritti dell'uomo a delineare i nuovi confini di tutela della *privacy*, precisando che la raccolta e la conservazione dei dati costituisce un'ingerenza nella vita intima della persona[9]. D'altra parte l'art. 8 C.E.D.U. prevede che *«ogni persona ha diritto al rispetto della vita privata e familiare, del suo domicilio e della sua corrispondenza»*[10]. Ne discende che il potere pubblico può limitare le prerogative individuali soltanto qualora occorra tutelare interessi superiori e, comunque, assolutamente eccezionali[11]. Con specifico riguardo alle perquisizioni e ai sequestri informatici, la Corte di Stra-

---

[8] Per un approfondimento circa l'articolata vicenda della *data retention* nel contesto eurounitario, cfr. R. Flor, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in *Dir. pen. cont.*, 2014, 2*;* P. Di Stefano, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale: solo un obbligo per il legislatore o una nuova regola processuale?,* in *Cass. pen.,* 2021, 2556 ss.; G. Leo, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *Sist. Pen.,* 2021; G. Spangher, *I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali,* in www.giustiziainsieme.it, 3 maggio 2021; G. Formici, *op. cit.*, *passim*; Id., *L'incerto futuro della data retention saga nell'Unione europea: osservazioni a partire dalla sentenza H.K. v. Prokuratuur,* in *SIDI Blog,* 2021; o, ancora, O. Pollicino, M. Bassini, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. pen. cont.*, 2017, 5 ss.

[9] Corte EDU, sent. 16 febbraio 2000, *Amann c. Svizzera.*

[10] S. Bartole, B. Conforti, G. Raimondi, *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fomentali*, 2001, 312 ss.; G. Ubertis, *Principi di procedura penale europea. Le regole del giusto processo,* 1999, 125 ss.

[11] Corte EDU, sent. 28 gennaio 2003, *Peck c. Regno Unito.*

sburgo ha fornito delle direttive per evitare che le ingerenze nell'intimità della persona siano autoritarie.
Procedendo con la tecnica *case by case*, i giudici della Corte EDU hanno ritenuto violato l'art. 8, comma 2, C.E.D.U., a causa delle modalità con cui la polizia giudiziaria, nell'ambito di indagini relative al traffico illegale di prodotti farmaceutici, aveva proceduto a raccogliere dati informatici presso l'ufficio del difensore, atteso che tali modalità avevano reso la ricerca ed il sequestro di dati sproporzionate rispetto allo scopo investigativo perseguito, vanificando le prerogative individuali della persona[12].
In altra occasione la Corte EDU ha ribadito che la ricerca di dati informatici si concretizza in un'indebita intrusione nella vita privata altrui, comportando la violazione dell'art. 8, comma 2, C.E.D.U., qualora il mandato di perquisizione, eccessivamente generico, consenta un sequestro *omnibus* sproporzionato. A ciò si aggiunga la mancanza sia di un mezzo per contestare la legittimità del mandato e della sua esecuzione, sia di garanzie volte ad evitare che l'intero contenuto sequestrato possa essere indistintamente visionato[13].
Evidente è, dunque, la preoccupazione, per i giudici di Strasburgo, di assicurare un'adeguata e rafforzata tutela alla *privacy*[14]. Il formante giurisprudenziale della Corte EDU avvalora la riflessione circa la possibilità di estendere i margini dell'inutilizzabilità a tutela del diritto alla riservatezza.
Se è pacifico che, in un contesto di pluralismo delle fonti, si imponga l'interpretazione ragionevolmente conforme al diritto EDU, ne consegue che, anche in materia di acquisizione di dati digitali, i giudici interni non possono non conformarsi ai *dicta* provenienti da Strasburgo.
Legittimo è, a tal punto, chiedersi quale sia la sorte del dato informatico appreso, qualora la Corte EDU riconosca l'eccessiva ingerenza nella vita privata del singolo e, quindi, se sia possibile ragionare in termini di inutilizzabilità convenzionale, cui il giudice domestico dovrebbe essere ragionevolmente vincolato, pur mancando una previsione legislativa interna.
La risposta al quesito richiede, preliminarmente, l'identificazione

---

[12] Corte EDU, Sez. IV, sent. 16 ottobre 2007, *Wieser e Bicos Beteillingungen GMBH c. Austria*, in *Ind. pen.,* 2008, 765 ss., con nota di F.S. Cassibba, *Le perquisizioni presso lo studio del difensore alla luce della Convenzione europea dei diritti dell'uomo, ivi.*
[13] Corte EDU, Sez. V, sent. 22 agosto 2008, *Ilya Stefanov c. Bulgaria.*
[14] Corte EDU, sent. 3 luglio 2012, *Robathin c. Austria.*

delle condizioni in presenza delle quali la Corte europea abbia riconosciuto il *vulnus* alla riservatezza altrui. Al riguardo si segnala l'assenza di una disposizione sul punto, la sproporzionalità e non necessità a fini investigativi dell'ingerenza; la mancanza di un provvedimento autorizzatorio emesso da un giudice o sul quale quest'ultimo abbia esplicato un controllo successivo; alla natura bagatellare del reato; l'assenza di adeguati mezzi di impugnazione per contestare i provvedimenti di perquisizione e sequestro informatici. Infine, vanno verificate le ripercussioni negative sulla propria reputazione e sulla propria dignità[15].

Non sempre, come specifica la Corte europea nei suoi *dicta*, la lesione della riservatezza implica iniquità processuale, giacché la lesione del diritto al *giusto processo* va riscontrata in presenza di una violazione delle garanzie difensive[16].

È chiaro che le situazioni individuate dalla Corte EDU, quali integrative di una lesione dell'art. 8 CEDU, hanno una portata flessibile e sono connotate da ampia discrezionalità. Sicchè non potrebbe parlarsi, almeno stando ad una lettura rigorosa della giurisprudenza convenzionale, di un'inutilizzabilità degli atti acquisiti, avendo tali requisiti al più il ruolo di criteri legali di valutazione, cui il giudice italiano deve orientarsi, sebbene non sia rigidamente vincolato ad essi.

E se si condivide l'assunto della Corte EDU nella parte in cui si riconosce una violazione dell'art. 8 C.E.D.U. ogni qualvolta l'ingerenza sia assolutamente sproporzionata; altrettanto non può ritenersi per la parte in cui non si pronuncia sulla sanzione processuale rispetto ad atti intrusivi e né riconosce una compressione delle garanzie del *giusto processo*. Ciò premesso, sarebbe auspicabile che il pregiudizio sia riscontrato anche qualora gli atti che ne costituiscono fondamento siano stati assunti con modalità lesive di diritti inviolabili della persona.

Se il sistema multilivello dei diritti, che oggi connota la post-modernità, impone di massimizzare la tutela di diritti inviolabili, l'espressione "*giusto processo*" andrebbe necessariamente intesa come il luogo in cui le prerogative inviolabili della persona trovano massima realizzazione: in questi termini, l'intrusione indebita nella vita inti-

---

[15] Corte EDU, sent. 3 luglio 2012, *Robathin c. Austria*, cit., cfr. pure S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. e proc. pen.*, 2012, 601 ss.

[16] M. Daniele, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale*, in *Cass. pen.*, 2013, 1, 367 ss.

ma dell'Io darebbe vita ad un processo iniquo, giacché sarebbero compromesse le prerogative inviolabili di uno Stato di diritto su cui si fonda l'equo processo garantito dalla Legge.
Il bisogno di conferire effettiva protezione al diritto alla riservatezza si avverte anche nelle pronunce della Corte di giustizia, ove i giudici, sino dalle più recenti pronunce, sono ben consapevoli che un'acquisizione generalizzata di dati informatici, oltre ad essere misura sproporzionata rispetto agli scopi investigativi, leda il diritto di ciascuno a vedere tutelata la propria intimità[17]. Non sfugge però l'atteggiamento cauto della Corte di giustizia che pur manifestando l'esigenza di introdurre una garanzia processuale rimette poi il compito di tipizzazione al legislatore interno.
A tal scopo, si segnala la pronuncia[18] che, nell'autunno del 2021, ha determinato la modifica dell'art. 132 cod. *privacy*[19]. In questa occasione, la Corte di giustizia ha riproposto affermazioni di principio, di cui già si aveva contezza nelle precedenti pronunce euro-unitarie[20], osservando che l'acquisizione di dati informatici non possa essere sproporzionata, né essere rivolta all'accertamento di qualsiasi reato. Da ultimo, la Corte non ha mancato di ribadire che, ferma restando l'indubbia utilità investigativa della *data retention*, l'apprensione *omnibus* non è tollerabile in una civiltà democratica[21], salvo che si tratti di reati di particolare gravità e allarme sociale, rispetto ai quali si potrebbe giustificare, sia pure in via eccezionale, una captazione generica.
Da qui la responsabilizzazione degli Stati membri nell'arduo compito di individuare soluzioni rispettose dei diritti inviolabili. Tuttavia,

---

[17] F. Iovene, *Data retention tra passato e futuro. Ma quale presente*?, in Cass. pen., 2014, 4274 ss.; E. Colombo, *Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE,* in *Cass. pen.,* 2014, 2705 ss.

[18] Corte U.E., Grande sezione, 2 marzo 2021, *Prokuratuus*, C-746/18. In dottrina, R. Flor, *La giurisprudenza della Corte di Giustizia dell'UE sulla data retention,* in R. Flor, S. Marcolini (a cura di), *Dalla data retention alle indagini ad alto contenuto tecnologico, cit.,* 27 ss.

[19] M. Pisati, *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali,* in *Proc. pen. giust.,* 2020, 4, 963 ss.; S. Signorato, N*ovità in tema di data retention. La riformulazione dell'art. 132 codice privacy da parte del D.lgs. 10 agosto 2018 n.101,* in *Dir. pen. cont.*,2018, 11, 153 ss; E. Lorenzetto, U*tilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto, passando per la copia,* in *Cass. pen.,* 4, 2010, 1522 ss.

[20] Si riprendono i principi esplicitati nella sentenza "*Quadrature du Net*": cfr. Corte U.E., Grande Sezione, 6 ottobre 2020, C-511/18, C- 512/18 e C-520/18.

[21] Corte. U.E., 5 aprile 2022, C-140/20. In dottrina, E. Resta, *Dalla conservazione generalizzata a quella mirata e rapida: la Corte di giustizia ridelinea i contorni della data retention*, in www.giustiziainsieme.it, 2022.

è notorio che, pur volgendo lo sguardo ad ordinamenti diversi dal nostro, si continua ad affannare nel tentativo di ricostruire, in modo aderente ai principi euro-unitari, l'intricata e scivolosa materia, legittimando derive autoritarie e inquisitorie in nome dell'efficientismo, non compatibili con il tessuto assiologico di uno Stato costituzionale di diritto.
Questo *excursus* sui limiti della *data retention* in ambito convenzionale ed euro-unitario conferma la problematicità di tutelare, adeguatamente, il diritto alla *privacy*. Infatti, né la giurisprudenza convenzionale, né la Corte euro-unitaria sembrano propense a riconoscere, in modo netto ed incisivo, l'inutilizzabilità degli atti acquisiti in violazione dell'art. 8 C.E.D.U. e dell'art. 7 della Carta di Nizza, preferendo scaricare sul Legislatore la responsabilità di prevedere adeguate garanzie processuali, compendiate da altrettanto idonee sanzioni.

3. Vecchie e nuove aporie di sistema

La *querelle* in ordine alla necessità di presidi garantistici in materia di sequestri informatici è risalente nel tempo[22]. A conferma di ciò, basti pensare al lungo dibattito che ha interessato dottrina e giurisprudenza[23] in ordine alla natura giuridica di tali attività, rispetto al quale non si è ancora offerta una risposta univoca e pacifica[24].
Se l'intervento nel diritto penale sostanziale non si è fatto attendere[25], altrettanto non può ritenersi per quanto concerne la materia processuale, pur emergendo da subito che il punto nevralgico fosse l'individuazione di vincoli alla tecnica acquisitiva[26], rinvenendosi già i primi accenni, da parte della dottrina, al bisogno di limitare l'estendibilità del sequestro[27].

---

[22] G. Braghò, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. Luparia (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008 n.48),* 2009, 181 ss.

[23] Cass. pen., Sez. I, sent. 16 febbraio 2007, Pomarici, con nota di A. Logli, *Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica,* in *Cass. pen.,* 2008, 2955 ss.

[24] P. Tonini, *Documento informatico e giusto processo,* in *Dir. pen. proc.*, 2009, 402.

[25] Cfr. Legge n.547 del 1993, attuativa della direttiva n.91/250/CEE.

[26] F. M. Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.,* 2012, 2, 700 ss.

[27] A. Monti, *La nuova disciplina del sequestro informatico*, in L. Luparia (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Conven-*

Non si è dato, però, il giusto peso al problema di prevenire un sequestro *omnibus*[28], prevedendo, come si sarebbe auspicato, rimedi processuali.
Soltanto con l'entrata in vigore della legge attuativa della Convenzione di Budapest sul *cybercrime*[29], si è introdotto il "nuovo" art. 254-*bis* c.p.p., volto a dettare regole in materia di sequestro di dati, informazioni e programmi informatici, nell'intento di definire la questione in ordine alla natura tipica o atipica del sequestro probatorio.
È pacifico che le nozioni di "conformità all'originale", "immodificabilità", "assenza di alterazione"[30], che si ritrovano nell'art. 254-*bis* c.p.p., offrono un quadro di garanzie volte a preservare la genuinità [31] del dato appreso[32]: esse rappresentano la estrinsecazione processuale delle *best practice*, indicate a livello europeo.
Sicuramente svolge una funzione essenziale di trasparenza l'obbligatorietà della motivazione nel caso di sequestro informatico, avendo il pubblico ministero l'obbligo di indicare come procederà all'acquisizione di dati informatici per fare in modo che la genuinità delle informazioni venga preservata. La motivazione deve essere articolata e dettagliata, non essendo ammessi, considerati i diritti in gioco, provvedimenti generici, rivolti, cioè, all'esplorazione di tutto ciò che è contenuto nel supporto informatico[33]. Tuttavia, non è precluso a priori l'eventuale sequestro probatorio *omnibus*: l'autorità giudiziaria

---

zione di Budapest sul cybercrime (l. 18 marzo 2008 n.48), 2009, 197 ss.

[28] A. Monti, *No ai sequestri indiscriminati di computer, nota a Trib. Brescia, sez. II, 9 ottobre 2006*, in *Dir. internet,* 2007, 269.

[29] S. Aterno, *Modifiche al titolo III del libro terzo del codice di procedura penale,* in G. Corasaniti, G. Corrias Lucente (a cura di), *Cybercrime, responsabilità degli enti, prova digitale. Commento alla legge 18 marzo 2008, n. 48,* Padova, 2009, 195; G. Ziccardi, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche,* in L. Lupària (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime,* Milano, 2009, 165 ss.

[30] P. Tonini, *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, in *Corr. giur.,* 2012, 3, 432; M. Torre, *Sequestro probatorio - Il riesame del sequestro probatorio di documenti informatici*, in *Giur. it.,* 2019, 6, 1437.

[31] V. Denti, *La tutela della privacy e dell'esclusività del patrimonio informativo alla prova del sequestro dei dati informatici,* in *Resp. civ. prev.,* 2016, 4, 1304.

[32] A. Monti, *La nuova disciplina del sequestro informatico*, in L. Luparia (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008 n.48)*, 2009, 208; G. Braghò, *Le indagini informatiche tra esigenze di accertamento e garanzie di difesa,* in *Dir. dell'informazione e dell'informatica,* 2005, 3, 517 ss.

[33] A. Monti, *op. cit.,* 268 ss.

può procedervi a condizione che disponga immediatamente la restituzione del supporto, oltre che della copia dei dati appresi, secondo quanto affermato di recente dalla giurisprudenza di legittimità[34].
Il sequestro probatorio può avvenire sia attraverso la materiale apprensione del dispositivo "contenitore", sia attraverso la creazione di una copia clone dei dati digitali ivi contenuti: in ogni caso, oggetto del sequestro è il dato, l'informazione dematerializzata[35], non già il contenitore, e seppure quest'ultimo venga restituito, ciò non toglie che l'interessato possa essere pregiudicato dall'indistinta conservazione delle proprie informazioni.
La consapevolezza che la lesione permanga anche a fronte della restituzione del contenitore assume rilievo in punto di rimedi azionabili: il problema concerne esclusivamente la possibilità di disporre, in modo, esclusivo della copia ottenuta mediante l'acquisizione del dato, non già della facoltà, pacifica, di esperire il riesame avverso il decreto di sequestro del contenitore[36].
A tal proposito, si sono offerte differenti letture interpretative, rispetto alle quali sono intervenute le Sezioni unite[37], cercando di ricostruire l'equilibrio tra diritto alla esclusiva disponibilità del patrimonio informatico ed esigenze investigative[38].
In origine, la tesi sostenuta dalla giurisprudenza prevalente escludeva che si potesse estendere la facoltà di riesame nel caso di già avvenuto dissequestro del contenitore, venendo meno l'interesse a proporre gravame[39]. Minoritaria era, invece, l'opinione contraria, secondo cui sussisterebbe un diritto alla restituzione della copia indipendente dall'avvenuta restituzione del supporto informatico.
A fronte di un contrasto ermeneutico[40], le Sezioni unite sono inter-

[34] Cass. pen., Sez. VI, 2 dicembre 2020, n.34265, con nota di C. Fontani, *Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi,* in *Dir. pen. e processo,* 2022, 2, 237 ss.

[35] P. Tonini, *L'evoluzione delle categorie tradizionali: il documento informatico,* in A. Cadoppi, S. Canestrari, A. Manna , M. Papa (a cura di), *Cybercrime*, Milano, 2019, 1307 ss.

[36] M. Torre, *op. cit*., 1437.

[37] Cass., Sez. un., 20 luglio 2017, n.40963, *Andreucci*, *Rv.* 270497-01.

[38] G. Todaro, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*, in *Dir. pen. cont.,* 2017, 1, 157 ss.

[39] Cass. pen., Sez. II, 23 marzo 1999, n. 1480, *Ferrari*, Rv. n. 213306; Cass. pen., Sez. IV, 13 dicembre 2001, n. 26506, p.m. in *Mattei*; Cass. pen., Sez. II, 20 dicembre 2005, n. 3598, *Canzano*, Rv. n. 233335; Cass. pen., Sez. II, 14 giugno 2007, n. 24958, Cal, Rv. n. 236759; Cass. pen., Sez. II, 5 luglio 2007, n. 32881, *Sandalj*, Rv. n. 237763.

[40] Secondo un primo indirizzo, la facoltà di riesame andrebbe riconosciuta soltanto in caso di perdita valutabile del bene, dovendo essere altrimenti negata: cfr. Cass. pen.,

venute e, recependo la distinzione tra il dato informatico cristallizzato nella copia-clone e quello che assume le vesti di mero documento[41], riconoscono sempre l'accesso al riesame nel primo caso; nel secondo caso, il riesame è precluso in caso di restituzione del supporto, salvo che sopravviva un interesse alla esclusiva disponibilità del patrimonio informativo[42].
In altri termini, in quest'ultima ipotesi, la conservazione del doppione deve pregiudicare un interesse primario, tra cui, indubbiamente, la riservatezza o il segreto professionale.
Resta, in ogni caso, in piedi la ricorribilità per cassazione nel caso di conferma, in sede di riesame, del provvedimento di sequestro probatorio, sempre che venga dedotto l'interesse concreto alla esclusiva disponibilità del patrimonio informativo.
Nonostante l'intervento apparentemente *tranchant* del Supremo Consesso, permanevano talune incertezze ermeneutiche: non si comprendeva né come bisognasse dimostrare di avere interesse all'esclusiva disponibilità del patrimonio informativo, né in cosa consistesse tale interesse e, infine, se fosse riconducibile al concetto di *privacy*[43].
Successivamente è stato chiarito che è sufficiente che l'interesse si ricavi dagli atti processuali, così legittimando il passaggio ad una presunzione di interesse ad impugnare nel caso in cui si fosse proceduto all'acquisizione dei dati contenuti nei supporti informatici[44].

Sez. VI, 24 febbraio 2015, n.24617, *Rizzo*, in *Giur. it.*, 2015, 1503 ss., con nota di S. Lorusso, *Sequestro probatorio e tutela del segreto giornalistico*, in *Dir. pen. cont.,* 2015. In dottrina v, *ex multis*, F. Cerqua, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica,* in *Arch. n. proc. pen.,* 2016, 269 ss.; C. Costanzi, *Perquisizione e sequestro informatico. L'interesse al riesame nel caso di estrazione di copie e restituzione dell'originale*, in *Cass. pen.,* 2016, 286 ss. Diversamente, si estendeva la facoltà di riesame per il solo fatto che permanesse il vincolo di indisponibilità sui dati: cfr. Cass. pen., Sez. III, 21 settembre 2015, n. 38148, *Cellino*, in *Dir. pen. proc.,* 2016, 508 ss., con nota di V. Zamperini, *Impugnabilità del sequestro probatorio di dati informatici.*

[41] L. Bartoli, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen.,* 2018, 1, 2 ss.

[42] A. Chelo Manchia, *Sequestro probatorio di computers: un provvedimento superato dalla tecnologia?,* in *Cass. pen.,* 2005, 1634 s.; A. Monti, *No ai sequestri indiscriminati di computer*, in *Dir. internet*, 2007, 268 s.; Id., *La nuova disciplina del sequestro informatico*, in L. Luparia (a cura di), *Sistema penale e criminalità informatica, cit.,* Milano, 198-199; S. Venturini, *Il sequestro probatorio e fornitori di servizi informatici,* in L. Lupária (a cura di), *Internet provider e giustizia penale*, Milano, 2012, 116 s.

[43] G. Todaro, cit., 160.

[44] Cass. pen., Sez. VI, 3 febbraio 2022, n.18502, con nota di G. Cascone, *La disponibilità*

In merito alla possibilità di ricondurre l'interesse al concetto di riservatezza, non sono mancate prospettive più restrittive che sottolineano la matrice economica di tale interesse, ragionando, *mutatis mutandis*, in termini di diritti di privativa tipici della proprietà intellettuale[45]. In buona sostanza, la copia forense interromperebbe lo sfruttamento economico del dato immateriale, rendendone impossibile il pieno controllo.

A ben vedere, volendo conferire tutela effettiva, nel sistema multilivello di diritti, al concetto di *privacy*, è innegabile l'intrusione nella vita intima altrui provocata dall'acquisizione di dati in copia conforme, specie se non tutti potenzialmente utili alle indagini[46]. Si può ritenere che l'esclusiva disponibilità del patrimonio informativo sottintenda il concetto di *privacy*, oggi ricondotto nell'alveo dei diritti inviolabili a tutela della dignità della persona[47].

A ben vedere l'estensione della facoltà di riesame genera tensioni con il principio di tassatività dei mezzi di impugnazione: sennonché, ammettere una tale facoltà "in bianco" potrebbe avallare un'interpretazione *praeter* o, addirittura, *contra legem*[48]. Per quanto tale interpretazione sia maggiormente in linea con gli orientamenti della Corte di giustizia, essa si pone in contrasto con i principi fondanti lo Stato costituzionale di diritto e, in particolare, con il principio di parità trattamentale ispirato al concetto di ragionevolezza, giacché si ammetterebbe il riesame nel caso di sequestro del contenitore e non nell'ipotesi di acquisizione dei dati ivi contenuti. Stando così le cose, è pacifico che il criterio dell'interpretazione conforme[49] alle

---

esclusiva del dato informatico: una nuova pronuncia della Corte di Cassazione a tutela del "patrimonio informativo" in *Cass. pen.*, 2023, 2, 555 ss.

[45] S. Carnevale, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.,* 2009, 480. In questi termini, in giurisprudenza, si veda Cass. pen., Sez. VI, 24 febbraio 2015, n. 24617. In dottrina, cfr. A. Mari, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione dei dati*, in *Cass. pen.,* 2017, 4316; G. Todaro, *op. cit.*, 165; P. Rivello, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in *Arch. pen.,* 2018, 1, 139.

[46] A. Logli, *op. cit.,* 955.

[47] G. Todaro, *op. cit.,* 169.

[48] S. Signorato, *Le indagini digitali*, *cit.,* 229.

[49] M. Luciani, voce *Interpretazione conforme a Costituzione*, in *Enc. dir. Treccani*, 392; D. Pulitanò, *Diritto penale e tecniche interpretative: l'interpretazione conforme a Costituzione e il ruolo creativo del giudice,* in L. Pellizzone (a cura di), *Principio di legalità penale e diritto costituzionale. Problematiche attuali*, Torino, 2017, 65 ss.; V. Manes, *Il giudice nel labirinto. Profili delle intersezioni tra diritto penale e fonti sovranazionali,* Roma, 2012, 48.

fonti sovranazionali non possa squalificare diritti inviolabili che trovano censimento, prima di tutto, nel testo costituzionale[50]: per tali ragioni, andrebbe, a nostro avviso, avallata un'interpretazione che, prima di essere aderente ai testi convenzionali, sia conforme a Costituzione.

Sarebbe auspicabile che gli interpreti, almeno *de iure condito*, consentano alla parte interessata di proporre riesame per essere rimesso nella piena disponibilità del suo patrimonio informativo: l'ostacolo posto dal principio di tassatività potrebbe così essere ragionevolmente superato attraverso l'opera esegetica, antidoto più potente alla fluidità del post-moderno.

Se una simile prospettiva può essere *prima facie* rassicurante in punto di effettiva tutela delle prerogative inviolabili, non deve però essere passivamente accolta, atteso che la compressione subita dalla tutela della riservatezza non è integralmente neutralizzata attraverso l'esperibilità del riesame, considerati i tempi contingentati della procedura che, verosimilmente, non consentiranno agli organi investigativi di analizzare e selezionare il materiale acquisito per restituire quanto non pertinente ai fini delle indagini.

Di talché, se elevato è lo *standard* di tutela del diritto alla riservatezza, imposto dal sistema etero integrato, non ci si può più accontentare di un rimedio che, apparentemente, soddisfi la piena disponibilità del patrimonio informativo ma, a ben vedere, non riesce a conferire piena ed effettiva tutela alla *privacy*.

In definitiva, nonostante i presidi garantistici desumibili, da un lato, dalla lettura delle norme (rigorosa pertinenzialità al reato, necessaria istruttoria giustificativa, adeguata motivazione[51]) e, dall'altro, da un'interpretazione costituzionalmente orientata, si registra ancora una costante aporia nel sistema[52], soprattutto per quanto concerne la controllabilità dell'attività captativa nella prospettiva di una successiva inutilizzabilità processuale dei dati acquisiti illegittimamente. Si tratta di antinomie non superate dai recenti tentativi di riforma, in cui il Legislatore ha scelto di prediligere espressamente le esigenze

---

[50] M. Ruotolo, *L'interpretazione conforme a Costituzione torna a casa?*, in *Consulta online*, 2019, 3, 589 ss.

[51] C. Melzi D'Eril, *Tra « fondali » da investigare e «scandaglio probatorio»; qualche riflessione per evitare che il sequestro diventi una «pesca a strascico»,* in *Cass. pen.*, 2013, 1, 75 ss.

[52] E. Lorenzetto, *Le attività urgenti di investigazione informatica e telematica*, in L. Luparia (a cura di)*, Sistema penale e criminalità informatica, cit.,* 139-141; L. Luparia, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. La legge 18 marzo 2008, n. 48,* in *Dir. pen. proc.*, 2008, 6, 718.

di accertamento investigativo a scapito di una piena protezione del diritto alla *privacy*, glissando sulla necessità di riconoscere il divieto di utilizzo degli atti acquisiti in violazione di tali presidi. Una scelta, quest'ultima, che rivela ancor più la sua incoerenza sistematica se si guarda alle "vicine" discipline in materia di inutilizzabilità degli atti acquisiti all'esito di attività intercettativa illegittima (art. 291 c.p.p.) oppure con riguardo ai documenti assunti *contra legem (*art. 240 c.p.p.) o, ancora, per quanto concerne l'apprensione dei dati dai tabulati telefonici o telematici, rispetto ai quali il Legislatore, cercando di recepire i *dicta* provenienti dalla Corte di Lussemburgo sulla nota vicenda della *data retention*, ha ammesso il divieto di utilizzazione dei dati acquisiti in violazione delle nuove previsioni (art. 132 comma 3-*bis* cod. *privacy*)[53].

Pur mutando le coordinate di riferimento e pur evolvendosi la *digital evidence,* il problema di estendere la sanzionabilità processuale a tutela della *privacy* torna ciclicamente, non trovando compiute soluzioni.

4. Spunti di riflessione in chiave comparatistica

in molteplici ordinamenti si riscontra la comune tendenza di procedimentalizzare la disciplina dell'apprensione dei dati informatici: ci si riferisce, in particolare, all'esperienza processuale spagnola, ove, attraverso la modifica degli artt. 350, 351, 352 del *Codigo Procesal Penal*, si legittima la perquisizione *online* di un sistema informatico e la conseguente captazione dei dati, purché ciò avvenga nel rispetto di determinate modalità. A tal fine, è necessaria la previa autorizzazione da parte del *Tribunal de Garantías*, dovendo essere l'esigenza investigativa sollecitata per un reato di particolare gravità[54], oltre che una motivazione rafforzata che dia conto dell'idoneità, doverosità e proporzionalità dell'attività apprensiva. Pesa, tuttavia, l'assenza di qualsiasi indicazione, come si registra anche nel nostro ordinamento, circa l'eventuale non utilizzabilità degli atti acquisiti in spregio alle modalità sopra indicate.

In prospettiva più sbilanciata verso la tutela di istanze securitarie, si

---

[53] S. Marcolini*, La disciplina processuale italiana sulla data retention*, in S. Marcolini, R. Flor (a cura di), *Dalla data retention alle indagini ad alto contenuto tecnologico, cit.,* Torino, 2022; R. Flor, *Data retention, Accertamento e repressione dei reati*, in S. Marcolini, R. Flor (a cura di), *Dalla data retention alle indagini ad alto contenuto tecnologico, cit.,* Torino, 2022,108 ss.

[54] F. Iovene, *op. cit.*

può ricordare l'intervento della Corte costituzionale belga, chiamata a pronunciarsi in ordine alla legittimità della disciplina che prevedeva la raccolta generalizzata di dati personali nell'ambito delle telecomunicazioni[55]: in questa occasione, è stata sollevata questione pregiudiziale comunitaria alla Corte di giustizia[56], dubitando della compatibilità della disciplina con il diritto comunitario.
La Corte euro-unitaria ha ribadito che la conservazione e acquisizione dei dati debba essere mirata soltanto per ciò che risulti assolutamente pertinente ai fini delle indagini, salvo nei casi in cui debba essere fronteggiata una seria e grave minaccia all'ordine pubblico dello Stato, giacché, in tali evenienze, l'acquisizione può avere portata generalizzata.
Ciò posto, perplime l'intervento dei giudici del Belgio i quali, nuovamente aditi, hanno precisato che il diritto alla *privacy* non abbia portata assoluta, essendo consentite quelle ingerenze nella vita privata altrui espressamente previste dalla legge oltre che espressione di un ragionevole bilanciamento tra diversi interessi in gioco[57].
Peraltro, la tendenza a conferire priorità alle istanze securitarie piuttosto che alla tutela di prerogative individuali si evince anche da un recente progetto di legge, presentato nel 2021, definito «*une solution pour concilier vie privée et sécurite*»: viene promossa non solo una forma organica di conservazione dei dati ma anche una particolare tutela alla sicurezza nazionale e all'ordine pubblico attraverso tempi prolungati di conservazione[58].
Non è un caso che l'Autorità Garante belga per la tutela della *privacy* abbia richiesto un vaglio preventivo di conformità ai diritti inviolabili comunitari, manifestando dubbi in ordine al necessario rispetto della proporzionalità nella conservazione di informazioni per scopi investigativi: la pericolosa squalificazione di garanzie inviolabili della persona e la preoccupazione manifestata dal Garante per la tutela della *privacy* confermano la natura cosmopolita del dibattito che involge la *data retention.*
Volgendo lo sguardo all'ordinamento tedesco, il difficile equilibrio

[55] Per ulteriori approfondimenti sulla giustizia costituzionale belga, cfr. P. Carrozza, *La Cour d'Arbitrage belga,* in G.F. Ferrari, A. Gambaro *(a cura di), Corti nazionali e comparazione giuridica,* Napoli, 2006, 105 ss.; A. Pin, *La giustizia costituzionale*, in T. E. Frosini (a cura di), *Diritto pubblico comparato*, Bologna, 2019, 267 ss.
[56] Corte U.E., C-511/18, C-512/18, C-520/18.
[57] L. G. Sciannella, *La giurisprudenza della Cour Constitutionelle belga nel biennio 2020-2021*, in *Giur. cost.,* 2022, 5, 2423 ss.
[58] G. Formici, *op. cit.*, 316 ss.

tra perquisizioni *online* e diritti costituzionalmente garantiti è giunto all'attenzione dell'organo costituzionale: nel 2008, la Corte tedesca è intervenuta, con una pronuncia additiva, per dirimere il contrasto di legittimità costituzionale tra la legge sulla protezione della Costituzione del Nord Reno-*Westfalia* rispetto agli artt. 10 (segretezza della corrispondenza e delle comunicazioni) e 13 (inviolabilità del domicilio) della Legge fondamentale tedesca (GG)[59].

Pur dichiarando incostituzionale la norma in materia di acquisizione di dati, perché lesiva dei principi di proporzionalità e determinatezza, non ha escluso *in toto* l'ammissibilità di tali strumenti investigativi: i giudici di legittimità costituzionale hanno preso atto dell'esistenza di un nuovo diritto fondamentale alla garanzia della segretezza e integrità dei sistemi informatici, avente rilievo costituzionale e ricavato dal nucleo duro di diritti inviolabili sanciti dalla Costituzione federale[60].

Riprendendo le parole della Corte, il diritto alla garanzia dell'integrità e della riservatezza è espressione del generale diritto alla dignità dell'individuo, così come previsto dall'art. 1.1 della Costituzione tedesca, secondo cui *«[...] la dignità umana è inviolabile e tutti gli organi dello Stato hanno l'obiettivo finale di proteggerla»*[61].

Consapevole della potenziale intrusività dei nuovi strumenti informatici di indagine, la Corte tedesca ha ritenuto necessaria una tutela rafforzata ed ulteriore rispetto a quella già prevista: è necessario non solo un provvedimento autorizzativo del giudice ma altresì l'adozione di misure tecniche idonee ad impedire un accesso sterminato ai dati personali, nonché la previsione di adeguate garanzie consistenti nella distruzione dei dati appresi e nella loro inutilizzabilità processuale qualora siano acquisiti illegittimamente.

Da questa rapida comparazione tra ordinamenti, emerge come nella *digital era* lo sviluppo della personalità dell'uomo e la sua tutela non possono prescindere dall'impiego degli strumenti informatici a fini

---

[59] *BVerfG*, 27 febbraio 2008, *BVerfGE* 120, 274 ss. Per un commento alla sentenza si veda R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico e il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Dir. pen. cont.,* 2009, 697 ss.

[60] F. Iovene, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale,* in *Dir. pen. cont*., 2014, 3-4, 332 ss.

[61] W. Abel, *La decisione della Corte costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d›informazione - un rapporto sul caso BVerfGE, NJW,* 2008, 822, in www.jei.it.

investigativi: la comparazione vuole mettere in risalto come il problema di estendere la categoria dell'inutilizzabilità processuale a tutela della *privacy* riesca a obliterare i confini "domestici", assumendo un rilievo transnazionale.

5. Inutilizzabilità a tutela della *privacy*. Quali sviluppi (futuribili)?

Dalle considerazioni svolte si possono ricavare due prioritarie esigenze da soddisfare: da un lato, il bisogno di una ricostruzione tassonomica della prova digitale e, per quel che qui interessa, dei sequestri informatici; dall'altro, la necessità di individuare nuovi spazi di inutilizzabilità a tutela della riservatezza.

In primo luogo, sarebbe necessario ricostruire lo statuto della prova digitale, attraverso una disciplina *ad hoc* che riesca a salvaguardare l'integrità delle informazioni[62] e, soprattutto, il diritto di ciascuno a vedere rispettata la propria intimità, predisponendo adeguati presidi garantistici e rimedi azionabili dal privato[63].

Con riferimento al sequestro del contenitore e perquisizione, e copia, del contenuto, l'esigenza di garantire autenticità e integrità del dato è assurta a principio fondamentale[64], anche a costo di sacrificare le inviolabili prerogative dell'individuo[65]. I lavori di riforma, confluiti nella legge n.134 del 2021 (Riforma Cartabia), potevano essere l'occasione per ridefinire e tipizzare *ex ante* un'attività acquisitiva dai contorni sfuggevoli: nulla di tutto ciò è stato fatto, essendo stata prevista la sola possibilità di sollevare opposizioni avverso perquisizioni negative e senza che, con il rimedio esperito, si possa conseguire, realmente, l'inutilizzabilità degli elementi appresi.

Non sorprende che, poco dopo l'entrata in vigore della Riforma Cartabia, si sia ritenuto di intervenire nuovamente in materia di *data retention*, cercando di procedimentalizzare il sequestro informatico, individuando opportune scansioni e modalità di svolgimento.

Se il bisogno di tassatività pare essere, almeno sulla carta, soddi-

---

[62] S. Marcolini, *Le indagini atipiche* a *contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.,* 2015, 2, 760 ss.; *Id*., *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 2006, 417 ss., nonché, da ultimo, O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont.,* 2013, 3, 9.

[63] E. Lorenzetto, *op. cit.,* 135 ss.

[64] M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc.,* 2011, 286 ss.

[65] Sull'esigenza di contraddittorio nell'acquisizione di dati digitale, v., *ex multis*, M. Daniele, *La prova digitale nel processo penale*, *cit*., in *Riv. dir. proc*., 2011, 286 ss.

sfatto, continua a destare preoccupazione il silenzio normativo in merito alla possibilità di estendere la sanzionabilità processuale a tutela della riservatezza[66].

Gli argomenti individuati a suffragio di quanto si vuole sostenere sono, almeno, tre: in primo luogo, un argomento, di natura "sistematica", offerto dalle previsioni in materia di intercettazioni telematiche e acquisizioni di documenti all'estero, rispetto alle quali il Legislatore ha già in passato previsto specificamente il divieto di utilizzabilità.

Se l'obiettivo perseguito dal Legislatore è *«[...] il contemperamento delle esigenze di indagine, unitamente all'esigenza di tutela della privacy dell'indagato [...][67]»,* non può ritenersi felicemente e ragionevolmente realizzato tale scopo: passaggio necessario per una ridefinizione organica della materia avrebbe dovuto essere la previsione di una sanzione processuale a tutela della *privacy*.

D'altronde, la necessità di un rimedio è altresì doverosa se si volge lo sguardo alla "vicina" disciplina delle intercettazioni, atteso che lo stesso Legislatore, nel progetto riformatore, pare abbia guardato all'attività intercettativa. Infatti, se, con riguardo alle captazioni di dati[68], è specificamente previsto il ricorso all'inutilizzabilità[69] degli elementi acquisiti qualora non siano state osservate le forme prescritte *ex lege*[70], non si comprende perché analoga sanzione non sia stata posta sul tavolo di discussione per la riforma del sequestro informatico.

La sperequazione trattamentale è altresì evidenziata dal fatto che anche in materia di acquisizione dei dati relativi al traffico telefonico o telematico, è stata disposta la sanzione dell'inutilizzabilità: infatti,

---

[66] L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. e giust.,* 2020, 2, 291 ss.

[67] A.S., n. 690, *cit*.

[68] M. Torre, *Il captatore informatico, tra Riforma Orlando e sistema processuale*, in *Giur. it*., 2018, 7, 1774 ss.; S. Marcolini, *Le indagini atipiche*, cit., 760 ss.; cfr. anche W. Nocerino, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Padova, 2022.

[69] G. Illuminati, *L'inutilizzabilità della prova nel processo penale italiano,* in *Riv. it. dir. proc. pen.,* 2010, 526; D. Chinnici, *L'inutilizzabilità della prova tra punti fermi e profili controversi,* in *Dir. pen. proc.,* 2014, 889; R. Casiraghi, *Prove vietate e processo penale*, in *Riv. it. dir. proc. pen.,* 2009, 1768; N. Galantini, *L'inutilizzabilità della prova nel processo penale*, Milano, 1992, *passim*; F.M. Grifantini, *Inutilizzabilità,* in *D. disc. pen.,* VII, Torino, 1993, 245-246.

[70] E. Alvino, *Formante indiziario e intercettazioni nel prisma dei mezzi di ricerca della prova: lo standard probatorio e il rilievo delle cause di inutilizzabilità nella valutazione della gravità indiziaria*, in *Arch. pen.,* 2021, 3.

a norma dell'art. 240 c.p.p., vengono espunti dal contesto procedimentale «i documenti, i supporti e gli atti concernenti dati e contenuti di conversazioni o comunicazioni, [...], illegalmente formati o acquisiti [...]».
Se il Legislatore avesse realmente voluto ispirarsi a tali situazioni normative, avrebbe dovuto, a rigor di logica, prevedere la sanzione dell'inutilizzabilità, anche solo recependo l'espresso divieto di cui all'art. 240 c.p.p., che pure la giurisprudenza di legittimità[71] ha riconosciuto essere posto a presidio della riservatezza.
In conclusione, se, dapprima, con riguardo alle intercettazioni e, di recente, con riferimento all'acquisizione dei tabulati telefonici, investiti dalla riforma[72], il Legislatore ha quantomeno mostrato interesse alla materia, tentando di ricostruire i confini della captazione di informazioni in linea con il rilievo assunto dalla riservatezza[73], si auspica e si attende la stessa sensibilità per quanto concerne le indagini di carattere esplorativo.
In secondo luogo, si adduce un argomento di matrice "europeistica", che trae fondamento dalla rinnovata consapevolezza di conferire adeguata protezione alla *privacy*, di cui vi è traccia sia nella giurisprudenza sovranazionale[74] sia nelle pronunce della Corte costituzionale tedesca.
Le *guidelines,* offerte dalla giurisprudenza e dalla normativa sovranazionale, sono utili per affrontare le delicate questioni che involgono il terzo, ed ultimo, argomento a sostegno delle nostre conclusioni e, cioè, il valore che oggi assume il "nuovo" diritto alla *privacy*[75].
Se attraverso l'accesso ad un sistema informatico si può ledere la

---

[71] Cass., Sez. un., 25 marzo 2010, *Cagnazzo*; in dottrina, cfr. C. Conti, *Le intercettazioni illegali: lapsus linguae o nuova categoria sanzionatoria?,* in *Dir. pen. proc.,* 2007, 151; P. Dell'Anno, *Violazione della privacy e inutilizzabilità delle acquisizioni documentali correlate: presupposti e limiti,* in *Dir. pen. proc.*, 2012, 723.

[72] D.L. n.132/2021. Sul punto, non sono mancate le critiche. Cfr., G. Pestelli, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in www.quotidianogiuridico.it.

[73] L. Tavassi, *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità,* in *Arch. pen.*, 2022, 1, 4 ss.

[74] R. Flor, *Data retention, Accertamento e repressione dei reati*, in S. Marcolini, R. Flor (a cura di), *Dalla data retention alle indagini ad alto contenuto tecnologico, op. cit.,* Torino, 2022, 138 ss. Critico sul punto è L. Luparia, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Dir. internet*, 2019,4, 753 ss. In giurisprudenza, Corte. U.E., 5 aprile 2022, C-140/20.

[75] F. Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, 1083 ss.

sfera privata di ogni individuo, non sfuggono i delicati profili implicati di libertà e di segretezza delle comunicazioni (art. 15 Cost.), in uno con la inviolabilità del domicilio (art. 14 Cost.), con la tutela della riservatezza (artt. 2 Cost., 8 C.E.D.U., art. 7 Carta di Nizza) e dei dati personali (art. 8 Carta di Nizza, art. 16 T.F.U.E.)[76].
D'altra parte, la Corte costituzionale tedesca nella sentenza sulle *Online Durchsuchung* (perquisizioni *online*)[77] ha precisato che gli strumenti informatici sono congeniali allo sviluppo della personalità, pertanto, i luoghi virtuali vanno oggi protetti a livello costituzionale analogamente a quanto avviene per la tutela del domicilio e, anzi, anche in modo più intenso, giacché si tratta di salvaguardare dati, a prescindere dallo strumento in cui essi sono allocati[78].
Si afferma così una nuova sfera di riservatezza, i cui confini tradizionali, legati alla corporeità e fisicità delle informazioni, divengono evanescenti e lasciano il posto al dato immateriale[79]: trattasi di un nuovo bene giuridico – la riservatezza informatica –, tutelato da molteplici norme del diritto penale sostanziale (artt. 615 *ter*, 615 *quater,* 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.)[80], che si concreta nell'interesse alla protezione delle proprie informazioni. Esso postula un'attenzione maggiore rispetto sia al domicilio materiale sia alla segretezza delle comunicazioni, in quanto involge tutti i dati a-corporei che viaggiano nell'etere digitale.
Ciò posto, è necessario rintracciare il fondamento costituzionale del diritto alla riservatezza[81] informatica: tradizionalmente, esso è ricondotto all'art. 2 Cost.[82], interpretato quale fattispecie aperta a

---

[76] F. Iovene, *op. cit.,* 8 ss.; A. Capone, *Intercettazione e costituzione. Problemi vecchi e nuovi*, in *Cass. pen.*, 2017, 3, 1263 ss.

[77] R. Flor, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention,* in *Ciberspazio e dir.,* 2010, 359 ss.; C. Di Martino, *Il Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, in *Giur. cost.*, 2010, 4059 ss.

[78] A. Baldassarre, *Diritti della persona e valori costituzionali*, Torino, 1997, 45 ss.

[79] S. Rodotà, *Il diritto di avere diritti*, Roma, 2012, 319.

[80] *Ex multis*, L. Picotti, *Reati informatici*, in *Enc. giur. Treccani*, Aggiornamento, VIII, Roma, 2000, 1 ss.

[81] G. Pugliese, *Il diritto alla «riservatezza» nel quadro dei diritti della personalità*, in *Riv. dir. civ.*, 1963, I, 614 ss.

[82] R. Orlandi, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, 1154; cfr., pure, Id., *Osservazioni sul Documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in

nuovi diritti, esplicazione della personalità e dignità dell'uomo[83].
Sebbene il disposto costituzionale sia al centro di antinomiche letture, volte a interpretare la norma, da un lato, in termini di clausola aperta, in grado di abbracciare nuove istanze non emerse nella Costituente e, dall'altro, in termini anacronistici, rimanendo legati ai diritti tradizionali[84], non v'è dubbio che la teoria della portata chiusa del precetto sia frutto di un'impostazione non più aderente all'evoluzione, fisiologica, del catalogo dei diritti inviolabili della persona.
A questo, si aggiunga il valore impresso all'art.8 C.E.D.U., norma interposta ai sensi dell'art. 117 comma 1 Cost.[85], che tutela il diritto al rispetto della vita privata, individuando le condizioni affinché l'intromissione da parte del pubblico potere nell'intimità del singolo non sia lesiva dei diritti inviolabili.
La tutela dei diritti di *privacy* non si arresta all'ambito convenzionale, ma si rinviene altresì nella Carta dei diritti fondamentali dell'Unione Europea, a cui il Trattato di Lisbona ha attribuito lo stesso valore giuridico dei Trattati[86].
In definitiva, dunque, il diritto alla riservatezza informatica, oltrepassando i confini nazionali, è oggi espressione e sintesi della dignità della persona e trova ampia tutela agli artt. 2 Cost., 117 Cost. e artt. 8 C.E.D.U., 7 e 52 CDFUE.
La riconosciuta piena cittadinanza, nel sistema integrato di fonti[87], del diritto alla *privacy*[88] induce a riflettere su nuovi e inesplorati

---

Arch. pen. online, 25 luglio 2016; F. Palazzo, *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615-bis c.p.),* in *Riv. it. dir. proc. pen.,* 1975, 135.

[83] Corte. Cost., n.38 del 1973. A. Barbera, *Commento all'art. 2,* in G. Branca (a cura di*), Commentario alla Costituzione. Principi fondamentali: art. 1-12,* Bologna, 1975, 65 ss; G. Busia, *Riservatezza (diritto alla)*, in *Dig. pubbl.*, Agg., I, Torino, 2000, 481; A. Pace, *Diritti «fondamentali» al di là della Costituzione*, in *Pol. dir.* 1993, 3 ss.

[84] P. Barile, *Diritti dell'uomo e libertà fondamentali,* Bologna, 1984, 54 ss.; P. Grossi, *Inviolabilità dei diritti,* in *Enc. dir.*, vol. XXII, Milano, 1972, 728 ss.

[85] Corte cost., 24 ottobre 2007, n. 349, in *Giur. cost.*, 2007, 3535 ss., con nota di M. Cartabia, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici.*

[86] Nella recente sentenza sulla direttiva c.d. *data retention* (C-293/12, C-594/15, *Digital Rights Ireland* Ltd) la Corte di Giustizia ha riconosciuto che la conservazione dei dati di traffico telefonico e telematico costituisce un'interferenza con l'art. 7 della Carta.

[87] Corte cost., 26 novembre 2009, n. 311, in *Giur. cost.*, 2009, 4657 ss., con nota di M. Massa, *La "sostanza" della giurisprudenza europea sulle leggi retroattive.*

[88] L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.lgs. 10 agosto 2018 n.101*, in *Arch. pen.,* 2019,1, 7 ss.; A. Manna, M. Di Florio, *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissione dell'internet provider*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*,

sentieri dell'inutilizzabilità probatoria[89]: da ciò, deriva la lettura del divieto di utilizzabilità degli atti probatori in termini di sanzione generale e sovraordinata[90]. Conseguentemente, «può a pieno titolo definirsi incostituzionale qualsiasi prova o mezzo di prova, le cui modalità di formazione, di acquisizione o di assunzione – a prescindere dalla qualificazione dell'illecito e indipendentemente dalla presenza di specifici divieti, enunciati nelle norme processuali ordinarie – siano comunque in contrasto con le garanzie fondamentali della persona o del giudizio, che la Costituzione riconosce ed assicura ad ogni individuo, nell'ambito di quel processo equo e giusto»[91].

Dinanzi a condotte illecite legittimate dalla pubblica autorità, la regola di inutilizzabilità probatoria dovrebbe poter estendere i suoi ambiti operativi a presidio delle libertà fondamentali, prescindendo da specifici divieti posti dal Legislatore. Del resto, la "non" scelta del nomoteta, che ha trascurato il problema di un rimedio sanzionatorio a presidio di garanzie inviolabili, non è altro che la conferma di una deriva efficientistica imboccata dalla post-modernità, in cui domina la preminenza dell'interesse pubblico rispetto alla tutela dei diritti del singolo.

E, allora, se, alla luce dell'armonizzazione convenzionale ed euro-unitaria (artt. 7 e 8 Carta di Nizza[92]; art. 8 C.E.D.U.) e in ossequio ad un interpretazione costituzionalmente orientata, va garantito non più, e non soltanto, il diritto a non subire invasioni nella propria sfera privata, ma anche, e soprattutto, il diritto di prevenire l'indebita pubblicizzazione di informazioni personali e di essere rispettati nella propria intimità, va vista con favore la possibilità di ridefinire, in senso ampliativo, il rimedio dell'inutilizzabilità processuale, che realizza il grado massimo di effettività della dignità inviolabile dell'uomo.

Milano, 2019, 892.

[89] C. Conti, *Sicurezza e riservatezza*, in *Dir. pen. proc.,* 2019, 1573; L. Luparia, *Privacy, processo penale e diritti della persona,* in *Riv. dir. proc.,* 2019, 1448 ss.; D. Negri, *Diritto costituzionale applicato: destinazione e destino del processo penale,* in *Proc. pen. giust.,* 2019, 2, 556; F. Petrelli, *La grammatica della legalità,* in *Diritto di difesa,* 2020, 1, 1 ss.

[90] C. Iasevoli, *La funzione "dissuasiva" del processo penale nel relativismo delle tecniche di bilanciamento,* in *Arch. pen.,* 2020, 3, 25 ss.

[91] L.P. Comoglio, *Perquisizione illegittima e inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. pen.*, 1996, 1548.

[92] O. Pollicino, *Commento all'art. 8 della Carta di Nizza*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 136.

Del resto, «[...] la storia delle libertà fondamentali è in gran parte la storia del rispetto delle garanzie procedurali [...][93]».

[93] *Felix Frankfurter Mc Nabb v. United States,* 318 U.S. 332, 1913.