QUESITI

JACOPO DELLA TORRE,
ALESSANDRO MALACARNE*

L'utilizzo dei *file* di *log* per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni

Il contributo si propone di analizzare i profili critici che emergono dalla nuova disciplina italiana in materia di *data retention* (d.l. 30 settembre 2021, n. 132), con specifica attenzione ai c.d. *file* di *log* acquisiti per finalità di contrasto alla criminalità.

The use of log files for law enforcement purposes: issues and remedies

The paper focuses on the critical profiles arising from the new Italian regulation on data retention (Law Decree no. 132 of 30 September 2021) with specific reference to the so-called "log file" acquired for law enforcement purposes.

1. *Premessa.* Con l'adozione del d.l. 30 settembre 2021, n. 132, conv. in l. 23 novembre 2021, n. 178[1], il legislatore ha modificato la disciplina in materia di acquisizione dei dati relativi al traffico telefonico e telematico per finalità di contrasto alla criminalità[2]. Come noto, siffatto intervento si è reso necessario

* Pur essendo il presente lavoro frutto di una riflessione congiunta, Jacopo Della Torre ha redatto i §§ 1, 3, 5 e 6; Alessandro Malacarne i §§ 2 e 4.

[1] Per un commento alla novella, v., tra i molti, FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *www.penaledp.it*, 1° ottobre 2021; LASAGNI, *Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della* privacy, in *www.lalegislazionepenale.eu*, 21 luglio 2022; PESTELLI, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *www.quotidianogiuridico.it*, 4 ottobre 2021; PASTA, *Luci e ombre nella disciplina dei tabulati telefonici nel processo penale*, in *Cass. Pen.*, 2022, 12, 4458 ss.; TAVASSI, *Acquisizione di tabulati, tutela della* privacy *e rispetto del principio di proporzionalità*, in *questa Rivista web*, 20 gennaio 2022; nonché, volendo, MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *www.sistemapenale.it*, 8 ottobre 2021.

[2] La letteratura sul tema è particolarmente ampia. A livello monografico, si segnalano ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018; FLOR-MARCOLINI, *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; e, nella dottrina costituzionalista, con uno sguardo attento ai profili di tutela della riservatezza, FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali*, Torino, 2021. Cfr., altresì e senza pretese di esaustività, ANDOLINA, *La raccolta dei dati relativi alla localizzazione del cellulare ed al traffico telefonico tra inerzia legislativa e supplenza giurisprudenziale*, in *questa Rivista web*, 17 dicembre 2020; ID, *L'ammissibilità degli strumenti di capta-*

onde allineare l'ordinamento italiano rispetto a quanto stabilito dal diritto dell'Unione europea, così come interpretato dalla Corte di giustizia dell'U.E[3]. A spingere i *conditores* ad agire è stata, in particolare, la nota sentenza *H.K. c. Prokuratuur*[4], la quale ha chiarito che l'art. 15 della direttiva 2002/58/CE, letto alla luce degli artt. 7, 8, 11 e 52, par. 1, della Carta di Nizza, osta a una disciplina nazionale che: *i*) non circoscriva l'accesso di autorità pubbliche a dati, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate, «a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica»; *ii*) affidi al pubblico ministero e non a un soggetto terzo

---

zione dei dati personali tra standard *di tutela della* privacy *e onde eversive*, in *questa Rivista*, 2015, 3, 916 ss.; CISTERNA, *Cedu e diritto alla* privacy, in *I principi europei del processo penale*, a cura di Gaito, Roma, 2016, 193 ss.; F.R. DINACCI, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. pen. giust.*, 2022, 2, 301 ss.; ID., *La localizzazione mediante celle telefoniche tra limiti costituzionali e comunitari*, in *Le indagini atipiche*, a cura di Scalfati, Torino, 2019, 470 ss.; LUPÁRIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di internet*, 2019, 4, 753 ss.; MARCOLINI, *L'istituto della* data retention *tra legalità interna ed internazionale*, in *Cybercrime*[2], diretto da Cadoppi, Canestrari, Manna, Papa, Milano, 2023, 1849 ss.; NERONI REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *Sist. pen.*, 2020, 5, 183 ss.; RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, in *Dir. pen. cont.*, 2016, 3, 156 ss.; SAMBUCO, *Note in tema di* data retention, in *questa Rivista web*, 30 giugno 2022; nonché, volendo, MALACARNE, *Corte di giustizia e* data retention: *ultimo atto?*, in *Cass. Pen.*, 2021, 12, 4105 ss.

[3] Si vedano Corte giust. UE, 7 settembre 2023, *Lietuvos Respublikos generalinė prokuratūra*, C-162/22; Corte giust. UE, 17 novembre 2022, *Spetsializirana prokuratura*; Corte giust. UE, 20 settembre 2022, *VD* e *SR*, C-339/20 e C-397/20; Corte giust. UE, 20 settembre 2022, *Space Net*, C-793 e 794/19; Corte giust. UE, 5 aprile 2022, *Commissioner of An Garda Síochána e. a.*, C-140/20; Corte giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, C-746/18; Corte giust. UE, 6 ottobre 2020, *Privacy International*, C-623/17; Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, C 511/18, C 512/18 e C 520/18; Corte giust. UE, 2 aprile 2018, *Ministerio Fiscal*, C-207/16; Corte giust. UE, 21 dicembre 2016, *Tele 2 e Watson*, C-203/15 e C-698/15; Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, C-293/12 e C-594/12.

[4] Corte giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, cit. Per un commento alla pronuncia, v., *ex multis*, ANDOLINA, *La sentenza della Corte di giustizia UE nel caso* H.K. c. Prokuratuur: *un punto di non ritorno nella lunga* querelle *in materia di* data retention*?*, in *Proc. pen. giust.*, 2021, 5, 1195 ss.; 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.*, 2023, 7-8, 2563 ss.; FILIPPI, *Il legislatore deve urgentemente riformare la disciplina dell'acquisizione dei tabulati relativi al traffico e all'ubicazione*, in *www.ilpenalista.it*, 15 marzo 2021; LA ROCCA, *Dopo la Corte di Giustizia in materia di tabulati: applicazioni e disapplicazioni interne*, in *questa Rivista web*, 2021, 2, 1 ss.; RAFARACI, *Verso una* law of evidence *dei dati*, in *Dir. pen. proc.*, 2021, 7, 853 ss.; RESTA, *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla* data retention*. I riflessi sulla disciplina interna*, in *www.giustiziainsieme.it*, 6 marzo 2021; SPANGHER, *I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali*, in *www.giustiziainsieme.it*, 3 maggio 2021.

(come il giudice) la competenza ad autorizzare l'accesso alle medesime informazioni.

Ed è proprio in questa prospettiva che il menzionato decreto 132/2021, interpolando l'art. 132 del d.lgs. 30 giugno 2003, n. 196 (c.d. "codice della *privacy*"), ha, per un verso, limitato la possibilità di acquisire i dati relativi al traffico telefonico o telematico alla necessità di contrastare una serie di fattispecie di reato, tassativamente individuate dalla legge[5], nonché, per un altro, attribuito all'autorità giurisdizionale e non più alla pubblica accusa il compito di autorizzare *ex ante* o di convalidare comunque *ex post* l'apprensione dei medesimi.

Pur avendo segnato un passo avanti rispetto allo *status quo*, deve riconoscersi come l'attuale regolamentazione della c.d. "*data retention*" presenti ancora svariati profili di criticità[6]. Tra questi va annoverata la tematica dell'archiviazione e delle modalità acquisitive dei c.d. *file* di *log*; locuzione di sintesi con cui, come si vedrà meglio a breve, si fa riferimento a una sorta di diario ove vengono registrate, in ordine cronologico, tutte le attività realizzate *online* dall'utilizzatore di un apparecchio telematico[7]. La *quaestio iuris*, con la

---

[5] Il nuovo terzo comma dell'art. 132 codice *privacy* limita l'impiego del mezzo di ricerca della prova in esame ai soli «reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi». Alcuni autori, tuttavia, hanno osservato come il catalogo dei reati previsto dal legislatore e i limiti di pena individuati all'art. 132 non possano essere ricondotti nel concetto di "reato grave", così per come definito dalla giurisprudenza europea in argomento (per questa opinione, v., *in primis*, F.R. DINACCI, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia*, cit., 315. Concorde pure MURRO, *Dubbi di legittimità costituzionale e problemi di inquadramento sistematico della nuova disciplina dei tabulati*, in *Cass. Pen.*, 2022, 6, 2446). Dubbi in proposito sono manifestati anche da SPANGHER, Data retention: *svolta garantista ma occorre completare l'impianto*, in *Guida dir.*, 2021, 39, 13; PASTA, *Luci e ombre nella disciplina dei tabulati telefonici nel processo penale*, cit., 4462, nt. 20. *Contra*, invece, PESTELLI, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, cit.

[6] Per un esame dei quali, cfr. F.R. DINACCI, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia*, cit., 301 ss.; FILIPPI, *Tabulati telefonici e telematici e rispetto della vita privata*, in *www.dirittodidifesa.eu*, 5 febbraio 2022; PASTA, *Luci e ombre nella disciplina dei tabulati telefonici nel processo penale*, cit., 4458 ss.; SPANGHER, *I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali*, cit.; DEMARTIS, *La nuova disciplina sui tabulati: un completo adeguamento agli* standard *europei?*, in *Dir. pen. proc.*, 2022, 3, 299 ss.; TESSITORE, *Acquisizione dei tabulati telefonici e* privacy: *l'interpretazione della Corte di Cassazione e le ultime modifiche normative*, in *Proc. pen. giust.*, 2022, 2, 472 ss.; e, volendo, MALACARNE-TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?*, in *questa Rivista web*, 15 settembre 2022.

[7] L'espressione inglese *log*, diffusasi solo nella metà del XX secolo in ambito informatico, deriva dal gergo nautico e risale al 1800, periodo in cui i marinai utilizzavano un registro chiamato "*logbook*" per annotare la velocità della nave, le condizioni metereologiche e altri eventi significativi accaduti nel corso

quale gli interpreti hanno dovuto, fin da subito, confrontarsi concerne, più nello specifico, la possibilità di impiegare o meno l'art. 132 codice *privacy* anche per giustificare l'apprensione di quella che è stata descritta come «*log evidence*»[8], la quale non è stata menzionata, in modo espresso, dal legislatore né in questa, né in altre disposizioni.

È bene precisare fin da subito come si tratti di un quesito di significativa importanza pratica: attraverso l'analisi di siffatta categoria di evidenze digitali le autorità possono, invero, compiere svariate attività di rilievo primario per il contrasto alla criminalità, quali, ad esempio, l'identificazione delle generalità di un bersaglio che operi sul *web*, oppure, ancora, il tracciamento dei suoi contatti o delle sue ricerche *online*, sino ad arrivare anche all'individuazione del luogo in cui si trovi l'apparecchio da lui impiegato[9].

Se un tanto è vero, è, tuttavia, opportuno rendersi conto di come, attraverso la consultazione di tali "registri informatici", le forze dell'ordine siano in grado di compiere un controllo – a seconda dei casi – anche molto penetrante sulle abitudini di una persona. Non è un caso, dunque, che l'Unione europea, seppur in un atto dedicato alla cooperazione internazionale – il regolamento (UE) 2023/1543 (c.d. "regolamento *e-evidence*"), relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche[10] – abbia, di recente, chiarito che, per l'apprensione di tali categorie

---

del viaggio. A sua volta, questa locuzione traeva origine da un antico strumento denominato "*chip log*" consistente in un pezzo di legno galleggiante collegato a una corda con nodi regolari, grazie al quale i navigatori potevano calcolare la velocità delle imbarcazioni.

[8] Per tale denominazione, v. KENNEALLY, *Digital logs-proof matters*, in *Digital Investigation*, 2004, 1, 97.

[9] CASEY, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, San Diego, 2011, 535 ss.; KENNEALLY, *Digital logs-proof matters*, cit., 94; LALLA-FLOWERDAY-SANYAMAHWE-TARWIREYI, *A Log File Digital Forensic Model*, in *Advances in Digital Forensics VIII*, 2012, 247 ss.

[10] Per un commento alla versione definitiva approvata dal Parlamento, v. GAUDIERI, *Novità in tema di cooperazione giudiziaria: i nuovi ordini europei di conservazione e produzione delle prove elettroniche*, in *Dir. pen proc.*, 2023, 9, 1231 ss.; FORLANI, *The E-evidence Package. The Happy Ending of a Long Negotiation Saga*, in *www.eucrim.eu*, 19 ottobre 2023; JUSZCZAK-SASON, *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. An Introduction to the New EU Package on E-evidence*, in *ivi*, 19 ottobre 2023; TOPALNAKOS, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, in *ivi*, 12 ottobre 2023. In merito ai lavori preparatori, v., invece, *ex multis*, BURCHARD, *Regolamento europeo* e-evidence. *Deficitario dal punto di vista dello Stato di diritto, superato dalla realtà e a lungo termine in contrasto con gli interessi europei*, in *Rivista Eurojust*, 2020, 2, 199 ss.; CORHAY, *Private Life, Personal Data Protection and the Role of Service Providers: The EU E-Evidence Proposal*, in *European Paper*, 2021, 6, 441 ss.; DEPAUW, *Electronic Evidence in Criminal Matters: How About E-Evidence Proposal*, in *European Criminal Law Review*, 2018, 1, 62 ss.; GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento* e-evidence, in *Cass. Pen.*, 2019, 3, 1340 ss.; POLLICINO-BASSINI, *La proposta di regolamento*

di dati, è necessario rispettare le garanzie previste dall'*acquis* eurounitario in materia di protezione della vita privata e dei dati personali[11] (tra cui, in ambito penale, spiccano gli artt. 7 e 8 della Carta di Nizza, nonché la direttiva 2016/680/UE).
Preso atto di ciò, scopo del presente lavoro sarà quello di fare chiarezza in merito al rapporto tra ordinamento interno, così come novellato a seguito dell'approvazione del d.l. 132/2021, e la conservazione e l'acquisizione di *file* di *log* per scopi di *law enforcement*. Più in particolare, dopo aver fornito alcune precisazioni di carattere terminologico e concettuale in merito a tale categoria, l'obiettivo sarà quello di comprendere se la vigente normativa italiana sia idonea a garantire, da questa peculiare prospettiva, il rispetto dei valori sovraordinati in gioco, oppure se, al contrario, risulti necessario predisporre un ulteriore intervento correttivo, volto ad assicurare un bilanciamento più adeguato tra esigenze di repressione dei reati e di protezione dei diritti fondamentali della persona.

2. *Disorientamenti definitori in tema di "*file *di* log*"*. Come anticipato, nel lessico informatico, la locuzione "*file* di *log*" fa riferimento a un *file*, in formato di testo, nel quale vengono indicate le operazioni compiute da un determinato utente durante una sessione di lavoro del proprio dispositivo elettronico, sia esso un *personal computer*, uno *smartphone*, un *tablet*, e così via[12]. Trattasi, in buona sostanza, di vere e proprie "impronte digitali 2.0"[13], le quali assu-

---

e-Evidence: *osservazioni a caldo e possibili sviluppi*, in *www.medialaws.eu*, 26 ottobre 2018; nonché, volendo, GIALUZ-DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont*, 2018, 5, 277 ss.

[11] Cfr. il considerando n. 32 del regolamento, ove si stabilisce che «gli indirizzi IP devono essere considerati quali dati personali e devono godere di piena protezione a norma dell'*acquis* dell'Unione sulla protezione dei dati».

[12] Per questa definizione, v. CASEY, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, cit., 535; ZICCARDI, *L'origine della* computer forensics *e le definizioni*, in Lupária, Ziccardi, *Investigazione penale e tecnologie informatiche. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, 32, nt. 40. La nozione sembra essere ampiamente condivisa pure nella dottrina penalistica e processualistica, v., ad es., FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in *Cybercrime*, diretto da Cadoppi, Canestrari, Manna, Papa, Milano, 2019, 182, nt. 100; GIORDANO, *L'acquisizione dei* file *di* log *dopo la conversione del decreto sui tabulati*, in *www.ilpenalista.it*, 30 maggio 2022; TONINI, *L'evoluzione delle categorie tradizionali, il documento informatico*, in *Cybercrime*[2], diretto da Cadoppi, Canestrari, Manna, Papa, cit., 1315, nt. 29; VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, 24, nt. 2.

[13] KENNEALLY, *Digital logs-proof matters*, cit., 97. L'immagine è ripresa pure da MARAFIOTI, Digital evidence *e processo penale*, in *Cass. Pen.*, 2011, 12, 4509.

mono una notevole importanza specie sul versante investigativo, giacché consentono agli inquirenti di mappare, analiticamente, le attività realizzate nel *web* da un determinato bersaglio. Attraverso la loro analisi, diviene, infatti, possibile conoscere: *i*) gli orari e la durata della connessione a *internet* di un certo *target*; *ii*) l'indirizzo IP utilizzato per la connessione; *iii*) le informazioni (strutturate in "pacchetti") che questi ha inviato o ricevuto attraverso l'indirizzo IP assegnato[14]; oppure, ancora, *iv*) l'anagrafica dell'intestatario di un contratto di utenza. Alla luce di ciò, ben si comprende il perché gli studiosi d'oltreoceano abbiano coniato l'espressione «*behavioral evidence*», onde descrivere le enormi potenzialità dei "registri telematici", la cui analisi è in grado di determinare, con un elevato grado di dettaglio, «*what an individual did or was trying to achieve [on the web]*»[15].

Da un punto di vista classificatorio, i più accreditati esperti di *digital forensics* sono soliti distinguere quattro tipologie di registri principali[16].

Si parla, in proposito, di "*authentication log*" per indicare quei *file* che mostrano a quale *account*, indirizzo IP e numero telefonico è associata una richiesta di connessione alla rete (ad esempio al servizio di posta elettronica o a un *social network*) proveniente dall'*host,* cioè dal dispositivo elettronico in uso al bersaglio. Con l'impiego della locuzione "*application log*" ci si riferisce, invece, a quei diari elettronici contenenti informazioni sulle attività *online* realizzate da un determinato apparecchio digitale. Si tratta, in estrema sintesi, degli indirizzi IP utilizzati dal *client* (*rectius*, il *target*) e conservati dal *server provider*, dai quali è possibile determinare tutte le operazioni compiute nel *web* in uno specifico arco temporale. Vi sono, poi, i c.d. "*operating system log*", cioè registri di testo nei quali vengono cristallizzati eventi particolarmente significativi, come, a mero titolo di esempio, i riavvii o gli errori del sistema operativo. Da ultimo, è possibile identificare i c.d. "*network device log*", ovverosia i *log* contenuti nei dispositivi di rete, come il *router*, i quali, pur avendo spesso una quantità limitata di memoria per archiviare le operazioni eseguite nel *web*, possono essere molto utili per corroborare la genuinità dei *log* provenienti da altre fonti[17].

---

[14] Si pensi, ad esempio, all'accesso ai siti, allo scaricamento di pagine *web* o di specifici *file*, alle conversazioni in *chat*, alla partecipazione a *newsgroup*, o, ancora, alla trasmissione o ricezione di posta elettronica.

[15] Per entrambe le citazioni, v. CASEY, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, cit., 261.

[16] Sul punto, v., nuovamente, CASEY, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, cit., 755-765.

[17] CASEY, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, cit.,

Partendo da tale divisione, è, inoltre, possibile distinguere ulteriormente tra: *i*) quei *file* di *log* prodotti dagli applicativi tutte le volte in cui viene attivata una comunicazione telematica (attraverso *internet*) fra due o più dispostivi elettronici; *ii*) quelli relativi alla mera consultazione di pagine o siti *online*, senza che sia avvenuta alcuna comunicazione; e, da ultimo, *iii*) quelli concernenti semplici dati di *background*, nei quali vengono registrate le operazioni compiute da un sistema pur in assenza di un'interazione diretta dell'utente.
Se, fino all'entrata in vigore del d.l. 132/2021, in campo processualpenalistico non vi erano stati particolari problemi nella definizione di tale categoria di prove elettroniche, va segnalato come, a valle di tale novella, si sia delineato in proposito un acceso contrasto esegetico. Il che si spiega in ragione del fatto che la necessità di rispettare uno *standard* maggiore di garanzie, sia a livello oggettivo, sia di procedura applicabile, per apprendere i c.d. dati relativi al traffico telefonico e telematico ha portato gli interpreti a chiedersi se lo stesso livello di tutela vada rispettato anche laddove a essere oggetto di analisi siano i *file* di *log*.
Al riguardo, va osservato come un primo gruppo di interpreti abbia avanzato, in proposito, un'esegesi restrittiva[18], tesa a distinguere nettamente tra tale nozione e i "dati di traffico".
Più in particolare, in questa prospettiva, si è proposto di ricomprendere nella locuzione di "*file* di *log*" esclusivamente i dati sulla connessione assegnata a un'utenza (cioè, l'indirizzo "IP di destinazione", ovverosia l'IP che consente di identificare i siti *web* visitati dall'utente[19]) slegati dall'avvenuta comunicazione telematica tra due o più dispositivi. L'interpretazione in parola è stata giustificata, principalmente, muovendo dal tenore letterale dell'art. 121, co. 1 lett. *h*) del d.lgs. 196/2003[20], a mente del quale i «dati relativi al traffico», acquisibili nei casi e nei modi stabiliti dal novellato art. 132 codice *privacy*, sono

764, il quale sottolinea, per l'appunto, come «*even when the activities were recorded by other systems, logs from network devices can be used for corroboration, providing independent sources of digital evidence relating to the same events*».

[18] La tesi è sostenuta da PESTELLI, *Convertito in legge il D.L. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *www.quotidianogiuridico.it*, 18 novembre 2021; GITTARDI, *Sull'utilizzabilità dei dati del traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in *www.giustiziainsieme.it*, 7 ottobre 2021.

[19] In proposito, v. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, 26.

[20] Ad ulteriore conferma della bontà di tale esegesi muoverebbe, altresì, l'indicazione contenuta all'art. 2, co. 1 lett. b) della Direttiva 2002/58/CE, ove si specifica, al pari di quanto previsto nel codice della *privacy* italiano, che per «dati relativi al traffico» deve intendersi qualsiasi informazione sottoposta a trattamento «ai fini della trasmissione di una comunicazione» sulla rete *internet*.

definiti alla stregua di «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica». Da questo angolo di visuale, si è, pertanto, affermato che la lettera della legge indurrebbe ad annoverare nel *genus* dei "dati di traffico telematico" solo quei *bit* che attengono a una dinamica *stricto sensu* comunicativa, mentre in quello dei "*file* di *log*" le tracce digitali non legate a una conversazione telematica.
Sennonché, a tale esegesi, se ne è ben presto contrapposta una antitetica, estensiva, stando alla quale, nonostante il dettato del codice della *privacy*, vi sarebbe una perfetta coincidenza tra il concetto in esame e quello di "dati di traffico telematico". In questa prospettiva, si è, ad esempio, autorevolmente affermato che «sono proprio e soltanto i c.d. *log files* che contengono dati relativi al traffico telematico»[21]. Vale la pena di precisare come questa impostazione si giustifica sulla base di lodevoli intenti valoriali; e, in particolare, in ragione del carattere potenzialmente assai intrusivo dell'attività acquisitiva dei *log file*. Come si è, infatti, anticipato, le informazioni contenute nel "registro telematico" sono idonee a rivelare elementi di dettaglio sulle abitudini di vita di un soggetto, posto che indicano gli accessi effettuati, i siti visitati, la durata della connessione, etc.: trattasi, pertanto, proprio di quei "dati" che le istituzioni europee sono solite ricondurre nell'alveo di tutela degli artt. 7 e 8 della Carta di Nizza e dell'art. 8 C.E.D.U.[22].
Al riguardo, mette conto di aggiungere come anche la pur non cospicua giurisprudenza di legittimità paia, a sua volta, divisa sul punto.
A fronte di un *obiter dictum*, nel quale i giudici hanno adottato un approccio volto a ricomprendere nel concetto di "dati sul traffico" pure i *file* di *log* (nel caso di specie, relativi a un *account Instagram*)[23], senza alcuna distinzione di sorta, in una successiva pronuncia la Corte ha prospettato un'impostazione più restrittiva. In un caso relativo all'acquisizione dei dati di traffico disposta dal pubblico ministero nella vigenza della vecchia formulazione dell'art. 132 codice *privacy*, il Supremo consesso ha operato esplicitamente una distinzione tra i «dati c.d. "esterni" alle conversazioni», resi fruibili nel processo me-

[21] Testualmente, FILIPPI, *Riservatezza e* data retention: *una storia infinita*, in *www.penaledp.it*, 23 giugno 2022, par. 17; ID., *Tabulati telefonici e telematici e rispetto della vita privata*, cit. Parrebbero orientati in tal senso pure ATERNO-CAJANI, *L'acquisizione dei dati di traffico*, in AA.VV., Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, 322; PARODI, *Convertito il decreto in tema tabulati: (quasi) tutto chiaro*, in *www.ilpenalista.it*, 19 novembre 2021, il quale si domanda «quali sarebbero i dati sul traffico telematico – escludendo i *file* di *log* – la cui acquisizione sarebbe subordinata al provvedimento del GIP? Difficile trovarne»; TAVASSI, *Acquisizione di tabulati, tutela della* privacy *e rispetto del principio di proporzionalità*, cit., 3.
[22] FILIPPI, *Riservatezza e* data retention: *una storia infinita*, cit., par. 17.
[23] Ci si riferisce a Cass., Sez. V, 26 ottobre 2021, n. 45278, in *Dejure*

diante la produzione della stampa dei tabulati, e «altre tipologie di dati», tra i quali sono stati annoverati, per l'appunto, i «*file* di *log*»[24].
Se quanto finora descritto rappresenta lo stato dell'arte a livello interno, deve osservarsi come l'Unione europea, mediante il già menzionato regolamento UE 2023/1543, abbia optato per una terza impostazione, che risulta, di per sé, preferibile in quanto maggiormente in linea con il significato tecnico-informatico del termine in esame.
Dalla lettura dell'art. 3 di tale atto, da leggersi assieme ai considerando n. 32-34, si desume, infatti, come il legislatore eurounitario abbia fatto propria una nozione ampia della locuzione "*file* di *log*", definendola come l'insieme degli indirizzi IP e dei numeri di accesso alla rete legati *lato sensu* all'impiego di apparecchi telematici. Nel contempo, però, ha avuto la cura di precisare che il concetto di *log evidence* e quello di "dati di traffico", pur intersecandosi, non sono del tutto coincidenti. Difatti, l'atto europeo ha ricompreso nella categoria dei "*traffic data*" solo quei *file* di *log* impiegati per obiettivi diversi dalla mera identificazione di un utente[25]. Come si vedrà meglio in seguito, secondo lo schema delineato dall'Unione, a contare non è, invero, tanto la natura tecnica della *digital evidence* appresa, quanto l'utilizzo che venga fatto della medesima da parte dell'autorità: più l'invasione nella sfera giuridica del singolo sarà incisiva, maggiori garanzie andranno previste a livello processuale per contemperare i diversi interessi in gioco.
Giunti a questo punto, è opportuno soffermarsi sugli effetti che, sul piano dell'ordinamento interno, si verificano laddove si scelga di aderire a una o all'altra delle impostazioni finora descritte.

3. *La conservazione e l'acquisizione dei "registri telematici" alla prova della legislazione vigente*. Come è facilmente intuibile, la definizione, più o meno

[24] Cfr. Cass., Sez. V, 24 febbraio 2022, n. 8968, par. 3.1, in *Dejure*.
[25] Nel considerando n. 32 si legge espressamente che «gli indirizzi IP come pure i numeri di accesso e le relative informazioni possono rappresentare un punto di partenza fondamentale per le indagini penali in cui l'identità di un indagato non è nota. Tipicamente essi costituiscono componenti di una registrazione di eventi, anche conosciuta come "*log server*", che indica l'inizio e la fine di una sessione di accesso utente a un servizio. Il più delle volte si tratta di un indirizzo IP, statico o dinamico, o di un altro identificatore che individua l'interfaccia di rete usata durante la sessione di accesso». Posta tale definizione, nel considerando n. 33 si specifica che «qualora gli indirizzi IP, i numeri di accesso e le relative informazioni non siano richiesti al solo scopo di identificare l'utente nell'ambito di un'indagine penale specifica, essi sono generalmente richiesti per ottenere informazioni più invasive della vita privata. [...] È pertanto essenziale che, in tali situazioni, gli indirizzi IP, i numeri di accesso e le relative informazioni non richiesti al solo fine di identificare l'utente nell'ambito di un'indagine penale specifica siano trattati come dati relativi al traffico e richiesti nel quadro dello stesso regime applicabile a quello dei dati relativi al contenuto, quali definiti nel presente regolamento».

ampia, che si ritenga opportuno attribuire al concetto di *file* di *log* incide, in modo determinante, sulle garanzie da applicare per apprendere i medesimi.
Le conseguenze della scelta di optare per la sopra descritta esegesi restrittiva, tesa a creare una distinzione ontologica tra i "diari di bordo" in esame e i dati di traffico, sono, infatti, chiare. Ove le cose stessero così, per la conservazione e l'acquisizione dei primi non potrebbe utilizzarsi lo strumento dell'art. 132 del codice *privacy* (e ciò per la semplice ragione per cui tale disposizione si riferisce unicamente ai «dati di traffico»), bensì solamente altri canali processuali. Tra questi sono stati, ad esempio, menzionati gli artt. 256[26] e 254-*bis*[27] c.p.p., i quali, oltre a non contemplare limiti edittali di sorta, consentono al pubblico ministero di attivarsi direttamente, senza dover chiedere un'autorizzazione giudiziale *ex ante* o *ex post*.
Benché, come si è visto, tale interpretazione si dimostri coerente con il dettato letterale dell'art. 121 codice *privacy*, essa presta il fianco a un triplice ordine di problemi.
In primo luogo, viene a determinarsi una palese forzatura da una prospettiva tecnico-informatica: a ben considerare, infatti, tanto i "*file* di *log* di destinazione" (cioè, quelli relativi ai siti *web* visitati), quanto quelli "comunicativi", vanno certamente ricondotti in una stessa macrocategoria, costituita, per l'appunto, dalla *log evidence*. Ne consegue, pertanto, che una tale lettura presenta il problema di attribuire al termine *de quo* un significato diverso da quello proprio delle parole secondo l'accezione comune, ponendosi, pertanto, in contrasto con uno dei criteri interpretativi generali dell'ordinamento, fissati dall'art. 12 delle preleggi.
In seconda battuta, l'esclusione dei *file* di *log* dal campo applicativo dell'art. 132 creerebbe un preoccupante vuoto normativo concernente la conservazione (c.d. *data storage*) di questi dati. In effetti, se la disposizione in parola riferisce l'obbligo, in capo ai *service provider*, di memorizzare solamente i «dati di traffico», ne conseguirebbe, all'evidenza, l'impossibilità di applicare la disciplina prevista nel primo comma con riguardo a tutte quelle informazioni che fuoriescono da tale concetto.
Infine, non va tralasciato come la scelta di consentire l'acquisizione dei "registri telematici" per la generalità dei reati e, oltretutto, a un organo non terzo, quale la pubblica accusa, rischierebbe di determinare frizioni rispetto ai diritti fondamentali dell'individuo, posto che anche attraverso l'acquisizione di tali dati l'autorità pubblica è in grado di compiere un controllo significativo sulla

[26] La prospettazione è di PESTELLI, *Convertito in legge il D.L. 132/*2021, cit.
[27] Circa tale ipotesi, v., ad esempio, GIORDANO, *L'acquisizione dei* file *di* log, cit.

sfera di riservatezza dell'individuo[28]; con tutto ciò che ne consegue in termini di frizione con le garanzie previste agli artt. 7 e 8 della Carta di Nizza, così come interpretati dalla Corte di giustizia.

Nel caso in cui, per converso, si propendesse per l'esegesi estensiva, secondo la quale vi sarebbe una totale coincidenza tra *file* di *log* e dati di traffico telematico, il quadro normativo applicabile diverrebbe ben diverso. In tale evenienza, sarebbe, infatti, senz'altro utilizzabile l'art. 132 codice *privacy*, il quale, oltre a contemplare un vaglio di proporzionalità in astratto e uno giudiziale in concreto sull'acquisizione dei dati, stabilisce pure uno specifico regime di conservazione per i medesimi. Il che significherebbe ovviare a due delle principali criticità che affliggono la prima lettura.

Ciò nondimeno, pure l'interpretazione in questione non può dirsi esente da critiche.

Come si è visto, infatti, è lo stesso diritto dell'Unione europea (*rectius*, il regolamento *e-evidence*) che, in determinate circostanze, tende, oramai, a escludere espressamente una totale assimilazione tra i *file* di *log* e i dati di traffico in senso stretto. Ma, soprattutto, tale lettura pare difficilmente conciliabile con un'interpretazione letterale della vigente versione dell'art. 121, co. 1 lett. *h*) del codice *privacy*, a mente del quale, lo si è detto, i «dati relativi al traffico» vengono qualificati in termini di informazioni sottoposte a «trattamento ai fini della trasmissione di una comunicazione». Da un tanto ne consegue, dunque, che l'adozione di un'esegesi rigorosa del termine "comunicazione" renderebbe inapplicabile l'art. 132 del codice *privacy* per tutte quelle tipologie di *file* di *log* non strettamente legate a una conversazione in senso stretto[29].

---

[28] Lo stesso considerando n. 33 del Regolamento *e-evidence*, lo si è visto, specifica che «qualora gli indirizzi IP, i numeri di accesso e le relative informazioni non siano richiesti al solo scopo di identificare l'utente», essi «potrebbero servire per definire il profilo completo di una persona, ma al tempo stesso possono essere trattati e analizzati più facilmente rispetto ai dati relativi al contenuto, essendo già presentati in un formato strutturato e standardizzato».

[29] A tal proposito, peraltro, potrebbe prospettarsi una possibile soluzione esegetica che passa per la scelta di accogliere una nozione estensiva del concetto di "comunicazione digitale", così come tipizzato all'art. 121 codice *privacy*. Per quanto riguarda gli apparecchi telematici, detta locuzione dovrebbe essere, in particolare, interpretata in maniera più ampia, fino a ricomprendervi tutti i casi in cui la macchina "comunichi" con la rete e intrattenga con essa uno scambio di dati, a prescindere, dunque, da una trasmissione di contenuto informativo tra più soggetti. In proposito, va, del resto, ricordato come autorevole dottrina abbia esteso il concetto di comunicazione anche alle «*machine-to-machine interaction or human-computer interaction*». Si vedano le riflessioni di QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, 59 s. A ciò va aggiunto che, a deporre in tal senso, potrebbe essere, inoltre, il *dictum* dell'art. 4, co. 2 lett. c) dello stesso codice *privacy*, nella parte in cui definisce le «reti di comunicazione elettronica» come quei «sistemi di trasmissione [...] che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici [...] compresa *Internet*». Il tenore te-

Infine, laddove si preferisse risolvere l'*impasse* adottando un'esegesi dei termini "*file* di *log*" e "dati di traffico" analoga a quella cristallizzata nel regolamento *e-evidence*, il quadro diverrebbe il seguente. In tutti i casi in cui il registro informatico venisse appreso per finalità di *law enforcement* onde compiere un "tracciamento dinamico" delle varie attività *online* compiute da un utente, si potrebbe applicare l'art. 132 codice *privacy*, in quanto, stando al citato provvedimento UE, saremmo di fronte a veri e propri "dati di traffico". Per contro, qualora le autorità investigative avessero la necessità di ottenere un indirizzo IP, nonché i numeri di accesso e le relative informazioni, al solo fine di conoscere le generalità di un utente ("controllo statico"), tale previsione non potrebbe applicarsi, trattandosi di un "dato relativo agli abbonati", e dovrebbe farsi uso di altri canali processuali, come, per l'appunto, quelli di cui agli artt. 256[30] o 254-*bis* c.p.p.[31].

Non sfuggirà, però, come anche tale soluzione ermeneutica, oltre a conciliarsi difficilmente con l'attuale formulazione letterale dell'art. 121 del codice *privacy*, lasci in piedi, a sua volta, problemi non secondari, tra cui quello di far riferimento a un atto europeo espressamente dedicato alla cooperazione internazionale e non alle fattispecie puramente interne, il quale non è, oltretutto, ancora entrato in vigore[32].

Ma il problema maggiore è rappresentato dal fatto che, in ogni caso, la disciplina italiana non contemplerebbe un regime di conservazione specifico – e, dunque, temporalmente limitato – per quanto concerne i *file* di *log* impiegati per meri scopi di identificazione. Non venendo in gioco l'art. 132 codice *privacy*, si potrebbe, invero, far sì uso di regole per acquisire tali informazioni nel procedimento, ma mancherebbe una previsione *ad hoc* che ne stabilisca i tempi e modi di stoccaggio da parte dei *provider*[33]. Ed è noto che la fissazione di limiti cronologici di conservazione dei dati, acquisiti per finalità di contra-

---

stuale della disposizione potrebbe, infatti, giustificare, *de iure condito*, l'adozione di una nozione particolarmente estesa di "comunicazione a mezzo *web*", ricomprendendovi pure quelle trasmissioni di dati "*machine to internet*".

[30] Sulla possibilità di ricorrere a un semplice decreto di acquisizione al solo fine di acquisire i *file* di *log* per «rintracciare e identificare il soggetto registrato presso un servizio di accesso o di comunicazione», v. pure PARODI, *Convertito il decreto in tema tabulati*, cit., il quale, però, non opera alcun riferimento al contenuto del regolamento *e-evidence*.

[31] Cfr., ancora, GIORDANO, *L'acquisizione dei* file *di* log, cit.

[32] Come stabilito all'art. 34 del regolamento, la disciplina *ivi* contenuta si applicherà a decorrere dal 18 agosto 2026.

[33] In proposito, non sembra poter venire in rilievo la disciplina della conservazione per finalità di fatturazione, di cui all'art. 123 codice *privacy*, in quanto, per l'appunto, destinata a uno scopo diverso da quello penale-repressivo.

sto alla criminalità, rappresenta uno dei requisiti essenziali fissati dalla Corte di giustizia per rendere proporzionate le limitazioni dei diritti fondamentali alla vita privata e alla protezione delle informazioni personali[34].
Alla luce di quanto finora osservato, un elemento sarà emerso con chiarezza: pur a fronte di significativi sforzi esegetici, l'attuale tessuto normativo nostrano non pare in grado di adattarsi, in modo fisiologico, alla tematica della *data retention* dei *file* di *log*. Il quadro che emerge dalle disposizioni vigenti risulta, infatti, oltremodo frastagliato e fitto di nodi problematici difficilmente solubili *de iure condito*, con tutto ciò che ne consegue in termini di incertezze per gli operatori giuridici e di pericolo di frizioni con i diritti fondamentali della persona. Il che consente di rispondere, fin da ora, in un senso positivo al quesito posto in premessa circa la necessità di adottare un ulteriore intervento correttivo in materia.

4. *La distinzione tra accessi ai* file *di* log *"intrusivi" e "limitatamente intrusivi"*.
Al fine di strutturare una possibile disciplina in tema di conservazione e di acquisizione della *log evidence*, che si dimostri, finalmente, in grado di contemperare i diritti fondamentali dell'individuo con le esigenze repressive dell'autorità, è opportuno richiamare alcuni insegnamenti sviluppati dalla giurisprudenza della Corte di giustizia con riguardo alla più generale materia della *data retention*.
Come noto, a questo proposito, i giudici europei hanno, da tempo, delineato una distinzione, ispirata al principio di proporzionalità, tra: *i*) ingerenze gravi nella vita privata e *ii*) ingerenze lievi con riguardo a tale diritto fondamentale[35].
Al riguardo, sin dalla celebre sentenza *Digital Rights Ireland*, si è affermato,

[34] Corte giust. UE, 21 dicembre 2016, *Tele 2 e Watson*, cit., parr. 95-98; Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit., parr. 34, 44, 45.
[35] Cfr., in particolare, Corte giust. UE, 7 settembre 2023, *Lietuvos Respublikos generalinė prokuratūra*, cit., par. 31; Corte giust. UE, 5 aprile 2022, *Commissioner of An Garda Síochána e. a.*, cit., par. 59; Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, cit., par. 158; Corte giust. UE, 2 aprile 2018, *Ministerio Fiscal*, cit., parr. 56 e 57; Corte giust. UE, 21 dicembre 2016, *Tele 2 e Watson*, cit., par. 102; Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit., par. 60. In dottrina v. FLOR-MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico*, cit., 17; nonché la tabella predisposta nell'ambito di un recente studio in tema di *data retention*, dalla quale emerge chiaramente la differente modulazione degli *standard* di tutela richiesti dalla Corte di giustizia a seconda della gravità dell'intrusione nella vita privata dei singoli individui (cfr. MITSILEGAS-GUILD-KUSKONMAZ-VAVOULA, *Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks*, in *European Law Journal*, 12 maggio 2022, 7); volendo, pure MALACARNE, *Il ricorso a strumenti investigativi a cd. contenuto tecnologico. La* Data retention *nel procedimento penale alla luce della giurisprudenza europea e della (ondivaga) giurisprudenza di merito italiana*, in *Diritto di internet*, 2021, 4, 613.

più in particolare, che, laddove determinate informazioni digitali siano idonee a consentire di trarre precise conclusioni sulla vita privata delle persone – come nel caso dei metadati relativi agli spostamenti giornalieri e ai luoghi abitualmente frequentati da un utente – l'ingerenza nei diritti tutelati dagli artt. 7 e 8 della Carta di Nizza deve qualificarsi come «grave»[36].

Per converso, tutte le volte in cui l'accesso a dati personali non consenta «di per sé, di conoscere la data, l'ora, la durata e i destinatari delle comunicazioni effettuate, né i luoghi in cui [le] comunicazioni sono avvenute», esso deve ritenersi inidoneo a disvelare le abitudini di vita di un determinato soggetto e, pertanto, l'ingerenza che comporta una conservazione di tali informazioni non può, in linea di principio, essere qualificata come «grave»[37].

Muovendo da tali considerazioni, i giudici europei hanno ricondotto nella categoria delle "intrusioni gravi" l'insieme dei «dati di traffico» telematico «suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente [...] o sull'ubicazione delle apparecchiature terminali utilizzate da quest'ultimo»[38].

Nel gruppo delle "intrusioni lievi" sono, invece, state annoverate quelle informazioni utilizzate «al solo scopo di identificare l'utente», senza consentire in alcun modo all'autorità pubblica di inferire conclusioni in merito alle telecomunicazioni effettuate dal bersaglio. Così, ad esempio, nel caso *Ministerio Fiscal*, la Corte ha qualificato in termini di ingerenza *soft* la semplice richiesta di ordinare al *provider* la trasmissione dei numeri di telefono attivati da un determinato soggetto, il relativo codice IMEI e i dati personali concernenti l'identità civile del titolare. In quest'ultima evenienza, infatti, tali contenuti non forniscono, «a parte le coordinate degli utenti» (quali, ad esempio, i loro indirizzi), «alcuna informazione sulle comunicazioni effettuate e, di conseguenza, sulla loro vita privata»[39].

Ebbene, ci pare che la divisione appena menzionata sia utile anche per quanto riguarda le prove elettroniche qui analizzate.

In questa scia, si potrebbe, più in particolare, distinguere tra accessi ai *file* di *log* "intrusivi", cioè quelli che consentono di conoscere le abitudini di vita di un soggetto, e "limitatamente intrusivi", i quali, per contro, non sarebbero idonei a incidere in maniera significativa sul diritto alla riservatezza garantito

[36] Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit., parr. 57-60.

[37] Corte giust. UE, 2 aprile 2018, *Ministerio Fiscal*, cit., par. 57; Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net e altri*, cit., par. 152 ss.

[38] Testualmente, Corte giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, cit., par. 35.

[39] Corre giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, cit., par. 34.

dalle fonti sovraordinate di diritto primario (artt. 7 e 8 Carta di Nizza, cui va aggiunto l'art. 8 C.E.D.U.) e derivato (direttive 2016/680/UE e 2002/58/CE).
Nella prima categoria, dovrebbero essere ricondotte, non solo le acquisizioni di *file* di *log* volte a tracciare comunicazioni telematiche già avvenute, ma anche quelle che forniscono dati sull'ubicazione del terminale e, in generale, tutte quelle che consentono di trarre precise conclusioni sulla vita privata del bersaglio. Si pensi, ad esempio, all'apprensione dei registri di *log* al fine di ricavare la frequenza con cui un determinato utente ha visitato un certo sito *internet*, oppure volte a mappare i suoi spostamenti nel *web* e nello spazio.
Nella seconda classe, invece, dovrebbe ricondursi la raccolta dei *file* di *log* mossa dallo scopo "statico" di identificare, unicamente, un soggetto attivo in rete. Si consideri, in via esemplificativa, l'ipotesi in cui l'autorità inquirente, individuato il *nickname* del *target*, richieda l'acquisizione dei "registri di navigazione" con l'unico obiettivo di conoscere l'identità del bersaglio intestatario del dispositivo o di un contratto con un *provider*[40].
Peraltro, va messo in luce come una precisa conferma della bontà della distinzione appena delineata si ricavi dal più volte citato regolamento UE 2023/1543.
Come si è avuto modo di accennare, tale provvedimento all'art. 3 e ai considerando 32-34 divide il più generale insieme dei "*file* di *log*" in due categorie: da un lato, quelli appresi con la mera finalità di identificare l'utente nell'ambito di un'indagine penale, i quali, determinando un'ingerenza nei diritti della persona, classificata dal legislatore europeo come "lieve", vengono fatti rientrare tra i "dati relativi agli abbonati"; da un altro, quelli utilizzati per scopi diversi, che, andando a creare un'invasione più penetrante nella sfera privata, sono collocati nella diversa categoria dei "dati di traffico".
E, se è pur vero che, come già menzionato, tale regolamento riguarda soltanto la materia della cooperazione internazionale[41], lo stesso pare comunque costituire, da subito, un importante parametro di riferimento esegetico anche per il legislatore interno; e ciò in quanto l'atto UE compie, da questa prospettiva, una sorta di cristallizzazione della giurisprudenza della Corte di giustizia in tema di conservazione e di acquisizione di dati personali.
Ma vi è di più.

[40] Per un esempio concreto, cfr. Tribunale Milano, Sez. IX, 15 giugno 2021, n. 5678, in *Dejure*.
[41] A tal proposito, il considerando n. 18 – il cui contenuto è pedissequamente recepito all'art. 1, co. 1 – prevede che il regolamento debba applicarsi «in tutti i casi transfrontalieri in cui il prestatore di servizi ha lo stabilimento designato o il rappresentante legale in un altro Stato membro [dell'Unione europea]».

Prendere a modello, quantomeno come *standard* minimo di riferimento, la richiamata fonte eurounitaria è utile anche al fine di non provocare una pericolosa discrepanza tra il livello di tutela richiesto per limitare i diritti della persona nei casi transnazionali e in quelli puramente interni. Difatti, prevedere che, a fronte della necessità di acquisire dati probatori identici, alcuni individui godano di salvaguardie inferiori solo perché i *file* di *log* sono stati richiesti a un *provider* collocato sul territorio nazionale e non a uno situato in un altro Paese dell'Unione rischierebbe di provocare frizioni, tanto con il principio di ragionevolezza, quanto con quello di non discriminazione, tutelati sia dalla Carta costituzionale, sia a livello europeo.

5. *Segue. La necessità di una modulazione proporzionata degli* standard *di tutela.* Una volta accolta la distinzione tra apprensioni di *file* di *log* più o meno intrusive, è opportuno ora soffermarsi sui diversi *standard* di tutela che devono essere riconosciuti nelle due fattispecie.
Seguendo, nuovamente, gli insegnamenti della Corte di giustizia va, anzitutto, affrontato il tema dei mezzi atti ad assicurare la proporzionalità "in astratto" della limitazione dei diritti fondamentali dell'individuo. A questo proposito, i giudici di Lussemburgo, nella loro giurisprudenza in tema di *data retention*, hanno sostenuto che le intrusioni significative nella vita privata sono ammissibili solo se circoscritte al contrasto delle «forme gravi di criminalità o per la prevenzione di gravi minacce per la sicurezza pubblica», sempreché i soggetti destinatari della misura siano stati individuati *ex ante* in maniera chiara e puntuale[42]. Al contrario, ad avviso della Corte, quelle ingerenze che non possono essere qualificate in questi termini ben potrebbero essere giustificate dall'obiettivo di prevenzione e di accertamento dei «reati in generale»[43], non essendo richiesto un elevato *standard* di gravità.
Ebbene, traslando sul piano della *log evidence* questi insegnamenti, è possibile sostenere la necessità di creare, pure da questa prospettiva, una disciplina duplice. Se la conservazione e l'apprensione di siffatte prove elettroniche, per meri scopi di identificazione, può essere autorizzata con riguardo alla generalità delle fattispecie di reato, le cose stanno diversamente per le forme più intrusive di acquisizione dei "registri del traffico telematico". In questo secondo

[42] Cfr. Corte giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, cit., par. 33; Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, cit., par. 140; Corte giust. UE, 2 aprile 2018, *Ministerio Fiscal*, cit., par. 54; Corte giust. UE, 21 dicembre 2016, *Tele 2 e Watson*, cit., par. 102; Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit., par. 60.
[43] Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, cit., par. 157; Corte giust. UE, 2 aprile 2018, *Ministerio Fiscal*, cit., par. 57.

caso, infatti, i *conditores* sono tenuti a selezionare uno specifico novero di delitti, connotati da una determinata soglia di gravità, con riferimento ai quali l'impiego di tale strumento investigativo e/o probatorio risulti ammissibile. È facile intuire come un punto di riferimento "naturale" a questo proposito non possa che essere rappresentato dall'elenco di reati oggi contenuto nell'art. 132, co. 3 del codice *privacy*[44], nonché, a livello europeo, da quello di cui all'art. 5, par. 4 del regolamento (UE) 2023/1543.

Un secondo aspetto da chiarire concerne, invece, il regime temporale di conservazione dei *file* di *log*. Anche in questo caso, infatti, la Corte di giustizia è stata chiara nello stabilire che, onde limitare al massimo le intrusioni nella sfera dei privati, «le autorità nazionali competenti sono tenute a garantire, in ciascun caso di specie, che tanto la categoria o le categorie di dati interessati, quanto la durata per la quale è richiesto l'accesso a questi ultimi, siano, in funzione delle circostanze del caso di specie, limitate a quanto è strettamente necessario ai fini dell'indagine in questione»[45].

Se un tanto è vero, è, tuttavia, noto come, anche a valle della riforma del 2021, in tema di modalità acquisitive dei tabulati telefonici o telematici, l'ordinamento italiano sia rimasto, da siffatta prospettiva, caratterizzato da una disciplina assai problematica[46], dato che il legislatore non è intervenuto sul

---

[44] Cfr. *supra*, nt. 5.

[45] Testualmente, Corte giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, cit., par. 38. Nello stesso senso, v. pure Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, cit., par. 130; Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit., par. 52.

[46] La dottrina, del resto, ha sottolineato, a più riprese, la macroscopica sproporzionalità, rispetto alle finalità perseguite, dei termini di conservazione dei metadati di traffico fissati dalla legislazione italiana. È noto, infatti, che l'operare congiunto dell'art. 132, co. 1, codice *privacy* e l'art. 24, l. 20 novembre 2017, n. 167 obblighi, di fatto, i *provider* a stoccare dette informazioni per un periodo di 72 mesi a decorrere dalla data di avvenuta comunicazione. Cfr., in senso critico rispetto all'attuale regolamentazione, ANDOLINA, *La raccolta dei dati relativi alla localizzazione del cellulare ed al traffico telefonico tra inerzia legislativa e supplenza giurisprudenziale*, cit., 14-16; LASAGNI, *Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della* privacy, cit., 9; FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof Filippi*, cit.; FLOR-MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico*, cit., 54, 89-91; FORMICI, *"*The three Ghosts of data retention"*: passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Rivista AIC*, 2022, 1, 139; SIGNORATO, *Novità 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, 160; e, volendo, MALACARNE-TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia*, cit., 17. Pure il Garante per la protezione dei dati personali, come risaputo, ha messo in luce più volte la necessità di un intervento normativo volto a ridurre sensibilmente i tempi di archiviazione dei dati di traffico: cfr., ad es., GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, 10 settembre 2021; ID., *Parere*

punto, continuando a prevedere limiti cronologici di conservazione particolarmente lunghi, i quali superano finanche quelli previsti dall'art. 6 della direttiva 2006/24/CE, dichiarata, anche per questo motivo, del tutto invalida dai giudici di Lussemburgo[47]. Alla luce di ciò, l'auspicio non può che essere quello di una correzione di rotta sul punto: è, infatti, indispensabile ridurre, in generale, i termini di stoccaggio dei dati personali (quantomeno a una durata inferiore rispetto a quella contemplata dalla c.d. "direttiva Frattini"[48]) attraverso la creazione di una disciplina capace di limitare davvero allo stretto indispensabile l'invasione nella sfera giuridica degli individui.

Un terzo aspetto delicato concerne, infine, la determinazione dello *standard* di garanzie da rispettare con riguardo alla fase acquisitiva delle prove elettroniche in esame. Come si è avuto modo di accennare in premessa, la Corte di Lussemburgo ha stabilito la necessità che l'apprensione dei dati di traffico o relativi all'ubicazione sia autorizzata solo da un «giudice o un'autorità amministrativa indipendente»[49], a cui spetta il compito di realizzare un vaglio di proporzionalità in concreto rispetto all'invasione nella riservatezza della persona. Sviluppando tale assunto, i giudici europei, nella citata sentenza *H.K.*, hanno, per di più, fornito una sorta di "interpretazione autentica" di siffatta locuzione, precisando come, laddove a essere appresa sia tale categoria di informazioni, detta qualifica possa essere riconosciuta solamente a un organo che goda d'indipendenza rispetto al potere politico, assolva i «propri compiti in modo obiettivo e imparziale» e, soprattutto, si collochi, dal punto di vista ordinamentale e processuale, in «posizione di neutralità [e terzietà] nei confronti delle parti del procedimento penale»[50].

Tenuto conto di ciò, sembra necessario affermare che per tutte le acquisizioni dei *file* di *log*, idonee a determinare un'intrusione grave nei diritti di cui agli artt. 7 e 8 della Carta di Nizza (cioè, quelle concernenti dati esterni a comuni-

---

sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, 22 maggio 2018.

[47] Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit.

[48] L'art. 6 della direttiva 2006/24/CE, come si ricorderà, prevedeva un periodo di conservazione variabile, da sei mesi a due anni.

[49] V., *in primis*, Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit., par. 62; e, in seguito, Corte giust. UE, 21 dicembre 2016, *Tele 2 e Watson*, cit., par. 120; Corte giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, cit., par. 51 ss.; Corte giust. UE, 5 aprile 2022, *Commissioner of An Garda Síochána e. a.*, cit., par. 106. Sui riflessi nel panorama nazionale del *dictum* della Corte, con specifico riguardo al ruolo ricoperto dal pubblico ministero nella fase di acquisizione dei tabulati telefonici, v. GAETA, *Consensi e dissensi sulla indipendenza del p.m. (a proposito del potere di acquisire i tabulati telefonici)*, in *questa Rivista web*, 7 ottobre 2021.

[50] Cfr., per le ultime citazioni, Corte giust. UE, 2 marzo 2021, *H.K. c. Prokuratuur*, cit., parr. 53, 54.

cazioni telematiche già avvenute, ma anche quelle che forniscono dati sull'ubicazione del terminale e, in generale, che consentono di trarre precise conclusioni sulla vita privata del bersaglio), vada necessariamente rispettato un analogo *standard* di tutela. Ad autorizzare *ex ante* o a convalidare, in un limitato periodo di tempo, *ex post*, l'apprensione della prova elettronica dovrà, invero, per forza essere un giudice, così come già oggi previsto dall'art. 132 codice *privacy*. Una precisa conferma di tale tesi si ricava, d'altra parte, dall'art. 4 e dal considerando n. 36 del regolamento (UE) 2023/1543, i quali, per l'appunto, prevedono che soltanto un giudice possa emettere un ordine europeo di produzione per ottenere dati sul traffico.

È, invece, più complesso comprendere quale debba essere la disciplina nel caso in cui la richiesta di apprensione dei *file* di *log* sia volta unicamente a identificare un utente sulla rete. Trattandosi pur sempre di un'intrusione nella sfera giuridica protetta, tra l'altro, dagli artt. 7 e 8 della Carta, i quali prevedono la necessità di un controllo di un'"autorità indipendente", si potrebbe essere tentati di estendere gli insegnamenti di *H.K.* anche a tale fattispecie, richiedendo, pertanto, un avallo giurisdizionale della misura.

Una tale soluzione non pare, tuttavia, per forza imposta al legislatore interno, per diversi ordini di ragioni.

In prima battuta, va, infatti, rilevato che la sentenza *H.K.* si è occupata di invasioni gravi nella riservatezza individuale e non di ingerenze di tipo lieve; di modo che essa non sembra poter rappresentare un precedente necessariamente vincolante per la fattispecie dell'acquisizione delle evidenze in esame (si legga, quelle "lievi"), come quelle per meri fini identificativi.

In secondo luogo, anche un ragionamento basato sul più volte menzionato principio di proporzionalità sembra giustificare la scelta di disciplinare, in modo diverso, le due fattispecie. Difatti, muovendo dalla natura qualitativamente più limitata nell'invasione nella sfera del singolo, che si verifica nel caso di *file* di *log* richiesti per soli fini di identificazione, si può giungere alla conclusione per cui la loro acquisizione possa avvenire a seguito di un provvedimento motivato del pubblico ministero. E ciò, perlomeno, in un ordinamento, come quello italiano, in cui tale soggetto è istituzionalmente caratterizzato da una piena indipendenza funzionale rispetto all'esecutivo. Per contro, onde salvaguardare a livello tanto formale, che sostanziale, lo spirito di quanto previsto dall'art. 8, par. 3, della Carta di Nizza, un atto investigativo di questo tipo non ci pare poter essere comunque emesso, in modo autonomo, dalla polizia giudiziaria.

A ben vedere, optare per una tale soluzione, altro non significa che estendere

al vaglio di proporzionalità in concreto un ragionamento coerente rispetto a quello applicato dalla stessa Corte di giustizia per quanto concerne quello di proporzionalità in astratto: così come le ingerenze lievi nella riservatezza sono ammesse per una fascia più ampia di reati, ci pare che le stesse possano essere autorizzate da un soggetto sì sempre indipendente, ma diverso dal giudice, quale un pubblico ministero, laddove tale organo, per come strutturato a livello ordinamentale, goda di garanzie tali da essere autonomo istituzionalmente e funzionalmente dagli altri poteri.

A tal proposito, è, d'altra parte, utile ricordare come una soluzione simile a quella qui proposta, tesa a delineare uno *standard* di tutela differenziato a seconda della gravità dell'ingerenza, sia stata già intrapresa da altri Stati dell'Unione europea. La mente corre, in particolare, al sistema spagnolo e, in specie, all'art. 588-*ter* lett. *m*) della *Ley de Enjuiciamiento Criminal*, ove si prevede una procedura di "acquisizione speciale" allorquando vengano in rilievo dati informatici, inidonei a disvelare le condizioni personali dei cittadini. La disposizione, rubricata «*Identificación de titulares o terminales o dispositivos de conectividad*», stabilisce che il *ministerio fiscal*, qualora risulti necessario «*conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación*», possa ottenere questi dati rivolgendosi direttamente al *provider*, sul quale, peraltro, grava l'obbligo, penalmente sanzionato, di «*cumplir el requerimiento*».

Ma, soprattutto, una precisa conferma della fondatezza di tale lettura si ricava, anche in questo caso, dal regolamento e-*evidence*. Le già menzionate disposizioni del considerando n. 36, da leggersi assieme all'art. 4, stabiliscono, infatti, che, proprio in ragione della natura meno invasiva delle istanze concernenti dati richiesti al solo scopo di identificare l'utente, esse possono essere emesse o convalidate, alternativamente, da un «giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero». Di modo che, se il legislatore europeo ha considerato possibile bilanciare, in una fattispecie analoga, in un modo meno rigido le esigenze di protezione del singolo con quelle di contrasto alla criminalità, ci pare che un'operazione di questo tipo possa essere intrapresa anche a livello nazionale.

6. *Conclusioni*. Nel corso della presente analisi, si è avuto modo di dimostrare come la mancanza di riferimenti normativi espliciti al tema dell'acquisizione dei *file* di *log* e l'indeterminatezza di alcune nozioni di base rendano il vigente panorama interpretativo interno assai problematico. Il che, evidentemente, non può che produrre un effetto ben determinato: quello di

lasciare, di fatto, anche da questa prospettiva, alla giurisprudenza il compito di individuare, in modo creativo, le linee della regolamentazione della materia, con tutto ciò che ne consegue in termini di frizioni con il principio costituzionale di legalità processuale (art. 111, co. 1 Cost.).

Sotto tale profilo, dunque, il giudizio sulla riforma apportata dal d.l. 132/2021 non può che essere negativo. Nonostante essa sia intervenuta a valle di innumerevoli modifiche precedenti[51], il Governo e il Parlamento hanno perso, ancora una volta, l'occasione per risolvere i plurimi nodi problematici che affliggono la disciplina italiana della *data retention* in particolare e, più in generale, dei mezzi di ricerca della prova tecnologici. Non è un mistero, del resto, che il nostro ordinamento continui a non disciplinare un ampio novero di forme di *digital investigations* oggi essenziali per il contrasto alla criminalità[52].

È chiaro, peraltro, che una parte della responsabilità dello *status quo* si deve anche agli errori e alle timidezze del legislatore eurounitario, il quale, dopo l'invalidazione della direttiva 2006/24/CE da parte della Corte di giustizia[53], ha incontrato, a sua volta, notevoli difficoltà nel prendersi la responsabilità politica di regolare, a livello normativo, il fenomeno *de quo*.

Tuttavia, a seguito dello sviluppo della copiosa giurisprudenza dei giudici del Lussemburgo degli ultimi anni, nonché dell'approvazione, da parte dell'Unione, del regolamento *e-evidence*, a cui va aggiunto, sul piano del Consiglio d'Europa, il secondo protocollo addizionale alla Convenzione di Budapest sul Cybercrime[54], il quadro è oggi cambiato. Tali fonti forniscono,

---

[51] Per una rassegna, v. F.R. DINACCI, *La localizzazione mediante celle telefoniche tra limiti costituzionali e comunitari*, cit., 473, nt. 30.

[52] Il riferimento corre, ad esempio, al pedinamento GPS, alle videoriprese investigative e al *virus trojan* impiegato in modalità diversa rispetto alla semplice captazione ambientale. In generale, sulla necessità di un intervento legislativo volto a regolamentare queste nuove strumentazioni investigative, v., pur con differenti accentuazioni e prospettive di riforma, BENE, *Il pedinamento elettronico: tecnica investigativa e tutela dei diritti fondamentali*, in *Le indagini atipiche*, cit., 443 ss.; GIALUZ, *Premessa*, in *Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*, in *Diritto di internet*, 2020, Suppl. al n. 3, 7; MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. Pen.*, 2015, 2, 789 ss.; MIRAGLIA, *Il "*Trojan *(non) di Stato": una disciplina da completare*, in *Proc. pen. giust.*, 2023, 5, 1227 ss.; NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano, 2020, *passim*.; NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano, 2021, 317 ss.; ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, 3, 1153.

[53] Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cit.

[54] "Secondo protocollo addizionale alla Convenzione sulla criminalità informatica (Convenzione di Budapest), volto a rafforzare la cooperazione e la divulgazione delle prove elettroniche", 12 maggio 2022. Per una compiuta disamina del contenuto, v. i contributi presenti nel numero "*Speciale sul Secondo*

infatti, materiale copioso per regolare, finalmente, in modo adeguato il fenomeno delle evidenze digitali.
L'auspicio è, pertanto, che il legislatore nazionale si renda conto di ciò e compia un netto cambio di passo, anche prendendo spunto dall'operato di altri ordinamenti nazionali[55].
Come si è già accennato, per quanto concerne i dati esterni alle comunicazioni, i *conditores* dovrebbero, in tale contesto, completare la riforma del 2021, fissando, in particolare, un regime cronologico proporzionato di stoccaggio dei dati, atto a limitare al minimo necessario la durata dell'ingerenza nella sfera giuridica del singolo.
In secondo luogo, si dovrebbe stabilire una nuova definizione di "traffico telematico", aggiornata alle più recenti indicazioni provenienti dalla Corte di giustizia e dal regolamento *e-evidence*, che riconosca esplicitamente il fatto che anche i dati di navigazione, in grado di compiere un tracciamento capillare delle attività di un individuo, rientrino in tale categoria, indipendentemente dalla sussistenza di una comunicazione in senso stretto.
Sul fronte che qui rileva maggiormente, infine, l'auspicio è che venga introdotta una previsione *ad hoc* per quanto concerne l'acquisizione dei *file* di *log* per scopi meramente identificativi, la quale dovrebbe specificare, tanto il soggetto chiamato ad autorizzare la misura (che, come si è avuto modo di vedere, ci pare poter essere anche il pubblico ministero, ma non la polizia giudiziaria), quanto i tempi specifici di conservazione di tali dati da parte dei *service provider*.

Protocollo addizionale alla Convenzione di Budapest", pubblicato in *Dir. pen. proc.*, 2022, 8, 1017 ss.

[55] Il sistema processuale spagnolo, da questo punto di vista, è senz'altro all'avanguardia sul versante della regolamentazione dei moderni strumenti intrusivi impiegati nella fase delle indagini preliminari. Il riferimento corre alla *Ley Oganica* 5 ottobre 2015, n. 13, con la quale il legislatore ha modificato la *Ley de Enjuiciamiento Criminal* con il dichiarato obiettivo di disciplinare «*las medidas de investigación tecnológica*» e, contestualmente, rafforzare «*las garantías procesales*» dei soggetti coinvolti nell'accertamento. Degna di nota è, in specie, la scelta di cristallizzare all'art. 588-*bis*-a i principi generali di «*especialidad*, *idoneidad*, *excepcionalidad*, *necesidad* y *proporcionalidad*» che devono sorreggere qualsivoglia mezzo di ricerca della prova a contenuto digitale. Per una panoramica sui contenuti della legge, v. BUENO DE MATA, *Las digilencia de investigacion penal en la cuarta revolucion industrial. Principios teoricos y problemas practicos*, Cizur Menor, 2019; PEREIRA PUIGVERT, *Las medidas de investigación tecnológicas y su injerencia en la privacidad de las personas y la protección de datos personales*, in *Investigación y prueba en los procesos penales de España e Italia*, diretto da Villar Fuentes, Cizur Menor, 2019, 297 ss.