SISTEMA PENALE

FASCICOLO 5/2020

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezo "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2020, p. 5 ss.

5/2020

DATI ESTERNI ALLE COMUNICAZIONI E PROCESSO PENALE: QUESTIONI ANCORA APERTE IN TEMA DI *DATA RETENTION*

Nota a Cass., Sez. III, 19 aprile 2019 (dep. 23 agosto 2019), n. 36380, Pres. Andreazza, Rel. Semeraro

di Isadora Neroni Rezende

La disciplina della data retention *costituisce ad oggi uno dei terreni di più delicato bilanciamento tra diritti fondamentali e uso dei mezzi tecnologici a fini repressivi. Sullo sfondo delle ormai note pronunce della Corte di giustizia sul tema, il presente contributo commenta la sentenza n. 36380 del 2019, che vede la Corte di Cassazione riconfermare la compatibilità dell'art. 132 cod.* privacy *con gli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Unione Europea. Dopo aver esaminato i profili più problematici dell'attuale disciplina dell'art 132 cod.* privacy, *si riflette sulla necessità di ripensare la ben nota distinzione tra dati esterni e contenuto delle comunicazioni. In conclusione, l'analisi si sposta sul ruolo del principio di proporzionalità nella complessa materia della* data retention.

1. Un'occasione mancata?

Ancora una volta, la Corte di Cassazione si sottrae alla resa dei conti con la tormentata disciplina della *data retention*, uno dei terreni di più delicato bilanciamento tra diritti fondamentali e uso dei mezzi tecnologici a fini repressivi[1]. Con la sentenza n. 36380 del 2019, difatti, la Corte ha nuovamente ribadito il suo precedente orientamento[2],

[1] Per un'attenta analisi del tema della *data retention* e delle libertà fondamentali incise da tale fenomeno, v. MARCOLINI S., *L'istituto della* data retention *dopo la sentenza della Corte di Giustizia del 2014*, in *Cybercrime* (a cura di Cadoppi A., Canestrari S., Manna A.), Utet Giuridica, 2019, pp. 1579-1582.

[2] Va evidenziato che la sentenza in commento riprende integralmente gli approdi cui la sezione V della

negando ogni profilo di incompatibilità dell'art. 132 cod. *privacy* con gli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Unione europea (di seguito: la Carta), così come interpretati dalla Corte di giustizia nelle ormai storiche sentenze *Digital Rights Ireland*[3] e *Tele 2/Watson*[4].

Nel caso specifico, uno dei ricorrenti – coimputato in un procedimento per traffico di stupefacenti – lamentava l'inutilizzabilità *ex* art. 191 c.p.p. dei dati emergenti dal tabulato telefonico relativo ad un'utenza a lui attribuita; tali dati, secondo la ricostruzione dei giudici di appello, lo avrebbero infatti collocato nel luogo in cui si presumeva fosse avvenuta la cessione della sostanza stupefacente in questione. L'inutilizzabilità, nell'opinione del ricorrente, si imponeva come logica conseguenza dell'incompatibilità dell'art. 132 cod. *privacy* con la normativa eurounitaria in materia di diritto alla *privacy* e alla protezione dei dati personali.

In particolare, le doglianze del ricorrente si articolavano su un duplice profilo. Da un lato, la disposizione censurata sarebbe stata in contrasto con il principio di limitazione delle finalità, non specificando le tipologie di reati per le quali l'acquisizione dei dati fosse autorizzata; dall'altro, sul piano delle modalità procedimentali di acquisizione, si lamentava l'inopportunità di attribuire al pubblico ministero la scelta di ricorrere a questo particolare mezzo di indagine. Come anticipato, nessuna delle tesi proposte dal ricorrente ha ricevuto accoglimento da parte della Corte.

Volendo circoscrivere fin da subito il perimetro d'indagine del presente contributo, è opportuno evidenziare che l'analisi della pronuncia in epigrafe si limiterà a ripercorrere i soli snodi motivazionali relativi agli elementi di incompatibilità rilevati dal ricorrente: ulteriori, ma non meno importanti, profili di problematicità dell'art. 132 non saranno dunque oggetto di una specifica trattazione[5]. Ciononostante, i rilievi della Corte saranno di spunto per riflettere, alla luce del rinnovato contesto tecnologico, sulla ben nota distinzione tra dati esterni e contenuto delle comunicazioni, nonché sul ruolo del principio di proporzionalità nella complessa materia della *data retention*.

Suprema Corte era già pervenuta in occasione della sentenza n. 33851 del 2018.

[3] CGUE, 8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12, annotata da FLOR R., *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd. "*data retention*" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. Pen. Cont. – Riv. trim.*, 2014, 2, pp. 178-188.

[4] CGUE, 21 dicembre 2016, *Tele 2/Watson*, cause riunite C-203/15 e C-698/15, con nota di POLLICINO O., BASSINI M., *La Corte di giustizia ed una trama ormai nota: la sentenza* Tele 2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. pen. cont.*, 9 gennaio 2017.

[5] Ad esempio, non saranno oggetto di analisi gli obblighi, in capo ai fornitori di servizi, relativi agli standard di sicurezza dei dati. Invero, secondo quanto statuito dalla Corte nella sentenza *Digital Rights Ireland*, i fornitori di servizi di telecomunicazione non possono essere autorizzati a tener conto di considerazioni di natura economica nel predisporre le misure tecnico-organizzative di sicurezza dei dati (v. §§ 66-68 della sentenza sopracitata). Inoltre, non saranno oggetto di trattazione le questioni relative alle tempistiche di conservazione dei dati, per cui si rinvia invece alle osservazioni di SIGNORATO S., *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, pp. 153-161.

2. Le ragioni poste dalla Corte di Cassazione a fondamento della propria decisione.

Prima di addentrarci nel merito della questione, non possono esser taciuti alcuni rilievi preliminari sulle considerazioni svolte dalla Corte di Cassazione quanto alla pertinenza della giurisprudenza sovranazionale evocata al caso della disciplina italiana in esame. La Corte ha difatti la premura di distinguere il contesto normativo italiano da quello austriaco e irlandese, i quali erano stati oggetto di scrutinio della Corte di giustizia nel caso *Digital Rights.* In particolare, la Corte di Cassazione sostiene che tali ordinamenti fossero privi – al contrario di quello italiano – di una regolamentazione sull'accesso e la conservazione dei dati[6]. Tale asserzione risulta tuttavia difficilmente condivisibile sia sul piano fattuale[7], sia su quello metodologico. Rispetto a quest'ultimo profilo, infatti, la Corte sembra affermare che, ai fini della compatibilità con i principi posti dagli ordinamenti sovranazionali in tema di *privacy* e protezione dei dati personali, sia sufficiente accertare la mera esistenza formale di una specifica disciplina sull'accesso e conservazione dei dati. Orbene, è più che noto che in materia di diritti fondamentali, il giudice preposto al controllo non può accontentarsi di verificare l'esistenza di una base legale limitativa dei diritti, ma deve estendere il proprio scrutinio anche al piano "sostanziale"[8], dovendo altresì esaminare la proporzionalità dell'ingerenza apportata ai diritti protetti. Come vedremo, tuttavia, dal percorso motivazionale della Corte difficilmente emergono profili di analisi sostanziale della disciplina italiana nella materia esaminata. Al contrario, essa sembra faticare nel dare il giusto peso alle questioni poste, finendo per far suoi gli argomenti già adottati in precedenza dai giudici interni, sia di merito, sia di legittimità[9].

3. Non basta una regolazione generica per ottemperare ai requisiti pretesi dai principi europei.

Ma veniamo ora al nucleo della questione. Tra i primi rilievi del ricorrente vi era l'eccessiva genericità dei fini posti alla base degli obblighi di conservazione dei dati esterni alle comunicazioni. Nell'attuale disciplina dell'art. 132 cod. *privacy*, in effetti, essi vengono individuati nelle esigenze legate all'accertamento e repressione dei «reati»[10], senza che sia indicata una soglia di gravità che limiti l'alveo delle fattispecie di rilevanza penale per cui l'accesso ai dati possa essere autorizzato.

Contrariamente a quanto sostenuto dalla Corte, vi sono seri argomenti per dubitare che la disciplina italiana di riferimento sia compatibile con gli articoli 7, 8 e 52

---

[6] Cass. pen., sez. III, n. 36380/2019, punto 3.5.

[7] L'affermazione per cui l'Irlanda e l'Austria fossero prive di qualsivoglia disciplina sulla conservazione e acquisizione dei dati esterni alle comunicazioni viene smentita da una veloce lettura della sentenza *Digital Rights Ireland*, v. § 17 per l'Irlanda, e il § 19 per l'Austria.

[8] RUGGIERI F., *Data retention e giudice di merito penale. Una discutibile pronuncia,* in *Cass. pen.*, 2017, 6, p. 2486.

[9] Lo esprime efficacemente LUPARIA L., Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di Internet*, 2019, 4, p. 762.

[10] Art. 132, comma 1, del d. lgs. 196/2003.

della Carta[11]. Già in *Digital Rights,* la Corte di giustizia aveva censurato la formulazione della direttiva *data retention* nella misura in cui questa lasciava agli Stati membri un'eccessiva discrezionalità nella definizione della cerchia di reati gravi per cui potesse essere legittimato l'accesso ai dati. Simile carenza, come noto, aveva portato, assieme ad altre ragioni, a dichiarare invalida la fonte normativa. Secondo la Corte di Lussemburgo, l'eccessiva indeterminatezza della disciplina della direttiva *data retention* poneva il rischio di un indebito allargamento dell'ambito di applicazione della misura di conservazione, che rischiava di essere utilizzata – a livello nazionale – anche per il perseguimento di fattispecie penali di scarsa rilevanza. Il tema della soglia di gravità dei reati che costituiscono il presupposto dell'acquisizione dei dati è stato poi oggetto di ulteriore elaborazione nella sentenza *Tele 2/Watson*. In quest'ultima pronuncia la Corte, tornando sul problema, ha infatti ribadito che, in applicazione del principio di proporzionalità, gli obiettivi perseguiti dalla normativa di *data retention* devono essere calibrati alla gravità dell'ingerenza prodotta nei diritti fondamentali interessati; di conseguenza, l'accesso ai dati personali a finalità di contrasto alla criminalità non può che essere limitato al perseguimento dei soli reati gravi[12].

Alla luce di ciò, pare molto difficile sostenere che l'attuale formulazione dell'art. 132 cod. *privacy* sia compatibile con i principi enunciati dalla Corte di giustizia. Come riconosciuto dalla stessa Suprema Corte, la disciplina nazionale sull'acquisizione dei dati esterni alle comunicazioni non è in alcun modo circoscritta in ordine alle tipologie di reato oggetto di indagine o di accertamento. Ciononostante, nell'ottica della Corte, il mero riferimento alle «finalità di repressione dei reati» sembra di per sé essere sufficiente a negare ogni ipotesi di contrasto della normativa nazionale con quella eurounitaria.

Nelle sue considerazioni, tuttavia, la Cassazione non solo omette di considerare adeguatamente i rilievi dei giudici del *Kirchberg* nella giurisprudenza da lei stessa citata, ma tralascia altresì qualsiasi riferimento al canone di proporzionalità. La centralità di questo principio, difatti, già espresso come visto in *Digital Rights*, è stata ribadita in una recente pronuncia della Corte di giustizia, sempre in tema di acquisizione di dati esterni delle comunicazioni elettroniche. Nella sentenza *Ministerio Fiscal*[13], la Corte del Lussemburgo ha infatti trasposto i principi già consolidati nella sua giurisprudenza anteriore al particolare caso dell'accesso ai dati che consentono di identificare anagraficamente i titolari di carte SIM attivate con il codice IMEI di un telefono cellulare rubato. Nel caso di specie, la Corte si è premurata di distinguere questa particolare ingerenza da quelle già esaminate nei casi *Digital Rights* e *Tele 2/Watson.* In effetti,

---

[11] Lo sostiene, *inter alia,* MARCOLINI S., *L'istituto della* data retention, pp. 1594-1596. La strada da percorrere, secondo l'Autore, risiederebbe nella declaratoria di inutilizzabilità dei dati ottenuti tramite accesso ai tabulati, fondata sul supposto contrasto dell'atto di indagine con il diritto eurounitario. Si auspicava, inoltre, che la Corte di Cassazione – quale organo giurisdizionale di ultima istanza – sollevasse alla prima occasione utile una domanda pregiudiziale *ex* art. 267 TFUE alla Corte di giustizia, al fine di acclarare la reale compatibilità dell'art. 132 d. lgs. 196/2003 con gli artt. 7, 8 e 52 della Carta. Sappiamo che, nella sentenza in commento, tale strada è stata invece esclusa dai giudici di legittimità, i quali hanno ritenuto che tale necessità non sussistesse nel caso di specie (cfr. Cass. pen., sez. III, n. 36380/2019, punto 3.1).

[12] CGUE, *Tele 2/Watson*, § 115.

[13] CGUE, 2 aprile 2018, *Ministerio Fiscal*, C-207/16.

un'operazione di accesso ai dati che abbia il solo scopo di collegare determinate carte SIM all'identità dei loro utilizzatori non implica, per il suo carattere circoscritto, un'intrusione nella sfera privata comparabile a quella che si produrrebbe con un trattamento incrociato dei dati relativi alle comunicazioni effettuate dagli utenti stessi[14]. Non potendo i soli dati anagrafici dell'utente fornire alcuna indicazione sulla data, l'ora, la durata, i destinatari delle comunicazioni effettuate con le carte SIM in questione, l'ingerenza provocata nei diritti alla *privacy* e alla protezione dei dati personali non può dirsi particolarmente penetrante. Di conseguenza, secondo la Corte, non occorre una soglia di rilevante gravità in relazione ai reati per cui una tale operazione di accesso può essere consentita[15].

Queste ultime considerazioni finiscono per rinforzare, inevitabilmente, la tesi qui proposta. Posto che il legislatore nazionale si astiene dal circoscrivere le fattispecie di reato che possono costituire il presupposto dell'operazione di accesso ai dati, i provvedimenti disposti *ex* art. 132 cod. *privacy* non possono considerarsi conformi al principio di proporzionalità ogniqualvolta essi riguardino l'integralità – o perlomeno una parte consistente – delle informazioni presenti sul tabulato. In questi casi, difatti, la compressione apportata al diritto alla riservatezza è molto significativa e richiede di essere giustificata da esigenze di accertamento di una fattispecie che attinga ad un certo livello di gravità. All'opposto, qualora la tipologia delle informazioni richieste non siano tali da permettere di ricostruire nel dettaglio la vita privata dell'interessato, la misura di accesso ai dati potrà dunque essere autorizzata anche nel quadro di procedimenti relativi a reati di scarsa rilevanza, non dovendo essere "supportata" da particolari necessità investigative.

In considerazione di tutto ciò, è ragionevole sostenere che la definizione dei «reati-presupposto»[16] del provvedimento acquisitivo sia di particolare urgenza nel caso italiano. Volendo infatti effettuare un giudizio in concreto sulla prassi applicativa dell'art. 132 cod. *privacy*, è necessario evidenziare come i diversi gestori di servizi siano soliti rispondere alle richieste di accesso secondo le proprie esigenze organizzative, fornendo i tabulati in un formato da loro confezionato, il quale può variare sensibilmente anche in relazione al dettaglio delle informazioni ivi riportate[17]. Il ventaglio dei dati contenuti nel tabulato sembra nella pratica esser dettato dall'organizzazione interna dei gestori, piuttosto che dalle effettive esigenze conoscitive degli organi inquirenti.

Per di più, posto che l'organo legittimato alla richiesta di acquisizione dei metadati viene identificato, nel nostro ordinamento, nel pubblico ministero, non pochi dubbi possono essere sollevati sul fatto che l'accesso ai dati venga – di volta in volta – limitato a quanto strettamente necessario ai bisogni delle attività di accertamento[18]. Sotto questo profilo, le note prassi di motivazioni apparenti o di comodo relative ai

---

[14] Ibid., §§ 60-61.
[15] Ibid., § 62.
[16] L'espressione è di FLOR R., *La Corte di giustizia*, cit., p. 190.
[17] REALE P., *I dati telefonici e telematici per l'autorità giudiziaria: la necessità di convergere su modelli di dati e procedure condivise*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, nn. 1-2, p. 335.
[18] Sul punto, v. *infra* par. 4.

provvedimenti di acquisizione[19] lasciano ben poche speranze quanto alla sussistenza, nella pratica giudiziaria, di un effettivo giudizio di proporzionalità *ex ante* sulla quantità e la tipologia di informazioni da acquisire.

Orbene, in assenza di una definizione dei reati-presupposto per i quali l'accesso ai dati può essere autorizzato, l'ingerenza nei diritti fondamentali provocata da questo particolare mezzo di indagine finisce per risultare particolarmente significativa nel caso di reati di scarsa gravità. Contrariamente a quanto sostenuto dalla Cassazione, la semplice enunciazione delle finalità di repressione dei reati non può in alcun modo bastare a garantire la conformità della disciplina interna al diritto dell'Unione. Tutt'al più, sarebbe più coerente immaginare un sistema che ricalchi il previgente "doppio binario"[20], un modello in cui le modalità di accesso ai dati non siano calibrate solo in relazione alle relative tempistiche di conservazione[21], ma anche alla quantità di informazioni estraibili dal tabulato stesso.

4. L'intervento del pubblico ministero: un'autorità veramente indipendente nel quadro dei principi dell'Unione?

Sul piano procedurale, la scelta dell'organo preposto all'acquisizione dei dati telefonici e telematici ha da sempre rappresentato uno dei punti più delicati della disciplina italiana sulla *data retention*. Ancor prima dell'intervento del legislatore con il d. lgs. 196/2003, la questione era stata oggetto – ormai oltre vent'anni fa – di contrastanti pronunce della Corte Costituzionale da un lato[22], e delle Sezioni Unite della Corte di

[19] La giurisprudenza sottolinea come l'obbligo motivazionale a sostegno del provvedimento acquisitivo possa dirsi adempiuto anche attraverso l'uso di "espressioni sintetiche", v. MARCOLINI S., *L'istituto della* data retention, cit., p. 1584. In particolare, l'Autore menziona un caso in cui la Corte di Cassazione ha ritenuto sufficientemente motivato il provvedimento che invocava esclusivamente l'assoluta necessità di acquisire i dati al fine del proseguimento delle indagini (cfr. Cass. pen., sez. I, n. 37212/2014).

[20] Sul punto, v. *infra*, par. 4.

[21] Per lungo tempo, la disciplina della *data retention* italiana è stata ispirata ad una struttura bifasica, la quale prevedeva diversi limiti temporali e condizioni procedurali di accesso a seconda della fattispecie penale oggetto d'indagine o accertamento. Secondo la disciplina predisposta dalla l. 45/2004 – che aveva convertito, con significative modifiche, l'assetto del d.l. 354/2004 – l'acquisizione dei dati *ex* art. 132 cod. *privacy* poteva essere autorizzata nei primi 24 mesi per tutte le tipologie di reato (cd. dati recenti); per i successivi 24 mesi l'accesso era invece legittimato nei soli procedimenti relativi ai reati di cui all'art. 407, comma 2, lettera a), c.p.p., nonché in quelli relativi ai delitti in danno ai sistemi informatici o telematici. Il sistema del doppio binario è poi sopravvissuto alla riforma del d.l. 144/2005 (cd. decreto Pisanu), sebbene venisse ormai ritenuto sufficiente l'intervento del pubblico ministero – e non del giudice, come nella previgente disciplina – per l'acquisizione dei dati cd. recenti. L'architettura bifasica del sistema è stata infine accantonata con la riforma introdotta dal d. lgs. 109/2008 – la quale ha trasposto nel nostro ordinamento la direttiva 2006/24/UE – coerentemente con l'eliminazione del provvedimento autorizzativo del giudice, e la generalizzazione dell'intervento del pubblico ministero nella procedura acquisitiva dei dati. Per un'ampia ricostruzione dell'evoluzione della disciplina dell'art. 132 cod. *privacy*, si veda, *inter alia*, RICCARDI M., *Dati esteriori delle comunicazioni e tabulati di traffico*, in *Dir. pen. cont. – Riv. trim.*, 3, 2016, pp. 156-189.

[22] Corte Cost., sent. n. 81/1993.

Cassazione dall'altro[23]. Punto di partenza della riflessione sul tema – all'epoca, ancora tutta interna al nostro ordinamento – era rappresentato dalla possibilità di estendere la tutela predisposta dall'art. 15 Cost. anche ai dati esteriori al colloquio telefonico. La soluzione prevalsa dopo un intenso dibattito – la cui ricostruzione esula dall'ambito di questo contributo[24] – fa ancora oggi perno su un'interpretazione estensiva della norma costituzionale di riferimento. In sostanza, la tutela accordata dall'art. 15 Cost. è ritenuta idonea a ricomprendere l'interesse a tenere riservata l'informazione relativa al fatto di comunicare con una persona in un determinato momento (pur senza apprendere il contenuto della conversazione); di conseguenza, anche l'acquisizione dei dati esteriori sulle comunicazioni richiede un provvedimento motivato dell'autorità giudiziaria, locuzione nella quale – è ben noto – deve essere compreso il pubblico ministero.

Certo non si può dubitare dell'inclusione del magistrato dell'accusa nel concetto costituzionale di «autorità giudiziaria»[25]; tuttavia, ha senso interrogarsi, a distanza di così tanto tempo da quelle pronunce, sull'opportunità (se non proprio la necessità) di attribuire al giudice *stricto sensu* la scelta di disporre questo particolare mezzo di indagine. Nel quadro normativo vigente, sembra difficile sviluppare una riflessione corretta sul punto in termini prettamente "interni"; l'irrompere infatti delle fonti sovranazionali nel processo penale – specialmente nel contesto post-Lisbona – impone oggi all'interprete di effettuare un costante vaglio di conformità della disciplina nazionale con gli *standard* di protezione dei diritti fondamentali posti dall'ordinamento dell'Unione, nonché da quello convenzionale.

Occorre dunque prendere in considerazione le fonti europee, a cominciare da quelle dell'Unione, che ha dettato una vasta regolazione della materia. Anzitutto, va ricordato l'art. 8(3) della Carta, il quale dispone che le regole in materia di trattamento di dati personali siano sottoposte al controllo di un'autorità indipendente[26]. In applicazione di questa norma, nonché dello stesso principio di proporzionalità, in *Digital Rights* la Corte di giustizia ha statuito che la richiesta di accesso ai dati sulle comunicazioni debba essere sottoposta al controllo preventivo di un giudice, o di un'autorità amministrativa indipendente ai sensi del diritto nazionale[27]. Nel definire cosa si debba intendere per «autorità indipendente» soccorre poi la giurisprudenza della

---

[23] Cass. pen., sez. un., 13 luglio 1998, Gallieri, con nota di CALAMANDREI I., *Acquisizione di dati esteriori di una comunicazione ed utilizzazione delle prove cd. incostituzionali*, in *Giur. it.*, 1999, pp. 1692-1695; Cass. pen., sez. un., 23 febbraio 2000, D'Amuri.

[24] Per un'attenta ricostruzione del dibattito dottrinale e giurisprudenziale sviluppatosi dalla prima pronuncia della Consulta fino al definitivo allineamento delle Sezioni Unite, v. CAMON A., *L'acquisizione dei dati sul traffico delle comunicazioni,* in *Cass. pen.*, 2005, pp. 596-599.

[25] CAIANIELLO M., *Increasing Discretionary Prosecutor's Powers: The Pivotal Role of the Italian Prosecutor in the Pretrial Investigation Phase*, in *The Oxford Handbook Online on Criminology*, New York, Oxford University Press, 2016, pp. 4-5.

[26] Si ricorda, per dovere di completezza, che l'art. 8 della Carta trova il suo corrispondente convenzionale nell'art. 8 CEDU. In applicazione dell'art. 52(3), qualora la Carta contenga diritti corrispondenti a quelli previsti in Convenzione, il significato e la portata degli stessi devono essere ritenuti eguali a quelli conferiti in Convenzione.

[27] *Cfr.* CGUE, *Digital Rights Ireland*, § 62.

Corte di giustizia[28], i cui rilievi sono altresì in linea con quanto elaborato nella giurisprudenza della Corte europea dei diritti dell'uomo (di seguito: Corte Edu)[29]. In sostanza, la nozione autonoma di indipendenza accolta dai giudici del Lussemburgo sembra esser legata non solo alla dimensione "esterna" – riferita ai rapporti dell'organo giudicante con il potere esecutivo – ma anche a quella prettamente "interna" di imparzialità, intesa come assenza di ogni interesse alla soluzione della controversia[30].

Alla luce di queste considerazioni, è lecito aver dubbi sulla possibilità di qualificare il pubblico ministero italiano come organo effettivamente indipendente nel quadro della giurisprudenza sovranazionale sopracitata[31]. Certamente, le garanzie di indipendenza del magistrato inquirente nei riguardi del potere esecutivo possono dirsi particolarmente forti nel nostro ordinamento – a differenza di quanto accade in numerosi altri Stati membri. D'altro canto, tuttavia, risulta difficile sostenere la posizione dell'organo di pubblica accusa all'interno del procedimento penale sia una di assoluta indifferenza quanto al risultato finale dell'accertamento di responsabilità[32]. La riforma

---

[28] *Cfr., inter alia,* CGUE, 19 settembre 2006, *Graham J. Wilson contre Ordre des avocats du barreau du Luxembourg*, C-506/04, §§ 51-52.

[29] Molti sono i riferimenti alla nozione di autorità indipendente, anche in riferimento alla specifica figura del pubblico ministero, nella giurisprudenza della Corte di Strasburgo. V., *inter alia,* Corte Edu, 29 marzo 2010, *Medvedyev c. Francia*, n. 3394/03, § 124; Corte Edu, 23 novembre 2010, *Moulin c. Francia*, n. 37104/06, § 58. Rispetto al caso italiano, è utile citare il recente caso *Brazzi c. Italia*, in cui la Corte di Strasburgo ha condannato lo Stato italiano per la mancata predisposizione di un controllo giurisdizionale effettivo sul decreto di sequestro del pubblico ministero (*cfr.* Corte Edu, 27 settembre 2018, *Brazzi c. Italia*, n. 57278/11, §§ 48 e 50). Il riferimento è qui di particolare interesse, considerato che l'acquisizione dei dati emergenti dai tabulati è stata più volte assimilata, dalla dottrina e dalla giurisprudenza, ad una particolare forma di sequestro probatorio. Per completezza, si specifica che ad oggi i tabulati – ottenuti mediante provvedimento acquisitivo del pubblico ministero – siano qualificati dalla dottrina come prove documentali ex art. 234 c.p.p. (v. MARCOLINI S., *L'istituto della* data retention, cit., p. 1585). Altrettanto può dirsi, sotto diverso profilo, del *contenuto* dei messaggi Whatsapp, conservati nella memoria del telefono cellulare in uso all'indagato, ed acquisiti dalla polizia giudiziaria mediante riproduzione fotografica della schermata (cfr. Cass. pen., sez. VI, n. 1822/2020, punto 2.1-2.3).

[30] CGUE, *Graham J. Wilson*, cit., § 52. Sul punto, v. anche le osservazioni di LASAGNI G., *Tackling phone searches in Italy and in the US. Proposals for a technological re-thinking of procedural rights and freedoms*, in *NJECL*, 2018, 9, pp. 396-397.

[31] Lo sostengono, *inter alia*, ANDOLINA E., *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, CEDAM, 2018, pp. 120-125; IOVENE F., Data retention *tra passato e futuro. Ma quale presente?,* in *Cass. pen.*, 2014, 12, p. 4274-4282.; LASAGNI G., *Tackling phone searches,* cit., p. 397; GATTO C.E., *Il principio di proporzionalità nell'ordine europeo di indagine penale*, in *Dir. pen. cont.*, 2019, 2, p. 87. È anche utile evidenziare che, nel quadro di un rinvio pregiudiziale attualmente pendente presso la CGUE, l'Avvocato Generale (AG) Pitruzzella ha espresso le sue perplessità quanto alla possibilità di qualificare il pubblico ministero estone (*Prokuratuur*) come figura indipendente ed idonea ad esercitare un controllo preventivo sulle richieste di accesso ai metadati sulle comunicazioni. In particolare, i rilievi dell'AG si sono concentrati sul fatto che il pubblico ministero estone (non troppo diversamente da quello italiano, si potrebbe sostenere) sia chiamato «a dirigere il procedimento istruttorio», nonché eventualmente a «rappresentare la pubblica accusa in giudizio». *Cfr.* Conclusioni dell'AG G. Pitruzzella nella causa *H.K. c. Prokuratuur* (C-746/18), §§ 118-124.

[32] È noto a chi scrive che la tesi qui proposta non è esente da criticità sul piano sistematico interno. Sotto il profilo esclusivamente funzionale, sembrerebbe difficile sostenere, in termini perentori, che la figura del pubblico ministero italiano sia connotata da un evidente *deficit* di imparzialità e indipendenza nella fase

del processo penale italiano in senso accusatorio sembra infatti delineare il pubblico ministero come figura portatrice di interessi sostanzialmente contrapposti a quelli della difesa[33].

Considerata la gravità dell'ingerenza nella vita privata oggi provocata dall'analisi incrociata dei metadati[34], sarebbe opportuno ridiscutere la scelta di affidare al pubblico ministero un potere così rilevante e potenzialmente invasivo della sfera privata. Ciò specialmente alla luce della ampiezza di scelta, che potrebbe dirsi discrezionalità sotto diversi aspetti, di fatto accordata al pubblico ministero nella fase delle indagini[35], nonché della vaghezza dei criteri – si pensi, ad esempio, all'assenza di presupposti probatori[36] – i quali ad oggi costituiscono le condizioni del provvedimento acquisitivo dei dati.

---

delle indagini preliminari. Si deve qui tener conto, difatti, del principio di obbligatorietà dell'azione penale, nonché di quello di tendenziale completezza delle indagini, i quali fungerebbero da argine alla discrezionalità del magistrato requirente nella fase che precede l'esercizio dell'azione penale (sulla completezza delle indagini si veda, *inter alia*, CAIANIELLO M., *Archiviazione*, in *Enciclopedia del diritto*, Annali, Vol. II, Tomo 1, Milano, Giuffrè, 2008, pp. 59 – 80). La questione – che per la sua portata non può essere affrontata nell'ambito di questo lavoro – è certamente densa di risvolti, talora anche ambigui, che sembrano in principio escludere qualsiasi soluzione univoca ed esauriente. È doveroso dunque ribadire che la posizione qui espressa prende le mosse da una prospettiva prettamente eurounitaria – la quale pone l'accento sul requisito di terzietà dell'organo preposto all'acquisizione dei dati – senza tuttavia ignorare le problematicità di tale approccio nell'ottica interna.

[33] Sul punto si vedano le riflessioni di CAIANIELLO M., *Poteri dei privati nell'esercizio dell'azione penale*, Torino, Giappichelli, 2003, p. 25. In particolare, l'Autore sostiene che la concezione dell'organo di pubblica accusa come parte assolutamente obiettiva e imparziale appartenga ad una visione ancora prettamente inquisitoria del processo penale. Con riferimento specifico al tema dell'acquisizione dei tabulati, v. DE LEO F., *Note a margine della legge sull'acquisizione e conservazione dei dati di traffico telematico,* in *Dir. Proc. Pen.*, 2004, p. 1272.

[34] Sulla necessità di ripensare la distinzione tra dati esterni e contenuto delle comunicazioni, v. *infra*, par. 5.

[35] V. *supra* nota 29. Si è detto che il principio di completezza ed effettività delle indagini viene generalmente annoverato tra i limiti alla discrezionalità del pubblico ministero nella fase precedente all'esercizio dell'azione. Tale principio, elaborato nella giurisprudenza costituzionale a partire dalla sentenza n. 88 del 1991, si fonda notoriamente sul combinato disposto degli artt. 326 e 358 c.p.p. Su quest'ultima disposizione, che prevede che il pubblico ministero svolga anche accertamenti a favore dell'indagato, la dottrina e la giurisprudenza si sono lungamente espresse, spesso in maniera contrastante. A dispetto della sua ambiguità, secondo parte della giurisprudenza tale previsione non intaccherebbe il ruolo di parte del pubblico ministero nel sistema accusatorio (*cfr. ex plurimis* Cass. pen., sez. I, n. 6599/1995, Abrate). Tale impostazione troverebbe infatti conferma nel fatto che il mancato esperimento di mezzi investigativi a favore dell'indagato non sfoci in alcuna sanzione processuale per il magistrato dell'accusa, che non avrebbe dunque un obbligo in tal senso (*cfr.* Cass. pen., sez. II, n. 3415/1997). Sul punto, v. ANDRONIO A., *Pubblico ministero e direzione delle indagini preliminari*, in *Trattato di procedura penale*, vol. 3 (a cura di Garuti G., opera diretta da Spangher G.), 2009, pp. 279-285. Parla invece di vero e proprio obbligo di svolgere accertamenti a favore dell'indagato GREVI V., *Archiviazione per "inidoneità probatoria" ed obbligatorietà dell'azione penale*, in *Riv. it. dir. proc. pen.*, 1990, p. 1299. Anche prima della riforma in senso accusatorio del processo, nel periodo di vigenza del vecchio codice alcuni Autori avevano messo in luce la discrezionalità di fatto esercitata dal pubblico ministero nella conduzione dell'istruttoria, *cfr*. ZAGREBELSKY V., *Indipendenza del pubblico ministero e obbligatorietà dell'azione penale,* in *Pubblico ministero e accusa penale* (a cura di Conso G.), Torino, Zanichelli, 1979, p. 18; DOMINIONI O., *Le parti nel processo penale: Profili sistematici e problemi*, Milano, Giuffrè, 1985, pp. 85-86; DOMINIONI O., *Azione penale,* in *Dig. Pen.*, vol. I, Utet, 1987, pp. 409-410.

[36] Si esprime in senso critico sul punto CAMON A., *L'acquisizione dei dati*, cit., p. 615.

Nel rifiutare la tesi prospettata dal ricorrente e qui riproposta, la Cassazione propone delle argomentazioni che, sul piano strettamente linguistico, potrebbero essere oggetto di critica. Per ribadire l'inapplicabilità della giurisprudenza europea invocata al caso della disciplina italiana sulla *data retention*, la Corte fa riferimento alla presunta erroneità della traduzione italiana della sentenza *Digital Rights*, scegliendo invece di rifarsi alle versioni inglese e francese.

Con particolare riferimento quest'ultima, la Corte fa leva sull'utilizzo del termine *juridiction*, il quale sarebbe riferibile «alla magistratura francese nel suo complesso, composta da giudici e pubblici ministeri (*magistrats du parquet*)». Orbene, questa soluzione interpretativa non può essere assolutamente condivisa. Invero, nella terminologia specialistica francese, il termine *juridiction* fa esclusivo riferimento agli organi – di natura giudiziaria o amministrativa – incaricati di risolvere una controversia in una posizione di terzietà rispetto alle parti[37]; la magistratura requirente non rientra dunque in questa categoria, anzi vi è radicalmente contrapposta. Stesse conclusioni valgono per il riferimento al termine inglese *court*, considerato dalla Corte come «promiscuo», e adatto a ricomprendere sia la figura del giudice sia quella del pubblico ministero. Anche qui, l'interpretazione fatta propria dalla Corte non può dirsi corretta: pacificamente, difatti, il termine *court* fa riferimento a una serie eterogenea di organi che abbiano la qualifica di "giudice", e siano cioè deputati alle attività di risoluzione delle controversie in posizione di terzietà rispetto alle parti[38].

Indubbiamente, errori di questo genere sono emblematici delle problematiche che possono insorgere nel contesto di multilinguismo che è proprio del diritto dell'Unione[39]. Se da sempre la lingua riveste un ruolo fondamentale – e delicato – in quanto strumento di espressione del diritto vigente, la sua importanza è oggi amplificata dall'inclusione nell'ordinamento interno di fonti provenienti *ab externo*, eventualmente espresse in lingue diverse da quella italiana. In questo senso, sarebbe auspicabile che le necessarie operazioni di traduzione venissero effettuate, in ambito giudiziario, sempre con la massima accortezza, proprio per la decisività che esse possono rivestire al fine della soluzione di sempre più numerose questioni giuridiche. Eventuali misinterpretazioni, come quelle qui riscontrate, possono mutare sensibilmente il ruolo della lingua, la quale da strumento con cui dare espressione al diritto già esistente può facilmente diventare quello attraverso il quale creare del diritto nuovo.

Alla luce di quanto esposto, la soluzione ai problemi esaminati dovrebbe passare – *de jure condendo* – per l'attribuzione al giudice del potere di acquisizione dei dati

---

[37] PUIGELIER C., *Dictionnaire juridique*, 2ème édition, Bruylant, Collection Paradigme, p. 587: «*Organe de l'ordre judiciaire ou administratif chargé de juger. – Ensemble des tribunaux de même ordre ou de même nature ou de même degré (par exemple, les juridictions du second degré ou les juridictions d'exception)*».

[38] Cane P., Conaghan J. (a cura di), *The New Oxford Companion to Law*, Oxford University Press, 2008, p. 249: «*The term court is used to describe such a wide variety of institutions in a legal system that it is difficult to identify common features beyond saying that most (but not all) courts consist of legally qualified judges and that courts are involved in making binding determinations of fact and law to resolve disputes through a process of adjudication (…)*».

[39] Sui problemi legati alla traduzione giuridica e al carattere multilinguistico del diritto dell'Unione, si veda per tutti BAJČIĆ M., *Multilinguism and EU legal concepts*, in *New Insights into the Semantics of Legal Concepts and the Legal Dictionary*, Amsterdam, John Benjamins Publishing Co., 2017, pp. 91-106.

emergenti dai tabulati telefonici e telematici. Solo questa figura sembra infatti soddisfare in pieno e senza riserve gli *standard* di indipendenza elaborati nella giurisprudenza delle due Corti europee.

Sono note le perplessità che in passato erano state mosse in dottrina[40], nonché in giurisprudenza[41], nei confronti di un sistema che legittimi il solo giudice a decidere sulla richiesta di accesso ai dati esterni alle comunicazioni. Diverse, tuttavia, sono le soluzioni che potrebbero eventualmente ovviare ai problemi derivanti da una riforma in questo senso. In primo luogo, sarebbe possibile immaginare un nuovo sistema a struttura bifasica, in cui l'intervento del giudice sia limitato alle richieste di acquisizione che riguardino l'integralità dei dati presenti sul tabulato. In linea con il principio di proporzionalità e di limitazione delle finalità, provvedimenti di questo tipo sarebbero autorizzati esclusivamente per una serie di reati di una certa gravità, legislativamente predeterminati. Al contempo, il potere di accesso del pubblico ministero potrebbe essere mantenuto solo per le misure che determinino una lieve ingerenza nei diritti protetti. Questo sarebbe il caso, ad esempio, dell'acquisizione dei soli dati anagrafici relativi agli utilizzatori di carte SIM: la scarsa gravità della compressione apportata ai diritti alla *privacy* e alla protezione dei dati permetterebbe qui di estendere la procedura di accesso alla generalità delle fattispecie di rilevanza penale, in linea con quanto statuito dalla Corte di giustizia nel caso *Ministerio Fiscal*. Del resto, la predisposizione di un sistema bifasico – e il conseguente coinvolgimento del giudice – sarebbe del tutto coerente con l'introduzione di un catalogo circoscritto di reati gravi che legittimi l'accesso all'integralità dei dati emergenti dal tabulato. Come è stato sostenuto in dottrina, infatti, quando il procedimento penale è suscettibile di articolarsi in diversi regimi – tra loro alternativi – è il giudice a dover controllare la legalità della scelta da cui scaturisce l'applicazione di una particolare serie di regole rispetto ad un'altra[42].

In secondo luogo, sarebbe indubbiamente necessario ripristinare una procedura di urgenza – un tempo prevista ai commi 4 e 4-bis dell'art. 132 cod. *privacy*, sul modello

---

[40] CANTONE R., *Le modifiche processuali introdotte con il «decreto antiterrorismo» (d.l. n. 144/05 conv. in l. n. 155/05)*, in *Cass. pen.*, 2005, p. 2512. Altri esponenti della dottrina, pur non censurando sul piano della stretta legittimità l'attribuzione al pubblico ministero del potere di acquisizione dei dati, avevano comunque messo in luce la diminuzione degli *standard* di garanzia che derivava dalla sottrazione al controllo del giudice delle operazioni di accesso ai dati cd. recenti. Sul punto, v. RAFARACI T., *Intercettazione e acquisizione di tabulati telefonici*, in *Contrasto al terrorismo interno e internazionale* (a cura di Kostoris R. E., Orlandi R.), 2007, Giappichelli, p. 278.

[41] G.i.p. Trib. Pavia, ord. 24 marzo 2004 (dep. 25 marzo 2004) – *Est.* Lambertucci, annotata da PINNA M., *"Garanzie" giurisdizionali nell'acquisizione dei tabulati telefonici: dubbi infondati intorno ad una norma (probabilmente) incostituzionale*, in *Cass. pen.*, 2005, p. 1401-1410. A seguito dell'entrata in vigore della legge di conversione n. 45/2004, la quale attribuiva al solo giudice il potere di acquisire i dati esterni alle comunicazioni, il g.i.p. di Pavia aveva sollevato una questione di legittimità costituzionale, in riferimento agli artt. 97 e 112 Cost., lamentando l'irragionevole stasi del procedimento – peraltro non bilanciata dalla previsione di una procedura di urgenza – che discendeva dal carattere indispensabile dell'intervento del giudice nell'acquisizione dei dati. Sulla questione, ritenuta non manifestamente infondata, si è in seguito pronunciata la Consulta con sentenza n. 372 del 2006. Il problema relativo all'intervento del giudice non è stato tuttavia oggetto di scrutinio da parte della Corte: l'adozione, nel frattempo, del d.l. 144/2005 che introduceva il sistema del c.d. doppio binario aveva privato di rilevanza la questione.

[42] DE LEO F., *Note a margine della legge*, cit., p. 1274.

di quanto già previsto in materia di intercettazioni – la quale permetta al pubblico ministero di acquisire i dati al ricorrere di determinate condizioni, con successiva convalida del giudice.

5. Nuovi paradigmi per metadati e contenuto delle comunicazioni nell'era dei *big data*.

La distinzione tra dati esterni e contenuto delle comunicazioni è ormai da tempo cristallina sia in dottrina, sia in giurisprudenza. Già a partire dagli anni Ottanta, infatti, l'individuazione degli estremi del colloquio telefonico – il cd. "blocco" – veniva qualificata come attività ontologicamente diversa rispetto a quella propriamente captativa del contenuto della comunicazione[43].

Benché il tenore dello scambio comunicativo resti sconosciuto, si considera – come già ricordato – che l'acquisizione dei dati esterni rientri comunque nell'alveo di protezione dell'art. 15 Cost. In sostanza, in questo caso è l'utilizzo del mezzo tecnologico – idoneo a lasciare una traccia del dato storico dell'avvenuta comunicazione – a richiedere lo spiegamento delle garanzie costituzionali[44]. Questa soluzione interpretativa, accolta dalla Consulta sin dal 1993, ha tuttavia come corollario un assunto mai veramente messo in discussione. Posto che l'acquisizione dei dati esterni non implica una conoscenza del contenuto proprio delle conversazioni, si ritiene che il *vulnus* arrecato al diritto alla segretezza delle comunicazioni non sia equiparabile a quello provocato dalle attività di intercettazione.

Nella sentenza in commento, la Suprema Corte abbraccia pienamente l'impostazione tradizionale[45], che del resto trova riscontro anche nelle considerazioni svolte dalla Corte di giustizia in *Digital Rights*[46]. Anche questa volta, tuttavia, c'è da chiedersi se il mutato contesto sociale non richieda un radicale ripensamento dei

---

[43] CAMON A., *Le intercettazioni nel processo penale*, Milano, Giuffrè, 1996, pp. 28-32. Per alcuni riferimenti giurisprudenziali sulla distinzione tra l'operazione di blocco (riferita ai soli telefoni fissi) e quella propria di intercettazione, v. p. 28 nota 84.

[44] CAMON A., *Le intercettazioni*, cit., p. 29; nello stesso senso, DE LEO F., *Controllo delle comunicazioni e riservatezza,* in *Cass. pen.*, 2002, p. 2213. È ben nota invece l'opinione contraria, rimasta minoritaria, che escludeva che i dati esterni alle comunicazioni fossero meritevoli di tutela ex art. 15 Cost. (v. CAPRIOLI F., *Colloqui riservati e prova penale,* Torino, Giappichelli, 2000, pp. 66-73; DIDDI A., *Tutela della* privacy *e acquisizione dei tabulati telefonici,* in *Giust. Pen.*, 1999, pp. 615-639).

[45] *Cfr.* Cass. pen., sez. III, n. 36380/2019, punto 3.7. Volendosi concedere una considerazione di carattere generale, è utile sottolineare come la tendenza, per così dire "conservatrice", della Suprema Corte accomuni in realtà diverse pronunce, che toccano – in forme diverse e variegate – il tema dell'uso dei mezzi tecnologici nel procedimento penale. In una recente sentenza, che concerne l'acquisizione del contenuto di messaggi *Whatsapp* mediante riproduzione fotografica della schermata di un telefono cellulare, i giudici di legittimità hanno confermato l'orientamento consolidato, ritenendo che i dati informatici acquisiti dalla memoria del telefono in uso all'indagato abbiano la natura di documenti *ex* art. 234 c.p.p. Ne consegue, secondo l'interpretazione della Suprema Corte, che l'acquisizione di tali dati non soggiaccia né alle regole sul sequestro di corrispondenza, né a quelle sull'intercettazione di comunicazioni informatiche e telematiche (cfr. Cass. pen., sez. VI, n. 1822/2019, punti 2.1-2.3).

[46] CGUE, *Digital Rights Ireland*, cit., § 39.

paradigmi tradizionali in materia. Le insidie che il fenomeno di incessante evoluzione tecnica porta con sé impongono all'interprete di lavorare costantemente sui principi, con l'obiettivo di apprestare sempre nuove – e più adatte – garanzie individuali nello spiegamento dei moderni mezzi di indagine. Questi ultimi, per il loro carattere raffinato e altamente invasivo, sono infatti idonei a comprimere i diritti costituzionalmente garantiti in forme prima impensabili.

Si pensi, anzitutto, al carattere capillare e pervasivo delle odierne tecnologie dell'informazione, che rendono inevitabile la disseminazione di un'enorme scia di dati in quasi ogni attività quotidiana. Diversi sono anche gli strumenti di trattamento automatizzato dei dati in questione, sempre più potenti e accessibili sotto il profilo economico[47]. È ormai noto che le moderne tecnologie di *big data*[48] permettono di ottenere una rilevante quantità di informazioni sulla sfera privata dell'individuo, anche solo ricorrendo all'analisi combinatoria dei dati esterni alle comunicazioni, nonché di quelli generati da molte attività quotidiane poste in essere grazie all'ausilio di una connessione ad *internet*. Le inferenze risultanti dal trattamento automatizzato dei metadati sulle comunicazioni, per giunta, possono diventare particolarmente dettagliate quando l'analisi integrata coinvolge anche i dati cd. *open source*, come quelli pubblicati sui *social network*[49].

Pur non mettendo in dubbio la ben marcata distinzione tra le due categorie, già in tempi meno critici degli attuali alcuni esponenti della dottrina avevano messo in luce la necessità di dare maggiore rilevanza alla compressione al diritto alla *privacy* che deriverebbe dal trattamento dei dati esterni alle comunicazioni[50]. Recentemente, la tesi dell'assimilazione dei dati esterni al contenuto delle comunicazioni sembra aver trovato un *endorsement* giurisprudenziale di non scarso rilievo. Sul punto, difatti, deve esser menzionata la nota sentenza *Big Brother Watch* – di cui si attende la decisione di Grande Camera – in cui la Corte di Strasburgo ha equiparato, sotto il profilo della gravità, l'ingerenza derivante dall'acquisizione dei dati esterni a quella relativa alla captazione del contenuto comunicativo[51]. Con il suo tipico approccio pragmatico, la Corte Edu ha difatti sostenuto che, in molteplici occasioni, il contenuto di una conversazione può anche non rivelare alcunché di interessante sulla vita degli interlocutori; è l'analisi dei metadati, spesso, a configurarsi invece come mezzo più utile ai fini delle indagini, permettendo di carpire molte informazioni sulle abitudini degli interessati, i loro

---

[47] Nel particolare caso dell'analisi dei dati esterni al traffico telefonico e telematico, è utile osservare che sono oggi in commercio degli strumenti informatici in grado di supportare le attività di indagine con una lettura incrociata dei dati acquisiti. *Cfr.* REALE P., *I dati telefonici e telematici,* cit., p. 336.

[48] I *big data* possono essere definiti come «dati che superano i limiti degli strumenti di database tradizionali. Il termine *big data* è poi utilizzato, per estensione, per definire le tecnologie volte ad estrarre conoscenza e valore da questa tipologia di dati». La definizione è di REZZANI A., Big data. *Architettura, tecnologie e metodi per l'utilizzo di grandi basi di dati*, Apogeo Education, Maggiori Editore, 2013, p. 10.

[49] Si parla in questo caso di *social media mapping*.

[50] *Cfr.* LONGO A., *Il regime processuale dei dati esterni alla comunicazione: un problema ancora aperto*, in *Giur. it.*, 1999, p. 2008.

[51] Corte Edu, 13 settembre 2018, *Big Brother Watch c. Regno Unito*, nn. 58170/13, 62322/14 e 24960/15, § 356.

spostamenti, le frequentazioni, le capacità economiche, o le opinioni politiche, filosofiche o religiose.

È doveroso specificare che le considerazioni qui proposte non vanno nel senso di un'acritica estensione della disciplina delle intercettazioni alle operazioni di accesso ai tabulati, quanto di un generale innalzamento delle garanzie previste oggi nell'art. 132 cod. *privacy*. La necessità di attribuire al giudice, almeno in alcune circostanze, la competenza nel decidere sull'opportunità di ricorrere all'acquisizione dei tabulati poggia, *inter alia*, sul progressivo venir meno della tradizionale distinzione tra dati esterni e contenuto delle comunicazioni. Il trattamento algoritmico dei metadati – se esteso e combinato a dati *open source* – può anche, in determinate circostanze, apportare un contributo investigativo maggiore rispetto alla captazione del contenuto di una comunicazione. Le capacità esplorative di questi mezzi di indagine non devono dunque essere sottovalutate, specie quando l'acquisizione dei tabulati interessa l'integralità dei dati conservati dai fornitori di servizi[52].

6. Principio di proporzionalità e *data retention*: dei nodi ancora da sciogliere per i sistemi di sorveglianza di massa

Si è già detto che il continuo avanzamento – e la metamorfosi – delle moderne tecniche di indagine rende oggi necessario un costante impegno dell'interprete, chiamato a lavorare sui principi, con l'obiettivo di preservare le garanzie individuali a fronte di mezzi sempre più invasivi[53]. In quest'incessante opera adeguatrice il principio di proporzionalità[54], come si è già in parte osservato, svolge un ruolo primario, ponendosi come strumento di bilanciamento tra le esigenze di protezione della vita privata e quelle di tutela della sicurezza e repressione degli illeciti penali.

Sebbene il principio in questione sia stato a più riprese valorizzato dalla giurisprudenza europea soprarichiamata, esso pone in realtà non pochi problemi applicativi nella complessa materia della *data retention*. Diversi sono infatti i nodi interpretativi che devono ancora essere sciolti dalla Corte di giustizia dopo la sentenza *Digital Rights*. Nell'ormai storica pronuncia, la Corte ha radicalmente escluso la compatibilità di una misura di sorveglianza generalizzata come quella della vecchia direttiva *data retention* con il principio di proporzionalità, il quale richiederebbe che la conservazione dei dati venisse circoscritta in base a criteri oggettivi di tipo geografico, temporale o soggettivo[55]. Due, tuttavia, sono i problemi sollevati da una soluzione ermeneutica di questo tipo. In primo luogo, la scelta di limitare la sorveglianza ad una

---

[52] V. *supra* par. 4.

[53] Così già LUPARIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica,* Milano, Giuffrè, 2007, p. 143.

[54] La centralità di questo principio è indubbia nel quadro delle fonti europee. Sulla valenza del principio nell'ordinamento interno si veda, per tutti, CAIANIELLO M., *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont. – Riv. trim.*, 2014, nn. 3-4, pp. 143-163. In materia di indagini digitali, nello specifico, NICOLICCHIA F., *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Dir. pen. cont. – Riv. trim.*, pp. 176-189.

[55] CGUE, *Digital Rights Ireland*, cit., § 59.

determinata cerchia di persone – seppur individuate secondo criteri oggettivi – è suscettibile di dar luogo a politiche di tipo discriminatorio, specialmente nel caso in cui la conservazione dei dati venga limitata a soggetti con precedenti penali a carico. In secondo luogo, delimitare a monte l'ambito di applicazione della misura di sorveglianza rischia, ancora prima della commissione degli illeciti penali, di determinare la perdita di elementi di prova preziosi ai fini delle future operazioni di indagine e accertamento.

Gli interrogativi suscitati dalla predisposizione di sistemi di sorveglianza di massa sono oggi al centro del dibattito giurisprudenziale a livello europeo. Se da un lato la Corte di giustizia mantiene la sua ferma opposizione alle misure di conservazione di dati generalizzate, dall'altro la Corte di Strasburgo sembra adottare un approccio discordante. In *Big Brother Watch*, ad esempio, la Corte ha nuovamente ribadito l'assenza di una radicale incompatibilità tra i sistemi di sorveglianza di massa e l'art. 8 della Convenzione[56]. Tuttavia ha introdotto la necessità di un cruciale correttivo: se gli Stati parte godono di un'ampia discrezionalità quanto alla scelta del sistema di sorveglianza da predisporre (generalizzato o circoscritto), altrettanto non può dirsi sulle modalità di conservazione e accesso ai dati, sulle quali la Corte è legittimata ad operare un controllo più stretto[57].

In assenza di posizioni concordi sulla compatibilità dei sistemi generalizzati di raccolta dati con gli strumenti europei di protezione dei diritti fondamentali, che soluzioni dare *medio tempore* ai dilemmi posti dalla disciplina della *data retention*?

Sul piano interno, alcuni spunti possono essere presi dagli ultimi sviluppi giurisprudenziali in tema di perquisizione e sequestro informatico. Come noto, le Sezioni unite Andreucci[58] hanno recepito la distinzione – già da tempo chiara in dottrina – tra il *computer*, considerato alla stregua di una vera e propria libreria fisica per le sue enormi capacità di archiviazione dei dati, e i singoli *file* che ne costituiscono il contenuto[59]. L'equiparazione del *computer* ad un intero archivio esclude generalmente la possibilità di un sequestro indiscriminato del sistema informatico nel suo complesso, posto che il principio di proporzionalità – applicabile anche in materia di sequestro probatorio – impone di sottoporre il sistema in questione ad una perquisizione mirata, nonché di limitare il provvedimento ablatorio ai soli dati che presentino un nesso di pertinenzialità con il reato da accertare[60].

---

[56] Corte Edu, *Big Brother Watch*, cit., § 314.

[57] *Id.*, § 315.

[58] Cass. pen, sez. un., n. 40963/2017, Andreucci, con nota di MARI A., *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati,* in *Cass. pen.*, 2017, 12, pp. 4312-4320; RIVELLO P., *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in *Cass. pen.*, 2018, 1, pp. 131-143; BARTOLI L., *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature,* in *Arch. pen.*, 2018, 1, pp. 1-24; TODARO G., *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare:* revirement *delle Sezioni Unite*, in *Dir. pen. cont.*, 2017, 11, pp. 157-172.

[59] *Cfr., inter alia,* Cass. pen, sez. VI, n. 24617/2015, Rizzo; Cass. pen., sez. III, n. 38148/2015, Cellino; Cass. pen., sez. V, n. 25527/2016, Storari.

[60] Nello stesso senso, si veda recentemente Cass. pen., sez. VI, n. 31593/2019. In un diverso caso – che ha tra l'altro ricevuto una certa attenzione a livello mediatico – la VI sezione penale della Suprema Corte ha annullato un decreto di perquisizione e sequestro che aveva interessato la quasi integralità dei supporti e del materiale informatico di proprietà degli indagati. Nel caso di specie, la Corte ha ritenuto non vi fosse

A ben vedere, la conservazione dei metadati sulle comunicazioni e la perquisizione di supporti informatici condividono, a livello logico, lo stesso problema di fondo: l'impossibilità di conoscere a priori il contributo di tipo conoscitivo suscettibile di essere apportato alle indagini dai dati che potrebbero essere oggetto di apprensione. E se a monte è difficile circoscrivere la cerchia di dati da sottoporre a perquisizione informatica o a conservazione, cruciale diventa – ad un livello successivo – valorizzare al massimo il principio di proporzionalità, con l'obiettivo di limitare quanto più possibile il sacrificio imposto al diritto alla *privacy* dalle attività di indagine degli organi inquirenti.

Su questo punto, ci sarebbe forse qualche lezione da imparare in materia di *data retention*. Anche ammettendo, in linea con la giurisprudenza convenzionale, la possibilità di sottoporre a conservazione i dati esterni alle comunicazioni della generalità della popolazione europea, il controllo di proporzionalità sull'accesso ai dati necessita di essere potenziato quanto più possibile nel singolo caso. Tuttavia, l'art. 132 cod. *privacy* non fornisce ad oggi, per le ragioni suesposte, adeguate garanzie in questo senso. Al contempo, l'atteggiamento "rassicurante" della giurisprudenza – pienamente rappresentato nella sentenza annotata – non sembra lasciare aperti molti spiragli di cambiamento nel prossimo futuro.

una netta distinzione tra il provvedimento di perquisizione, riferito a tutta documentazione relativa ai rapporti tra gli indagati e ai dispositivi comunque utilizzati per le comunicazioni, e quello di sequestro, il quale avrebbe invece dovuto – in ossequio al principio di proporzionalità – essere limitato ai soli dati significativi e utili all'accertamento di responsabilità degli interessati (v. Cass. pen., sez. VI, n. 30467/2018).