Le Conclusioni dell'Avvocato Generale nel rinvio pregiudiziale C-178/22 promosso dal Tribunale di Bolzano: *quo vadis, data retention*?*

Giulia Formici

Abstract

Le recenti Conclusioni dell'Avvocato Generale Collins relative alla domanda di pronuncia pregiudiziale proposta dal Tribunale di Bolzano rappresentano l'occasione per tornare a riflettere sulla complessa e articolata disciplina della conservazione e accesso ai metadati per scopi securitari nell'UE e nel contesto italiano. Il presente contributo intende fornire alcune prime considerazioni critiche sul presente e sul futuro della *data retention* nonché sulle sfide che diversi attori, tanto a livello nazionale quanto sovranazionale, dovranno affrontare nel difficile bilanciamento tra sicurezza e tutela dei diritti fondamentali nell'era digitale.

The recent Opinion of the Advocate General related to the request for a preliminary ruling proposed by the Bolzano Tribunal represents a renewed opportunity to discuss about the complex and articulated discipline concerning the retention and access to metadata for security purposes. The paper aims at providing some initial evaluations on the state of the art as well as on the possible future developments on data retention regulation, both at national and supranational level: different actors – legislators and courts – should confront with the difficult challenge of balancing security needs and fundamental rights protection in the digital era.

Sommario

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Generale Collins nel caso C-178/22. – 4. Tante tappe ma quale meta? La difficoltà di scorgere un punto di arrivo.

Keywords
data retention; rinvio pregiudiziale C-178/22; accesso ai metadati; sicurezza; diritti fondamentali

1. Il tortuoso percorso della *data retention* nell'Unione europea tra rallentamenti e inversioni di marcia

Le Conclusioni dell'Avvocato Generale nel caso C-178/22, avviato mediante rinvio pregiudiziale dal Tribunale di Bolzano[1], rappresentano solo l'ultima tappa della c.d. *data retention saga*. La disciplina della conservazione e accesso ai metadati per scopi securitari ha infatti seguito un percorso regolatorio, tra i più lunghi e travagliati nel contesto eurounitario, caratterizzato da molteplici battute d'arresto e inversioni di marcia nonché dal proliferare di sentieri normativi e giurisprudenziali paralleli, in cui legislatori e corti nazionali si sono spesso avventurati.
In questo articolato contesto, la Corte di giustizia dell'UE (CGUE) ha sicuramente contribuito, molto più di altri "viaggiatori", a dettare il passo e la direzione del cammino, a partire dalla prima pronuncia *Digital Rights Ireland*[2] sino ad arrivare, attraverso decisioni di estremo rilievo[3], alle recenti e fondamentali sentenze *Privacy International* e *La Quadrature du Net*[4] del 2020. Queste ultime[5] hanno innanzitutto rafforzato i principi già

[1] Conclusioni dell'Avvocato Generale Anthony Michael Collins, CGUE, C-178/22, sulla base della domanda di pronuncia pregiudiziale proposta dal Tribunale di Bolzano.

[2] CGUE, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications et al* (2014). Tra i numerosi commenti a questa storica pronuncia, si rinvia a: M. Dicosola, *La data retention directive e il dialogo tra Corti costituzionali e Corte di Giustizia nel sistema multilivello europeo*, in *Diritti comparati*, 20 febbraio 2014; M. Granger - K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review*, 6, 2014, 849 ss; A. Vedaschi, *Data retention and its implications for the fundamental right to privacy*, in *Tilburg Law Review*, 20, 2015, 19 ss.; G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in questa *Rivista*, 2, 2018, 64 ss.

[3] Si fa riferimento alle sentenze CGUE, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Secretary of State c. Post-och telestryrelsen (PTS) e Tom Watson et al.* (2016) e CGUE, C-207/16, *Ministerio Fiscal* (2018). Per un'analisi di tali pronunce sia consentito rinviare a G. Formici, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino, 2021 e alla bibliografia ivi citata.

[4] CGUE, C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al.* (2020) e CGUE, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net et al. v. Premier Ministre et al.* (2020). *Ex multis*, si rimanda, per un commento a: M. Rojszczak, *National security and retention of telecommunications data in light of recent case law of the European Courts*, in *European Constitutional Law Review*, 4, 2021, 607 ss.; V. Mitsilegas - E. Guild - E. Kuskonmaz - N. Vavoula, *Data retention and the future of large-scale surveillance: the evolution and contestation of judicial benchmarks*, in *European Law Journal*, 1, 2022, 1 ss.; S. Eskens, *The ever-growing complexity of the data retention discussion in the EU: an in-depth review of La Quadrature du Net & Others and Privacy International*, in *European Data Protection Law Review*, 8, 2022, 143 ss.; M. Tzanou - S. Karyda, *Privacy International and La Quadrature du Net: one step forward, two steps back in the data retention saga?*, in *European Public Law*, 1, 2022, 123 ss.; N. Ni Loideain, *EU data privacy law and serious crime. Data retention and policymaking*, Oxford, 2022.

[5] Merita ricordare sin da ora come le rilevanti pronunce del 2020 siano state seguite da alcune ulteriori sentenze della CGUE in materia di *data retention* che hanno rappresentato una conferma ulteriore

sanciti nella previa giurisprudenza europea[6]: da un lato viene ribadita l'incompatibilità con il diritto dell'UE di forme di conservazione generalizzata e indiscriminata (c.d. *bulk data retention*) per scopi di garanzia della sicurezza pubblica e repressione dei reati gravi, mentre dall'altro la *targeted data retention* viene riconfermata come l'unica forma di conservazione proporzionata e legittima. Sotto il profilo dell'accesso ai metadati da parte di autorità di *law enforcement* e di *intelligence*, inoltre, vengono riaffermati quali prerequisiti necessari tanto il carattere di gravità del reato perseguito, quanto il previo controllo da parte di un'autorità amministrativa indipendente o giurisdizionale connotata da indipendenza e terzietà. Accanto a tali importanti conferme, la CGUE non ha poi mancato di introdurre nelle due pronunce richiamate rilevanti novità, soprattutto per quanto concerne il vaglio di proporzionalità: per la prima volta viene promossa una significativa distinzione tra obiettivi di sicurezza pubblica e quelli di sicurezza nazionale[7], riconoscendo la maggiore rilevanza dell'ultima e quindi la possibilità di disporre, per tale finalità solamente, misure più invasive della sfera privata

dei principi e requisiti sanciti dai giudici di Lussemburgo: in particolare, si fa riferimento a CGUE, C-746/18, *HK v. Prokuratuur* (2021); CGUE, C-140/20, *GD v. Commissioner of An Garda Siochana et al.* (2022), e CGUE, cause riunite C-793/19 e C-794/19, *Bundesrepulik Deutschland v. SpaceNet AG e Telekom Deutschaland GmbH* (2022). Per uno studio di tali più recenti sentenze, si vedano, tra gli altri, S. Rovelli, *Case Prokuratuur: proportionality and the independence of authorities in data retention*, in *European Papers*, 2021, p. 199 ss.; E. Celeste, *Commission v. Spain and H. K. v. Prokuratuur: Taking the Plank out of EU's Own Eye*, in *BridgeBlog*, 15 marzo 2021; E. Andolina, *Ancora una pronuncia della Grande Camera della CGUE in tema di condizioni di accesso ai traffic data*, in *Processo Penale e Giustizia*, 5, 2021, 1195 ss.; X. Tracol, *The joined cases of Dwyer, SpaceNet before the European Court of Justice: the judgments of the Grand Chamber about data retention continue falling on deaf ears in Member States*, in *Computer Law & Security Review*, 48, 2023, 1 ss.; sia consentito anche il rinvio a G. Formici, *La CGUE torna a parlare agli Stati membri in materia di conservazione dei metadati e tutela dei diritti fondamentali: in un dialogo fra sordi, repetita iuvant?* , in *Diritti comparati*, 8 maggio 2023. In estrema sintesi, ciò che viene ribadito anche in tali ultime pronunce, è che «l'utilità della *data retention* per le investigazioni penali è indubbia; il modello di conservazione generalizzata e indifferenziata dei dati è inaccettabile in una società democratica; modelli alternativi di conservazione differenziata sono possibili e comunque spetta agli Stati l'obbligo di soluzioni ingegnose ma rispettose dei diritti sul punto; le eventuali difficoltà pratiche nel concepire detti modelli alternativi non possono costituire un pretesto per sposare o non abbandonare il modello generalizzato», R. Flor, S. 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, 31.

[6] Primo fra tutti il fatto che la disciplina della *data retention* rientra nell'ambito di applicazione della Direttiva *e-Privacy* (direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, direttiva relativa alla vita privata e alle comunicazioni elettroniche, c.d. Direttiva *e-Privacy,* GU 2002 L. 201/37) ogniqualvolta vengano sanciti obblighi in capo a *service providers* privati. Su questo dibattuto e tutt'altro che pacifico profilo, M. Zalnieriute, *A struggle for competence: national security, surveillance and the scope of EU la wat the Court of Justice of the EU*, in *Modern Law Review*, 85, 2021, 1 ss.

[7] La definizione di sicurezza nonché la linea di demarcazione – invero ricorrente e cruciale sotto il profilo del riparto di competenze tra UE e Stati membri – tra sicurezza nazionale e pubblica, resta un tema di estremo rilievo e complessità. Per riflessioni su tale concetto, si rinvia, *ex multis*, a P. Torretta, *Diritto alla sicurezza e (altri) diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'Aloia (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, 2003, 451 ss.; G. de Vergottini, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, 2004; T.E. Frosini, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni Costituzionali*, 2006, 1 ss.; A. Vedaschi, *À la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Torino, 2007; T. Giupponi, *La sicurezza e le sue "dimensioni" costituzionali*, in S. Vida (a cura di), *Diritti umani. Teorie, analisi, applicazioni*, Bologna, 2008, 275 ss.; G. Cerrina Feroni - G. Morbidelli, *La sicurezza: un valore super primario*, in *Percorsi costituzionali*, 1, 2008, 31 ss.; ma anche, sotto il profilo del diritto eurounitario, P. Vogiatzoglou - S. Fantin, *National and public security within and beyond the Police Directive*, in A. Vedder - J. Schroers - C. Ducuing - P. Valcke (eds.), *Security and law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Bruxelles, 2019, 27 ss.; M. Zalnieriute, *A struggle for competence: national security, surveillance and the scope of EU la wat the Court of Justice of the EU*, cit.

quali la *bulk data retention*, sebbene a specifiche condizioni e limiti[8].
Le articolate pronunce del 2020, i principi e limiti in esse sancite[9] hanno quindi certamente concorso a determinare «*an important barrier to the advent of a mass surveillance society*»[10], ponendosi in continuità e coerenza con una interpretazione "costituzionale" della disciplina della *data retention* che va ad inserirsi nella più ampia dinamica di «ridefinizione di un perimetro costituzionalmente orientato o quanto meno *human rights oriented* di disposizioni già in vigore quando la transizione da un'Europa dei mercati a un'Europa dei diritti non si era ancora del tutto completata»[11]. Nel fare questo, la CGUE non ha però mancato di adottare un approccio anche pragmatico – pur non scevro da critiche[12] – che ha ridefinito i contorni del vaglio di proporzionalità

[8] Questi limiti e condizioni possono essere così schematizzati: «il carattere non sistematico della conservazione generalizzata, la presenza di circostanze sufficientemente concrete che consentano di ritenere esistente una minaccia grave per la sicurezza nazionale reale e attuale o prevedibile, la previsione di un tempo di *data retention* limitato allo stretto necessario, la determinazione di garanzie rigorose contro il rischio di abusi, nonché la previsione di un effettivo controllo giurisdizionale o di un organo indipendente», G. Formici, *La sentenza HK c. Prokuratuur e il difficile dialogo tra CGUE e Stati membri in materia di conservazione e accesso ai metadati per finalità securitarie: spunti di riflessione su una questione vecchia ma ancora irrisolta*, in *Quaderni SIDIBlog*, 1, 2021, 237.

[9] La giurisprudenza della CGUE trova riflesso anche nelle decisioni di talune corti nazionali, come si avrà modo di approfondire anche nel prosieguo del presente lavoro. Per un'analisi dell'apporto del continuo dialogo tra corti nazionali e CGUE, si veda J. Podkowik - R. Rybski - M. Zubik, *Judicial dialogue on data retention laws: a breakthrough for European Constitutional Courts*, in *ICON-S*, 5, 2021, 1597 ss.

[10] V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 12; nello stesso contributo viene evidenziato come «*The evolution of the Court's case-law highlights the intricate institutional architecture at play when it comes to defining the future of mass surveillance and democracy in the digital era, with a complex part played by the judiciary, the legislative and the executive in a multi-level polity such as the EU*». Del resto, anche Fennelly riconosce il ruolo para-legislativo della CGUE, centrale nel percorso di "costituzionalizzazione" di taluni principi e requisiti in materia di sorveglianza massiva: «*the Court of Justice is arguably engaging in an exercise which would appear more legislative than judicial in its character (..). The Court in effect constitutionalizes these detailed requirements*», D. Fennelly, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018, 17; in questo senso, sul percorso di "costituzionalizzazione" della sorveglianza massiva operato dai giudici di Lussemburgo, sia consentito rinviare a E. Celeste - G. Formici, *Constitutionalizing mass surveillance in the EU: civil society demands, judicial activism and legislative inertia*, in *German Law Journal*, in corso di pubblicazione; ma si veda anche F-G. Wilman, *Two emerging principles of EU Internet Law: a comparative analysis of the prohibitions of general data retention and general monitoring obligations*, in *Computer Law & Security Review,* 46, 2022, 1 ss., che considera il divieto di *bulk data retention* come un principio generale della *EU Internet Law*; similmente anche M. Brkan, *Privacy, data protection and the role of European Courts: towards judicialization and constitutionalisation of European privacy and data protection framework*, in G. Gonzalez - R. Van Brakel - P. De Hert (eds.), *Research handbook on privacy and data protection law*, Londra, 2022, 274 ss.

[11] O. Pollicino - M. Bassini, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto penale contemporaneo*, 9 gennaio 2017.

[12] In senso critico M. Tzanou - S. Karyda, *Privacy International and La Quadrature du Net*, cit., che ravvisano nelle più recenti pronunce della CGUE e nel vaglio di proporzionalità ivi promosso, nella parte in cui viene riconosciuta la legittimità della *bulk data retention* per finalità di sicurezza nazionale, un passo indietro rispetto alle tutele previamente affermate. Problematicità, infatti, vengono riscontrate nella distinzione tra scopi di tutela della sicurezza nazionale e di quella pubblica, così come nella determinazione dei diversi limiti affermati dai giudici di Lussemburgo. Sebbene insomma alcuni autori abbiano riscontrato nelle pronunce *Privacy International* e *La Quadrature du Net* «*a culmination of efforts on behalf of the Court to reach a compromise and re-strike the balance between fundamental rights and the (loud and clear) desire of the Member States to uphold data retention schemes in favour of the latter*», essi non hanno mancato di rilevare come «*a clear distinction between the classification of the different public interest objectives may not always be an easy task. In any case, support for such reading does not seem to be widespread, as the judgments have not been received with enthusiasm by the Member States. On the contrary, Member States continue to try to find loopholes to circumvent the Court's findings, even though on initial observation, national courts seem to have followed them. The judicial acceptance of*

dinnanzi alle innegabili problematicità attuative e alle esigenze di garanzia della sicurezza nazionale evidenziate con forza negli anni dagli Stati membri.
Proprio per questa duplicità di profili, tensioni e soluzioni interpretative – che del resto riflettono la già nota difficoltà di attuare i principi di proporzionalità e necessità dinnanzi alle contrapposte spinte securitaria e garantista[13] –, le sentenze *Privacy International* e *La Quadrature du Net* hanno finito col ravvivare il mai sopito dibattito tra i diversi protagonisti del difficile percorso regolatorio della *data retention*.
Per parte della società civile e delle organizzazioni non governative (ONG) attive nell'ambito della tutela dei diritti alla privacy e alla protezione dei dati, la posizione espressa dalla CGUE costituisce il frutto di un mutato approccio più marcatamente pro-securitario, che finirebbe con il comprimere verso il basso le più garantiste tutele determinate nella previa *case law*[14].
Di segno opposto sono invece le perplessità evidenziate da numerosi Stati membri che hanno criticato la rigidità del vaglio di proporzionalità promosso: i limiti e le condizioni sancite condizionerebbero e limiterebbero eccessivamente la possibilità di impiego dei metadati, soprattutto quando ciò sia volto a scopi di lotta alla criminalità. Governi e legislatori nazionali, del resto, hanno sempre mostrato – e ancora mostrano, pur con diversi livelli di intensità – una certa resistenza nel modificare le normative interne in materia di conservazione e accesso ai metadati in senso conforme alla giurisprudenza della CGUE; le riforme che si sono avvicendate in molti Stati membri, pur disponendo salvaguardie più significative e profonde rispetto alle legislazioni dei primi anni 2000, non hanno infatti mai del tutto abbandonato l'imposizione di un obbligo generalizzato e indiscriminato di *retention* per la lotta alla criminalità[15].
Ed è tale complesso intrecciarsi del percorso sovranazionale con le scelte normative nazionali, nonché con l'intervento di società civile e corti interne, ad aver determinato nel tempo il formarsi – e il perdurare – di sentieri paralleli e talvolta divergenti da quello indicato dai giudici di Lussemburgo. Basti pensare alle diverse reazioni scaturite dalla pronuncia *La Quadrature du Net*: mentre il governo francese ha addirittura sottolineato la necessità di ricorrere – nella controversia dinnanzi al *Conseil d'Etat* da cui il rinvio

the permissibility of large-scale surveillance for national security purposes could be seen as a pragmatic approach of the CJEU to end the data retention saga through containing national data retention regimes by ensuring their subjection to significant safeguards and limitations so that large-scale surveillance is the exception rather than the rule», V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 17.

[13] Sul noto e articolato tema del rapporto tra libertà, diritti e garanzia della sicurezza, si rimanda, senza pretesa di esaustività, a Aa. Vv., *Convegno AIC. Libertà e sicurezza nelle democrazie contemporanee*, Padova, 2003; T. Groppi, *Democrazia e terrorismo*, Napoli, 2009; M. Cavino - M.G. Losano - C. Tripodina (a cura di), *Lotta al terrorismo e tutela dei diritti fondamentali*, Torino, 2009; C. Bassu, *Terrorismo e costituzionalismo. Percorsi comparati*, Torino, 2010; M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali*, in *Rivista AIC*, 3, 2016, 1 ss.; G. De Minico, *Costituzione. Emergenza e terrorismo*, Napoli, 2016; C. Graziani, *Sicurezza e diritti in tempi di terrorismo internazionale. Tra endiadi e antitesi*, Napoli, 2022.

[14] Basti pensare alle reazioni espresse dalla ONG StateWatch che ha titolato il proprio commento alle sentenze "*A victory and a defeat for privacy*". Sotto tale profilo, «*the judgment may be seen as primarily a victory for the law enforcement community, the surveillance powers of which have been significantly expanded*», V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 10; si legga anche A. Birrer - D. He - N. Just, *The State is watching you. A cross-national comparison of data retention in Europe*, in *Telecommunications Policy*, 47, 2023, 1 ss.

[15] Queste interpretazioni "difensive" della giurisprudenza della CGUE mirano a far salva la compatibilità con la Carta di Nizza di una forma di conservazione generalizzata, alla quale nessuno Stato membro pare ancora essere disposto a rinunciare del tutto. Sul punto molto chiara è la posizione espressa ad esempio da Europol (*Proportionate data retention for law enforcement purposes*, WK 9957/2017, 21 settembre 2017) che ha criticato la realizzabilità tecnica e l'utilità di una forma di *targeted data retention*.

pregiudiziale aveva tratto origine – al concetto di "*identité constitutionnelle*" per scongiurare l'applicazione dei principi sanciti dalla CGUE nella *data retention saga*[16], il legislatore belga è invece ultimamente giunto ad approvare una disciplina che pare introdurre una forma maggiormente targettizzata di conservazione dei metadati[17], dopo che la Corte costituzionale per ben tre volte aveva dichiarato l'illegittimità della disciplina interna. O ancora si veda quanto avvenuto in Portogallo dove solo recentemente e dopo numerosi anni di attesa si è assistito all'intervento del *Tribunal Constitucional* che ha spinto ad un rinnovato e acceso dibattito sulla necessità di una novella legislazione interna ispirata ai principi determinati dai giudici eurounitari[18]. Un dibattito, questo, che, in maniera simile, si è recentemente riaperto anche in Irlanda, dopo la decisione *Dwyer*[19] e in Germania a seguito della sentenza *SpaceNet*[20].

Questo variegato insieme di sentieri diversi, fatti di provvedimenti normativi e giurisprudenziali anche molto differenti tra loro per soluzioni e tempistiche, consente certamente di individuare un tratto comune: «*the resistance from Member States to the Court's rulings highlights the political struggle between EU institutions and Member States on the future of mass surveillance*»[21]. Un futuro, quello che con difficoltà e incertezza va delineandosi, che non ha certamente visto l'apporto di un altro importante "viaggiatore": il legislatore europeo. Questo non ha fino ad ora contribuito in alcun modo alla determinazione delle tappe e della meta finale del cammino regolatorio della *data retention* e risulta anzi immobile dinnanzi al moltiplicarsi di sentieri nazionali, incapace di ricondurli ad unità e di trovare una risposta di compromesso in grado di ricongiungerli alla strada indicata dalla CGUE.

---

[16] Si fa riferimento al caso deciso dal Conseil d'Etat, 21 aprile 2021, n. 393099. Per alcuni interessanti commenti quanto alla posizione espressa dall'intervenuto governo d'Oltralpe e sulla decisione dei giudici francesi, si leggano L. Azoulai - D. Ritleng - M. Bonini, *«L'État, c'est moi»: il Consiglio di Stato francese, fra salvaguardia della sicurezza nazionale e protezione dei dati (Consiglio di Stato, Section du Contentieux, 21 aprile 2021, French Data Network e a., nn. 393099, 394922, 397844, 397851, 424717, 424718)* , in *CERIDAP*, 26 luglio 2021; J. Ziller, *Il Conseil d'Etat si rifiuta di seguire il pifferaio magico di Karlsruhe*, in *CERIDAP*, 2, 2021, 1 ss.; V. Sizaine, J.-P. Foegle, *Les fausses notes du souverainisme juridique (openedition.org)*, in *La Revue des Droits de l'Homme*, giugno 2021, 1 ss.; M. Audiber, *Conservation des donnees de connexion. Comment le Conseil d'Etat a sauve la majorité des enquete judiciaires*, in *Vielle Juridique*, 96, 2021, 16 ss.; M. Rojszcazak, *The uncertain future of data retention laws in EU: is a legislative reset possible?*, in *Computer Law and Security Review*, 41, 2021, 1 ss.; V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit.; A. Vedaschi, *"Customizing" La Quadrature du Net: The French Council of State, National Security and Data Retention - Brexit Institute (dcubrexitinstitute.eu)*, in *Bridge Blog*, 5 maggio 2021; N. Perlo, *La decisione del Consiglio di Stato francese sulla data retention: come conciliare l'inconciliabile*, in *Rivista di Diritti Comparati*, 2, 2021, 168 ss.

[17] Per un approfondimento sulla giurisprudenza belga nonché sugli ultimi sviluppi normativi in tema, si rinvia a C. Van de Heyning, *The Belgian Constitutional Court's data retention judgment: a revolution that wasn't*, in *Diritti comparati*, 19 aprile 2022; V. Franssen - C. Van de Heyning, *Belgium's new data retention legislation: third time lucky or three strikes and you're out?*, in E. Kosta - I. Kamara (eds), *Data retention in Europe and beyond. Law and policy in the aftermath of an invalidated directive*, Oxford, in pubblicazione (2024). Sia consentito anche di rinviare a G. Formici, *La disciplina della data retention*, cit., con specifico riferimento al capitolo dedicato al Belgio.

[18] T. Violante, *How the Data Retention Legislation Led to a National Constitutional Crisis in Portugal*, in *Verfassungsblog*, 9 giugno 2022; A. Bottacci, *Judgment n. 268/2022 of the Portuguese Tribunal Constitucional and its contribution to the European dialogue on metadata retention and access regimes*, in *European Data Protection Law Review*, 8, 2022, 412 ss.

[19] Per alcune prime riflessioni sul tema, G. Brady, *Ireland, the Dwyer Case, and the 2022 Data Retention Bill – Where do we go from here?* , in *EMILDAI Blog*, aprile 2023.

[20] Una ricostruzione della normativa tedesca e del dibattito politico ingeneratosi a seguito della sentenza *SpaceNet*, è reperibile in T. Wahl, *CJEU: German Rules on Data Retention Not in Line with EU Law*, in *Eucrim*, 15 novembre 2022.

[21] V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 3.

L'introduzione di una specifica normativa sovranazionale in materia di conservazione e acquisizione dei metadati, capace di colmare il vuoto lasciato dalla invalidazione della *Data Retention Directive*[22], non è mai stata perseguita concretamente, nonostante le tante voci che hanno raccomandato e incoraggiato un intervento in tal senso[23]. Anche la proposta di regolamento che dovrebbe sostituire l'ormai vetusta Direttiva *e-Privacy* – e, dunque, il vago art. 15 che rappresenta ad oggi l'unica disposizione sovranazionale in materia di *data retention* per scopi securitari[24] – pare lontana dall'approvazione, bloccata su questioni – tra cui la disciplina della conservazione dei metadati, appunto – rispetto alle quali Commissione, Consiglio dell'UE e Parlamento europeo non riescono al momento a trovare una visione condivisa[25].

Nell'incerto procedere del cammino regolatorio della *data retention*, qui brevemente tratteggiato, vanno allora più recentemente ad inserirsi le Conclusioni dell'Avvocato Generale Collins nel caso C-178/22; queste impongono di esaminare con attenzione il percorso tracciato dai legislatori e dalla giurisprudenza italiana nel necessario e ormai imprescindibile dialogo con la CGUE e le Istituzioni europee. Il presente contributo intende pertanto proporre una prima analisi del contesto nostrano e delle ragioni che hanno condotto al rinvio pregiudiziale del Tribunale di Bolzano; verrà poi svolta una disamina delle Conclusioni dell'Avvocato Generale, per giungere ad alcune considerazioni finali: esse apriranno a profondi interrogativi sul futuro degli strumenti di conservazione e accesso ai metadati tanto a livello nazionale quanto sovranazionale ma anche, più ampiamente, sulle sfide che i diversi "viaggiatori" sono chiamati ad affrontare dinnanzi al proliferare di sofisticati quanto insidiosi sistemi di sorveglianza massiva sempre più digitalizzati ed invasivi.

---

[22] La direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006 , riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE GU 2006 L 105/54, invalidata dalla richiamata pronuncia *Digital Rights Ireland*, non è mai stata sostituita da alcune proposta normativa volta a disciplinare a livello sovranazionale la *data retention*.

[23] In questo senso si sono espressi, ad esempio, D. Fennelly, *Data retention: the life, death and afterlife of a directive*, cit.; L. Lupária, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019, 573 ss.; M. Rojszcazak, *The uncertain future of data retention laws in EU: is a legislative reset possible?*, cit. Il Consiglio dell'UE nel documento Conclusione sulla conservazione dei dati per finalità di lotta contro la criminalità, n. 9336/19 del 27 maggio 2019 aveva affidato alla Commissione il compito di avviare iniziative finalizzate a verificare l'opportunità di una apposita iniziativa legislativa *ad hoc* sulla conservazione dei metadati. L'appello all'adozione di uno strumento regolatorio comune europeo, che sia in grado di determinare una disciplina conforme alle indicazioni emerse dalla giurisprudenza della CGUE e di risolvere così le criticità derivanti dalla molteplicità di soluzioni normative sul territorio europeo, è emersa anche nel dibattito in seno alle Istituzioni europee: nel marzo 2021, infatti, il Ministro della Giustizia del Portogallo – Stato membro cui all'epoca era affidata la Presidenza del Consiglio dell'UE – aveva spinto in tale direzione.

[24] Questo articolo, come noto, attribuisce agli Stati membri una generica facoltà di deroga alla regola generale determinante la cancellazione dei metadati da parte dei *service providers*; gli Stati possono quindi disporre normative nazionali che ordinino la conservazione dei dati esterni delle telecomunicazioni per finalità – solo vagamente definite – di sicurezza nazionale, difesa, sicurezza pubblica, prevenzione, ricerca, accertamento e perseguimento di reati o di uso non autorizzato del sistema di comunicazione elettronica.

[25] Si tratta della Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final. Per approfondimenti sul contenuto della proposta e valutazioni critiche della stessa, soprattutto con riferimento alla disciplina della *data retention*, si leggano le considerazioni svolte dal European Data Protection Board, *Statement 3/2021 on the e-Privacy Regulation* del 9 marzo 2021.

2. Il sentiero italiano: la normativa e la giurisprudenza nazionale dinnanzi alla giurisprudenza della Corte di giustizia dell'Unione europea

2.1. Una necessaria ricostruzione della disciplina italiana in materia di conservazione dei metadati: "l'eterno ritorno del sempre uguale"?

Se, come sopra richiamato, in altri Stati membri dell'UE le decisioni della CGUE in materia di *data retention* hanno condotto, pur con tempi e risultati non omogenei, ad un vivace dibattito politico, legislativo e giurisprudenziale, l'Italia pare invece aver intrapreso un sentiero differente.

Pur non potendo qui ripercorrere nel dettaglio tutte le tappe normative e giurisprudenziali che hanno condotto all'oggi[26], pare utile fornire alcune informazioni essenziali circa l'evoluzione della disciplina in materia: ciò consentirà di cogliere appieno il travagliato rapporto che la "via italiana" ha intessuto con il diritto dell'UE e, in special modo, con la giurisprudenza della CGUE. L'art. 132 del d.lgs. 196/2003 (d'ora in avanti Cod. Privacy) ha infatti subìto solo in tempi estremamente recenti alcune sostanziali modifiche nella direzione di una – ancora solo parziale – "conciliazione" e adattamento ai principi sanciti a livello sovranazionale nella *data retention saga*. Se dunque per anni i giudici e i legislatori nostrani sono apparsi quasi indifferenti – se non più o meno consapevolmente disattenti – alle vicende che hanno animato le riflessioni giuridiche e normative in altri ordinamenti[27], gli interventi riformatori degli ultimi anni non hanno comunque risolto dubbi interpretativi e perplessità quanto alla compatibilità della disciplina nazionale con il diritto europeo e la *case law* dei giudici di Lussemburgo. Tali permanenti dubbi hanno così trovato conferma nel rinvio pregiudiziale promosso dal Tribunale di Bolzano, che ravviva un dialogo con i giudici sovranazionali – come si dirà – raramente attivato in passato.

Procedendo allora con l'analisi della normativa di riferimento, l'art. 132 Cod. Privacy stabilisce innanzitutto un obbligo generale di conservazione dei c.d. "dati esterni delle comunicazioni" per finalità di accertamento e repressione dei reati, prevedendo una *data retention* della durata di 24 mesi per i metadati telefonici, 12 mesi per il traffico telematico e 30 giorni per le chiamate senza risposta[28].

---

[26] Per uno studio dettagliato dell'evoluzione normativa e giurisprudenziale italiana sul tema della *data retention* e acquisizione dei metadati, si rinvia a E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018; R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit.; E. Poddighe, *Art. 132*, in R. D'Orazio - G. Finocchiaro - O. Pollicino - G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021; sia consentito anche il rinvio a G. Formici, *La disciplina della data retention*, cit., nel capitolo dedicato all'ordinamento italiano.

[27] Come rilevato da diversi autori, la giurisprudenza della CGUE in materia di *data retention* non ha suscitato, all'interno dei confini italiani, «l'interesse che meritava, né in dottrina né in giurisprudenza e soprattutto non ha turbato il sonno del legislatore nazionale», S. Marcolini, *L'istituto della data retention dopo la sentenza della CGUE del 2014*, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (a cura di), *Cybercrime*, Milano, 2019, 1591; ciò almeno sino alla sentenza CGUE, C-746/18, *H.K. v. Prokuratuur* (2021).

[28] Questa durata invero ha subìto svariate modifiche nel corso del tempo; per una ricostruzione del succedersi degli interventi normativi in materia, si rinvia a G. E. Vigevani, *Articolo* 132, in Aa. Vv., *Codice della privacy. Commento al D. Lgs. 30 giugno 2003, n. 196, aggiornato alle più recenti modifiche legislative*, Milano, 2004, 1668 ss.; C. Fatta, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*,

La disciplina della conservazione dei metadati per scopi securitari, tuttavia, non risulta essere unicamente regolata dall'art. 132 Cod. Privacy: con diversi interventi normativi, peraltro spesso disordinati e primariamente motivati da esigenze emergenziali[29], culminati da ultimo nella Legge Europea 2017[30], la "regola generale" sancita nella disposizione richiamata è divenuta *de facto* recessiva e residuale. Questo perché la Legge Europea, così come le disposizioni precedenti[31], dispone un obbligo di conservazione dei metadati in deroga a quanto previsto dal Cod. Privacy ed esteso a ben 72 mesi qualora vengano perseguiti scopi di repressione e accertamento di reati di cui agli artt. 51, c. 3-quater e 407, c. 2, lett. a) c.p.p. (terrorismo, saccheggio, associazione di tipo mafioso etc.). È questa durata di conservazione estremamente lunga e senza pari negli altri ordinamenti europei ad essere così divenuta di normale attuazione: poiché non risulta possibile conoscere in anticipo per quali obiettivi possa in futuro essere eventualmente richiesto l'accesso ai metadati, il *service provider* è tenuto a conservare tali dati in maniera generalizzata per il termine massimo di sei anni. Solo al momento della richiesta di accesso da parte dell'autorità giudiziaria, il fornitore di servizi di telecomunicazioni dovrà verificare, a seconda del reato perseguito, quale sia il periodo di conservazione relativo, ossia se quello stabilito dall'art. 132 Cod. Privacy – dunque più breve – o quello più ampio sancito dalla Legge Europea. Di conseguenza, come rilevato anche dal Garante per la Protezione dei Dati Personali, «benchè l'acquisibilità dei dati raccolti oltre il termine ordinario sia limitata a reati particolarmente gravi, proprio la natura retrospettiva di questo strumento investigativo implica la conservazione generalizzata dei dati di traffico per sei anni, salvo poi limitarne l'utilizzabilità processuale ai soli casi normativamente considerati»[32].

L'inversione del rapporto tra disciplina ordinaria e straordinaria è stata rilevata con grande enfasi anche dalla dottrina: molte sono state le critiche mosse tanto con riferimento alla tipologia di intervento normativo prescelto per modificare la regolamentazione della *data retention*, quanto sotto il profilo sostanziale. Rispetto a quest'ultimo, in particolare, sono state evidenziate la durata estremamente lunga della conservazione nonché la sua natura *de facto* generalizzata ed indiscriminata, non essendo stabilito alcun limite circa la tipologia di dati, le aree geografiche o i soggetti interessati dalla *retention*: nessuna targettizzazione della conservazione dei dati viene quindi prevista né nell'art. 132 Cod. Privacy né nelle successive modifiche intervenute

in *Diritto dell'Informazione e dell'Informatica*, 2008, 399 ss.; A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014, 722 ss.; M. Riccardi, *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Diritto penale contemporaneo*, 3, 2016, 170 ss.

[29] Prima con il c.d. d.l. antiterrorismo (d.l. 7/2015, convertito dalla l. 43/2015) e poi con il Decreto milleproroghe del 30 dicembre 2015 (d.l. 219/2015, convertito con l. 21/2016).

[30] L. 167/2017, Legge europea che reca le disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea. Per una lettura di tale disposizione si rinvia a L. Scaffardi, La Data retention va in ascensore, in *Forum di Quaderni Costituzionali*, 28 luglio 2017.

[31] Già con il d.l. 354/2003 veniva infatti previsto per i reati di cui all'art. 407, c. 2, lett. a) c.p.p. e i delitti a danno di sistemi informatici e telematici un ampliamento del periodo di conservazione, aumentato di ulteriori 24 mesi per i dati telefonici e 6 mesi per i dati di traffico telematico rispetto a quanto disposto nell'art. 132 Cod. privacy. Anche in quel caso, come per la modifica apportata dalla Legge europea, i *service providers*, non potendo sapere in anticipo se i metadati da conservare sarebbero serviti per indagini riguardanti qualsiasi reato o solo per quelli più gravi previsti nella normativa del 2003, si trovavano costretti a conservare tutti i metadati per il termine di tempo massimo e quindi più lungo.

[32] Garante per la Protezione dei Dati Personali, *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*, 2 agosto 2021.

mediante normative emergenziali. La presenza di una *bulk data retention*, peraltro significativamente prolungata, ha condotto così molti studiosi a porre in dubbio la compatibilità della legislazione italiana con il diritto dell'UE, soprattutto alla luce delle continue e coerenti pronunce dei giudici di Lussemburgo che hanno chiaramente dichiarato, come si è visto, l'illegittimità di una conservazione generalizzata per scopi di garanzia della sicurezza pubblica e repressione dei reati, quand'anche gravi[33].
Nonostante tali critiche e perplessità, però, in Italia non è mai decollato un serio dibattito sulla necessità di riformare la esaminata disciplina della *data retention*: le occasioni, anche in tempi recenti, non sono certo mancate – pensiamo alle significative modifiche apportate al Cod. Privacy all'indomani dell'entrata in vigore del regolamento UE 2016/679 (GDPR)[34] – ma il legislatore nostrano non è mai intervenuto sul profilo della conservazione dei metadati, neppure nella novella del 2021, di cui si parlerà a breve. A nulla sono valse quindi le sollecitazioni, osservabili anche con sguardo comparato e derivanti da quanto accadeva ed è accaduto in altri ordinamenti dell'UE. L'unico ambito regolatorio che ha visto il Governo e il Parlamento italiano attivarsi nella direzione di una riforma maggiormente garantista e conforme alla giurisprudenza della CGUE è quello attinente alla successiva fase dell'accesso ai metadati da parte delle autorità di indagine. Pare utile ricostruire brevemente le vicende che hanno portato a tale modifica, poiché in esse è possibile cogliere non solo un primo – tardivo – impatto della *case law* europea nell'ordinamento nostrano ma anche i semi delle questioni che emergeranno nel rinvio pregiudiziale oggetto di analisi nel presente contributo.

2.2. La novella del 2021 riguardante la disciplina dell'accesso ai metadati e il difficile dialogo promosso dalle corti nostrane con i giudici di Lussemburgo.

Prima della novella del 2021, l'art. 132 Codice Privacy attribuiva esclusivamente al p.m.

[33] «La locuzione impiegata [nell'art. 132] ricomprende qualunque reato, anche contravvenzionale e di minima gravità od offensività. Una disciplina del genere non può non contrastare con i dettami della CGUE che ha sempre affermato che il mezzo, vista la sua incidenza sul bene della riservatezza, deve applicarsi solo alla lotta contro le forme più gravi di criminalità; (..) l'obbligo italiano di conservazione universale dei dati esterni di ogni singola comunicazione elettronica effettuata da ogni cittadino, a prescindere dal suo ancorché minimo coinvolgimento in un qualsivoglia reato, per la durata di sei anni genera banche dati di sterminata dimensione, idonee a indagini e profilazioni dettagliate, ed esponendo così praticamente l'intera popolazione a quei rischi di abuso ed accesso illecito a più riprese ed accoratamente denunziati dalla giurisprudenza comunitaria. In definitiva, e senza alcun tema di smentita, la declinazione da parte del legislatore italiano delle tre variabili di conservazione dei dati esterni – i reati da contrastare, il tempo di conservazione dei dati, l'oggetto dell'obbligo di conservazione – è attualmente tra le deteriori che si possano immaginare dal punto di vista degli standard minimi di tutela della riservatezza», R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit., 47. Si leggano anche, similmente, L. Scaffardi, *La data retention va in ascensore*, cit.; L. Scudiero, *Data retention a sei anni. La Corte di Giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR*, in questa *Rivista*, 2017, 178 ss.

[34] Sul d.lgs. 101/2018 e sulle limitate e solo formali modifiche apportate in materia di *data retention* e accesso ai metadati, nelle quali si è sostanzialmente riconfermato l'assetto regolatorio precedente e sono state introdotte disposizione di coordinamento rispetto al GDPR, si veda S. Signorato, *Novità in tema di data retention. La riformulazione dell'art. 132 Codice Privacy da parte del D.Lgs. 10 agosto 2018*, in *Diritto penale contemporaneo*, 11, 2018, 157 ss. ma anche R. D'Orazio - G. Finocchiaro - O. Pollicino - G. Resta (a cura di), *Codice della privacy e data protection*, cit.

il delicato compito di vagliare e approvare le richieste di acquisizione dei metadati[35]. Inoltre, nessun limite quanto alla gravità dei reati era indicato neppure sul fronte dell'accesso, che veniva garantito per la repressione di qualsiasi tipologia di reato. La coerente e ricca *data retention saga* non aveva pertanto mai condotto, né con riferimento alla conservazione né rispetto alla disciplina dell'accesso, ad un ripensamento della normativa esistente né avevano mai posto in dubbio la compatibilità della cornice regolatoria nostrana rispetto ai principi sanciti dai giudici sovranazionali.

Un simile approccio trovava peraltro rafforzamento nella giurisprudenza nazionale, definita ormai dai più come portatrice di «orientamenti interpretativi salvifici»[36] o in altri termini, di interventi «rassicuranti», «espressione di un approccio semplicistico ad un tema (..) colmo di nodi irrisolti»[37]. Le corti italiane avevano dunque sempre optato per una lettura «restrittiva degli standard garantistici enunciati dalla CGUE» al fine di «salvare la disciplina interna (..) ed evitare ipotesi di inutilizzabilità probatoria»[38].

In questo contesto, la sentenza della CGUE *H.K. v. Prokuratuur* ha certamente rappresentato una prima significativa – per quanto parziale – spinta verso il cambiamento: tale pronuncia, pur riferendosi ad un caso estone, chiariva infatti i requisiti di terzietà ed indipendenza dei giudici o delle entità indipendenti chiamate ad effettuare il controllo preventivo all'accesso e ribadiva come quest'ultimo fosse da ritenersi limitato unicamente al perseguimento di reati caratterizzati da gravità. I profili di contatto e somiglianza tra la disciplina estone e quella italiana hanno così mosso il Tribunale di Rieti a promuovere il primo rinvio pregiudiziale azionato da giudici italiani in materia di *data retention* e accesso ai metadati[39], cui hanno inoltre fatto seguito alcune interessanti pronunce della Corte di Cassazione. Questa, pur ritenendo non direttamente applicabile la sentenza della CGUE da parte dei giudici nazionali per mancanza di autoesecutività[40], ha nondimeno dichiarato la necessità di un intervento

[35] Anche con riferimento alla disciplina riguardante l'accesso ai metadati conservati sono state disposte, nel corso del tempo, diverse modifiche normative rispetto al dettato originario dell'art. 132 Cod. privacy. Si pensi al c.d. Pacchetto Pisanu (d.l. 144/2015) che sanciva il previo controllo unicamente in capo al p.m., deputato ad emanare un decreto motivato autorizzante l'accesso ai metadati; solo in caso di reati di maggior gravità – quali quelli di cui all'art. 407, co. 1, lett. a) c.p.p. e i delitti a danno di sistemi informativi e telematici – veniva richiesta l'autorizzazione mediante decreto del giudice. Tale intervento veniva poi confermato anche dal successivo d.lgs. 109/2008, che attribuiva unicamente al p.m. il compito di autorizzare le richieste di acquisizione. Per maggiori dettagli, oltre alle fonti già richiamate in questo paragrafo, sia consentito rinviare a G. 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 *Osservatorio costituzionale*, 1, 2022, 125 ss.

[36] Così R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit.

[37] L. Lupária, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, cit.

[38] Ivi, 757. Nel medesimo testo si può ritrovare una utile ricostruzione delle maggiori pronunce delle Corti italiane in materia.

[39] Domanda di pronuncia pregiudiziale C-334/21, promossa dal Tribunale di Rieti, Sez. Penale, Ordinanza del 4 maggio 2021 (procedimento penale contro G.B. e R.H.); tale rinvio si è tuttavia poi concluso con il ritiro della domanda di pronuncia pregiudiziale a causa della riforma normativa del 2021 che ha fatto venir meno l'utilità stessa della pronuncia dei giudici di Lussemburgo rispetto a profili regolatori nel frattempo modificati dallo stesso legislatore nazionale. Sul punto G. Stamponi Bassi, *Acquisizione dei tabulati telefonici e telematici: il Tribunale di Rieti propone questione pregiudiziale alla Corte di Giustizia dell'Unione europea*, in *Giurisprudenza Penale*, 13 maggio 2021 ma anche Ufficio del Massimario e del Ruolo, Servizio Penale della Corte Suprema di Cassazione, *Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, 13 ottobre 2021.

[40] Su questo punto invero la giurisprudenza di merito ha mostrato, prima dell'intervento della Corte

riformatore della normativa italiana in grado di tenere in debito conto i principi della giurisprudenza sovranazionale[41].

Un intervento normativo, quello invocato da più parti, che non si è fatto attendere[42]: non potendo in questa sede vagliare nel dettaglio il percorso normativo che ha condotto al d.l. 132/2021 e le modifiche apportate nella successiva legge di conversione 178/2021, ciò che qui merita innanzitutto rilevare è come il legislatore nazionale abbia apportato una modifica parziale dell'art. 132 Cod. Privacy, nella sola parte attinente alla disciplina dell'accesso, ovvero il c. 3, introducendo poi l'art. 3 bis. Il c. 1 della disposizione in esame, già analizzato precedentemente e determinante l'obbligo di conservazione, non ha invece subìto alcuna riforma – sul punto si tornerà successivamente –. Cercando di conformare la normativa italiana a quanto emerso dalla pronuncia *H.K. v. Prokuratuur*, il legislatore nostrano ha stabilito la legittimità dell'accesso ai metadati solo qualora essi siano rilevanti ai fini della prosecuzione delle indagini nonché quando vi siano sufficienti indizi in ordine a determinate tipologie di reati considerati "gravi". Questi sono individuati nei reati per i quali la legge stabilisce la pena dell'ergastolo o la reclusione non inferiore nel massimo a tre anni – a norma dell'art. 4 c.p.p. – e nei reati di minaccia, molestia o disturbo gravi alle persone col mezzo del telefono. Oltre a queste importanti ed inedite restrizioni, anche il soggetto deputato a vagliare e autorizzare l'accesso è stato modificato, in conformità a quei criteri di indipendenza e terzietà emersi con maggior chiarezza dalla sentenza *H.K. v. Prokuratuur*: i metadati devono ora essere acquisiti sulla base di un decreto motivato del giudice, su richiesta del p.m. o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e di altre parti private[43]. In estrema sintesi, l'intervento del legislatore ha inserito, per la prima volta, una soglia di pena oltre la quale il reato è considerato grave – e quindi in grado di legittimare una ingerenza grave nella sfera personale – e ha altresì innalzato il livello di tutela dei soggetti colpiti dall'accesso prevedendo un intervento del giudice e non del p.m. a scopi autorizzativi preventivi.

Se quanto disposto va certamente nella direzione di un maggior garantismo ed

di Cassazione, approcci ondivaghi e talvolta confliggenti, come emerge ad esempio dalla Tribunale di Milano, VII Sez. Penale, ord. 22 aprile 2021, n. 585 e dal Tribunale di Roma, Sez. G.i.p.-G.u.p., decreto 25 aprile 2021. Su tali pronunce, si rimanda alle valutazioni critiche di J. Della Torre, *L'acquisizione dei tabulati telefonici dopo la Corte di Giustizia: un primo provvedimento garantista del gip di Roma*, in *Sistema Penale*, 29 aprile 2021; C. Parodi, *Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge*, in *ilPenalista*, 3 maggio 2021; A. Malacarne, *Ancora sulle ricadute della CGUE in tema di data retention: il G.i.p. di Roma dichiara il "non luogo a provvedere"* , in *Sistema Penale*, 5 maggio 2021; V. Tordi, *Data retention dopo la CGUE: Trib. Milano nega il contrasto della disciplina italian con il diritto sovranazionale*, in *Sistema Penale*, 7 maggio 2021; F. Torre, *Data retention: una ventata di "ragionevolezza" da Lussemburgo*, in *Consulta Online*, II, 2021, 540 ss.; ma anche A. Ciprandi, *La Cassazione sull'utilizzabilità dei tabulati acquisiti prima del DL 132/2021*, in *Sistema Penale*, 22 febbraio 2022.

[41] Nella sentenza n. 33116 del 7 settembre 2021, similmente a quanto già statuito nella pronuncia n. 28523 del 22 luglio 2021, la Corte di Cassazione ha ritenuto la sentenza *H.K. Prokuratuur* non direttamente applicabile dai giudici nazionali per mancanza di auto-esecutività. Il riconoscimento della importanza di una modifica della normativa vigente si pone in discontinuità rispetto alla previgente giurisprudenza delle Corti italiane (ad es. rispetto all'Ordinanza del Tribunale di Padova del 15 marzo 2017, Pres. Marassi o alla sentenza del 25 settembre 2019, n. 48737 della Cassazione stessa).

[42] L'Ordine del giorno 9/2670-A/10 del 1° aprile 2021, adottato dal Governo italiano, dimostra l'attenzione rinnovata e l'impegno a riformare la normativa nazionale all'epoca vigente sulla base dei principi sanciti dalla giurisprudenza della CGUE.

[43] Viene prevista una disciplina d'urgenza che consente al p.m. di disporre direttamente l'acquisizione dei metadati mediante proprio decreto, che deve tuttavia poi essere oggetto di apposita convalida.

attenzione ai requisiti sanciti a livello sovranazionale, interrompendo quella indifferenza e "disattenzione" caratterizzante la giurisprudenza ma anche il dibattito normativo italiano fino a quel momento, la riforma delineata ha nondimeno fatto sorgere alcune valutazioni critiche. Se ne vogliono riportare solo alcune, utili anche a comprendere la posizione assunta dal giudice di Bolzano nel rinvio pregiudiziale oggetto di analisi. Innanzitutto, dubbi sono emersi quanto alla soglia di gravità indicata: essa finisce invero col ricomprendere la gran parte dei delitti inseriti nel codice penale, così che la disposizione novellata darebbe solo «l'illusione di aver effettuato una delimitazione del perimetro delle violazioni ma in realtà non lascia fuori che le contravvenzioni e pochi delitti di davvero infima gravità»[44]. Inoltre non è mancato chi ha scorto nella determinazione in via astratta e generale di una soglia di pena, oltrepassata la quale si produce una «presunzione assoluta di proporzionalità, indipendentemente dalla valutazione del caso concreto», una soluzione incapace di rispondere ai profili di incompatibilità con il diritto eurounitario; dovrebbe, al contrario, essere «assolutamente indispensabile integrare la valutazione effettuata dal legislatore con quella operata dal giudice in concreto, valutando le peculiarità del caso di specie ed utilizzando i parametri indicati nel nuovo art. 132 (sussistenza dei sofficienti indizi di reato e rilevanza ai fini della prosecuzione delle indagini)»[45].

Ebbene proprio dai limiti e criticità[46], emersi all'indomani della riforma promossa dal legislatore nazionale, ha avuto origine il rinvio pregiudiziale che ci si appresta ad esaminare, nel quale è possibile ravvisare un primo e più significativo allontanamento – la cui portata è però ancora tutta da verificare – dalla previa interpretazione "salvifica" della normativa nazionale assunta dalle corti nostrane in passato.

Il caso da cui il rinvio prende le mosse trae origine da due procedimenti penali per furto aggravato di telefoni cellulari, nel corso dei quali il p.m. della Procura di Bolzano aveva avanzato al giudice del Tribunale richiesta di accesso a tutti i metadati conservati dalle compagnie telefoniche, relativi ai due dispositivi rubati[47]. Sulla base del già richiamato art. 132 Cod. Privacy, modificato dal d.l. 132/2021, i reati di cui agli artt. 624 e 625

---

[44] R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit., 54.

[45] F. Zani, *L'ingerenza nel diritto fondamentale alla vita privata ed alla riservatezza alla luce della recente sentenza della Corte di Giustizia 2 marzo 2021 tra principi dell'Unione europea e principi costituzionali*, in *Osservatorio costituzionale*, 6, 2021, 482.

[46] Sul punto, per una ampia e puntuale riflessione sull'evoluzione normativa in tema di *data retention*, si legga A. Malacarne - G. Tessitore, *La ricostruzione della normativa in tema di data retention e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?*, in *Archivio penale*, 3, 2022, 1 ss. Si consenta di rinviare altresì a G. Formici, *'The three Ghosts of data retention'*, cit., per una disamina delle posizioni, anche critiche, espresse dalla dottrina all'indomani della approvazione del d.l., soprattutto con riferimento all'introduzione del vaglio preventivo in capo al giudice e non più al p.m. e alla determinazione della soglia di gravità. Si fa riferimento alle posizioni espresse, tra gli altri, da F. Filippi, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi* , in *Penale. Diritto e procedura*, 1 ottobre 2021; G. Amato, *Nella costruzione normativa si è sminuito il ruolo del p.m.*, in *Guida al diritto*, 39, 2021, 22 ss.; F. Rinaldini, *La nuova disciplina del regime di acquisizione dei tabulati telefonici e telematici: scenari e prospettive*, in *Giurisprudenza penale*, 10, 2021, 1 ss.; G. Pestelli, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici,* in *Quotidiano giuridico*, 4 ottobre 2021; V. Palladini, *Data retention e privacy in rete: verso una regolazione conforme al diritto UE?*, in *Rivista italiana di informatica e diritto*, 1, 2022, 103 ss.

[47] In particolare, si fa riferimento a «utenze ed eventualmente codici IMEI chiamati/chiamanti, siti visitati/raggiunti, orario e durata della chiamata/connessione ed indicazione delle celle e/o ripetitori interessati, utenze ed IMEI mittenti/destinatari degli SMS o MMS e, ove possibile, generalità dei relativi destinatari) delle conversazioni/comunicazioni telefoniche e connessioni effettuate, anche in roaming, in entrata e in uscita anche se chiamate prive di fatturazione (squilli) dalla data del furto fino alla data della elaborazione della richiesta».

c.p. rientrano nel novero dei reati "gravi", essendo per gli stessi stabilita una pena di reclusione non inferiore nel massimo a tre anni.
Dinnanzi a tale disposizione, come attuata nel caso concreto, tuttavia, il giudice di Bolzano ha mostrato rilevanti perplessità quanto alla conformità rispetto al diritto dell'UE, come interpretato dalla CGUE, soprattutto nelle pronunce *Ministerio Fiscal* e *H.K. Prokuratuur*. In queste decisioni, infatti, viene ribadito con chiarezza come l'accesso a dati che consentono di trarre precise conclusioni sulla vita privata di un utente costituisca una grave ingerenza nei diritti fondamentali, in particolare quelli di cui agli artt. 7, 8 e 52 della Carta di Nizza. Una tale significativa compressione dei diritti e delle libertà dovrebbe pertanto essere legittimata unicamente dal perseguimento di obiettivi di lotta alla criminalità *grave* e solo a condizione che l'accesso sia subordinato a forme di controllo preventivo da parte di un giudice o di una entità amministrativa indipendente[48]. Considerando tali principi, a parere del giudice di Bolzano il limite edittale sancito dal novellato art. 132 Cod. Privacy, finirebbe, come nel caso concreto, per consentire una ampia acquisizione di tabulati telefonici anche per reati che, nella realtà dei fatti, «destano scarsissimo allarme sociale»[49] e mancano di quel necessario elemento di gravità affermato nella *case law* sovranazionale.
Il giudice italiano, sulla base della normativa interna, si troverebbe inoltre *obbligato*, secondo la lettura del Tribunale del rinvio, ad autorizzare l'accesso ai metadati ogniqualvolta ricorrano le condizioni sancite dall'art. 132 (sufficienti indizi di reato e rilievo dei dati ai fini dell'accertamento del reato), senza poter esercitare, cioè, alcuna valutazione specifica sulla concreta gravità del reato nella fattispecie realizzata. L'approvazione della richiesta di acquisizione risulterebbe quindi imposta in caso di raggiungimento della sola soglia di gravità sancita dal legislatore in maniera astratta, esulando dalla considerazione della reale gravità del reato perseguito e di quel nesso conseguenziale e di proporzionalità individuato tra la ingerenza significative nella sfera privata e il necessario perseguimento di un reato dotato di carattere di gravità.
Sulla base di tali valutazioni, che paiono peraltro tenere in conto quelle riflessioni critiche avanzate anche dalla dottrina all'indomani della riforma normativa e più sopra richiamate, il giudice di Bolzano ha deciso quindi di rimettersi alla CGUE affinché questa possa esprimersi «in ordine alla questione se l'art. 15 direttiva 2002/58/CE, così come interpretato nella sentenza C-746/18, osti ad una normativa nazionale che genericamente e senza differenziare tra i vari tipi di reato impone, in presenza di sufficienti indizi di reato, l'acquisizione dei tabulati telefonici per reati puniti con una pena non inferiore nel massimo a tra anni di reclusione e la multa»[50].

---

[48] *Ex multis*, per una lettura approfondita della pronuncia *H.K. v. Prokuratuur*, si veda I. Revolidis, *H.K. v. Prokuratuur: on balancing crime investigation and data protection (Opinion og AG Pitruzzella)*, in *European Data Protection Law Review*, 2, 2020, 319 ss.; E. Andolina, *Ancora una pronuncia della Grande Camera della Corte di Giustizia UE in tema di condizioni di accesso ai traffic data*, in *Processo penale e giustizia*, 5, 2021, 1204 ss.; S. Rovelli, *Case Prokuratuur: proportionality and the independence of Authorities in data retention*, in *European Papers*, 1, 2021, 199 ss.; B. Brunessen, *Chronique Droit européen du numérique. Les précisions sur l'interprétation et l'application du régime de l'e-privacy*, in *Revue trimestrielle du Droit européen*, 3, 2022, 481 ss.; G. Naddeo, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia*, in *Freedom, security & justice : european legal studies*, 2, 2022, 188 ss.; sia consentito anche il rinvio a G. Formici, *La sentenza H.K. c. Prokuratuur e il difficile dialogo tra CGUE e Stati membri in materia di conservazione e accesso ai metadati per finalità securitarie*, cit.

[49] Come si legge nell'Ordinanza di domanda di pronuncia pregiudiziale alla Corte di giustizia dell'UE (art. 267 TFUE) disposta dal Tribunale di Bolzano, Giudice delle indagini preliminari, RGNR 9794/ignoti 2021 e RGNR 9228/ignoti 2021.

[50] *Ibidem*.

3. La direzione indicata dalle Conclusioni dell'Avvocato Generale Collins nel caso C-178/22

Nelle sue Conclusioni, l'Avvocato Generale ripercorre utilmente i principi e requisiti di proporzionalità e necessità indicati dalla CGUE nella sua costante giurisprudenza; con riferimento, in particolare, ai metadati di traffico e localizzazione, in grado di rintracciare e identificare fonte e destinazione di una comunicazione, viene ribadito quanto già precisato nelle pronunce *Ministerio Fiscal* e *H.K. v. Prokuratuur*: la necessaria sussistenza di un reato grave per giustificare l'accesso a metadati in grado di fornire informazioni precise sulla vita dell'utente e quindi determinanti una ingerenza grave nei diritti alla riservatezza e alla protezione dei dati[51].

È proprio partendo da tali premesse che l'Avvocato Generale Collins legge il rinvio del Tribunale di Bolzano come la richiesta di un chiarimento e una maggior specificazione tanto della nozione di gravità del reato quanto del tipo di controllo *ex ante* che l'autorità giudiziaria è chiamata a svolgere dinnanzi a disposizioni nazionali, come quelle di cui all'art. 132 Cod. Privacy italiano, che impongono di autorizzare l'accesso qualora il reato superi la soglia di gravità stabilita dal legislatore stesso.

Ecco allora che l'Avvocato Generale osserva innanzitutto come né la Direttiva *e-Privacy* né la giurisprudenza della CGUE forniscano alcuna nozione del termine "reato" e tanto meno di "reato grave". Ne deriva, come sostenuto anche dalla Commissione e dagli Stati membri che hanno presentato osservazioni alla Corte, che sia da porsi in capo ai legislatori nazionali il compito di definire i reati che consentono l'accesso ai metadati. Ciò anche riconoscendo che «la definizione dei reati e delle sanzioni

[51] Del resto il caso *Ministerio Fiscal* presenta talune somiglianze e punti di incontro nonché alcune distinzioni rispetto ai fatti e alle questioni giuridiche poste alla base del rinvio italiano in esame: anche nelle vicende spagnole, infatti, le indagini prendevano avvio dal furto di un cellulare. In quell'ordinamento, tuttavia, diversamente da quanto disposto dalla normativa italiana vigente, il furto non rientrava nella definizione di "reato grave" fornita dal legislatore nazionale che fissava la soglia di gravità in caso di pena detentiva superiore a 3 anni, non intercorrente nel caso di specie. Il giudice istruttore spagnolo, quindi, si trovava nella condizione di dover negare l'emanazione dell'ingiunzione volta all'accesso ai metadati – e in particolare quelli identificativi – richiesta dalla polizia investigativa. Dinnanzi a tale situazione, il giudice del rinvio si era però chiesto se la normativa nazionale fosse compatibile con i principi fissati dal diritto dell'UE con riferimento al requisito della gravità del crimine legittimante l'intrusione nella sfera privata. Ebbene, in quel caso la CGUE non si era spinta – come si dirà anche a breve – ad identificare e specificare i criteri di determinazione della gravità del reato bensì aveva affermato un solo primo rilevante principio: i giudici nazionali, dinnanzi alla richiesta di accesso ai metadati, sono chiamati a valutare innanzitutto se la compressione dei diritti fondamentali sia di gravità e profondità tale da richiedere la sussistenza di un reato grave. Nello specifico caso spagnolo i dati richiesti dalla polizia non riguardavano né la localizzazione né i dettagli delle comunicazioni svolte, bensì si limitavano esclusivamente ai dati identificativi dei titolari di carte SIM attivate con il telefono rubato, che venivano richiesti peraltro per un arco di tempo estremamente limitato. Considerati tali profili, la CGUE aveva rinvenuto un'ingerenza non grave nella sfera privata dei soggetti potenzialmente colpiti dall'accesso, così che non si rendeva necessaria la sussistenza di un obiettivo di lotta alla criminalità grave al fine di concedere l'acquisizione dei dati. Oltre a questo vaglio di proporzionalità, i giudici di Lussemburgo non mancavano però di indicare alcuni principi e considerazioni di rilievo anche per il rinvio italiano e infatti ripresi nelle Conclusioni qui analizzate: in primis che i dati relativi a traffico ed ubicazione permettono di ricostruire abitudini, relazioni sociali e frequentazione di luoghi dei soggetti interessati, rappresentando così una ingerenza grave rispetto alla quale a nulla rilevano considerazioni quanto alla durata del periodo per il quale l'accesso viene richiesto o alla quantità di dati acquisiti. La CGUE ha infatti ribadito come anche l'accesso ad un quantitativo limitato di dati o per un breve periodo soltanto risulti comunque idoneo a trarre informazioni precise sulla vita privata dell'utente, tali da richiedere quindi la sussistenza di un reato grave. Queste valutazioni sono certamente di estrema importanza per guidare il giudice o l'autorità amministrativa indipendente nella fase di vaglio di proporzionalità e controllo preventivo.

riflette le sensibilità e le tradizioni nazionali, che variano notevolmente non soltanto da uno Stato membro all'altro, ma anche nel corso del tempo, parallelamente rispetto alle trasformazioni della società», § 28. Gli Stati membri, dunque, sono competenti a definire i criteri di gravità nelle proprie normative nazionali in materia di *data retention* e accesso ai metadati.

Occupandosi, in tale contesto, del residuale ruolo di controllo esercitabile dal giudice dinnanzi alla richiesta di accesso, l'Avvocato Generale propone un ragionamento articolato che merita qui di essere analizzato con attenzione. Sulla base della sentenza *H.K. v. Prokuratuur*, innanzitutto, viene riaffermato come la deroga alla riservatezza dei dati di comunicazione debba rappresentare una eccezione e non una regola generale: l'interpretazione restrittiva dell'art. 15 Direttiva *e-Privacy* impone di conseguenza che vengano rispettati i principi di equivalenza, effettività e proporzionalità, così che «l'obiettivo della lotta contro la criminalità grave deve sempre essere conciliato con il godimento dei diritti fondamentali in tal modo pregiudicati», § 32. Le disposizioni nazionali in materia devono pertanto consentire e prevedere non solo un controllo preventivo da parte di un'autorità giudiziaria o amministrativa indipendente ma anche che l'autorità così individuata «concili i diversi interessi e diritti in gioco, al fine di garantire un giusto equilibrio tra le necessità di indagine e della salvaguardia dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali degli interessati», § 33. È da questa considerazione che l'Avvocato Generale fa derivare le sue considerazioni sul ruolo del giudice, partendo però da una premessa rilevante: la legge italiana fissa in modo chiaro e preciso le condizioni alle quali il giudice deve consentire l'accesso ai dati (§ 34); in linea generale, e sempre considerando la norma nazionale in astratto, l'Avvocato Generale si spinge infatti ad affermare che «sebbene l'art. 132 riguardi, potenzialmente, un'ampia gamma di reati, la Corte [di giustizia dell'UE] non dispone, nell'ambito del presente procedimento, di alcun elemento idoneo a dimostrare che in esso ricada un numero talmente elevato di reati da rendere l'accesso ai dati ai sensi di tale disposizione la regola anziché l'eccezione. La soglia della reclusione non inferiore nel massimo a 3 anni non appare eccessivamente bassa», § 35.

Nonostante questa valutazione, l'Avvocato Generale si affretta però ad evidenziare come sia necessario osservare anche l'applicazione pratica e concreta dell'art. 132. Quest'ultimo stabilisce l'obbligo di autorizzazione dell'accesso ai metadati qualora tali informazioni «siano rilevanti per l'accertamento dei fatti e sussistano sufficienti indizi della commissione di un reato di minaccia e di molestia o disturbo alle persone per mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi» § 36) o della commissione di reati puniti, segnatamente, con la pena della reclusione non inferiore nel massimo a tre anni (§ 38). Secondo la lettura dell'Avvocato Generale, è possibile così identificare due distinti livelli di controllo preventivo che il giudice italiano è chiamato ad operare: nel primo caso, quando cioè sussiste un reato di minaccia e di molestia o disturbo alle persone per mezzo del telefono, viene richiesta una valutazione individuale, nel caso concreto, «della questione se l'ingerenza nei diritti sia proporzionata rispetto all'obiettivo di interesse generale della lotta contro la criminalità», § 36. Qualora invece si tratti della commissione di reati puniti con la pena della reclusione non inferiore nel massimo a tre anni, il giudice si trova limitato a stabilire solamente «che i requisiti oggettivi ricorrano, senza alcuna possibilità di effettuare una valutazione individuale degli interessi in gioco», § 38. I giudici nazionali, in tal caso, non parrebbero quindi essere competenti a sindacare e mettere in discussione la determinazione della soglia di gravità stabilita dal legislatore, che da sola basterebbe a limitare la valutazione e il ruolo del giudice nel concedere l'autorizzazione.

Su tale specifico punto l'Avvocato Generale giunge ad una considerazione di grande importanza: i giudici devono «*in ogni caso* essere competenti a effettuare una valutazione individuale" quanto alla proporzionalità della concessione dell'accesso (..) a dati sensibili che consentono di trarre precise conclusioni sulla vita privata dell'utente», § 39 (corsivo aggiunto). In questo modo, anche nel caso in cui sussista una soglia di gravità sancita per via legislativa, deve essere lasciato in capo ai giudici non tanto – o non solo – il compito di sancire il raggiungimento della gravità stabilita per legge, bensì – e questo è ciò che interessa maggiormente – l'onere di svolgere una valutazione o controllo individuali sulla proporzionalità della ingerenza rispetto all'obiettivo di lotta contro la criminalità nel caso concreto (§ 40). Ne consegue che «in taluni casi, l'accesso a siffatti dati può essere negato anche qualora il reato raggiunga la soglia di gravità prevista dal diritto nazionale» (§ 40), così lasciando un ruolo importante di discrezionalità e di considerazione concreta all'autorità di controllo, che non deve ritenersi in toto vincolata alle considerazioni del legislatore. Nel caso, quindi, in cui la soglia di gravità fissata per legge non venga raggiunta, il giudice del rinvio non potrà concedere l'accesso ai dati. Nel caso però in cui tale soglia sia superata, il giudice non è obbligato ad autorizzare l'accesso ma deve piuttosto controllare se «alla luce di tutte le circostanze che caratterizzano lo specifico caso di cui trattasi, l'ingerenza nei diritti fondamentali determinata dalla concessione dell'accesso (..) sia proporzionata all'obiettivo di interesse generale della lotta contro tale reato», § 42.

Nel caso concreto a lui sottoposto dal giudice italiano, l'Avvocato Generale sembra suggerire di considerare, ai fini della determinazione di questo rapporto di proporzionalità, tutti i diritti e gli interessi pertinenti, «compresi, segnatamente, i danni causati ai diritti di proprietà delle vittime tutelati dall'art. 17 della Carta [di Nizza], nonché il fatto che i telefoni cellulari possono contenere informazioni altamente sensibili relative alla vita privata, professionale e finanziaria dei loro proprietari. L'accesso ai dati in parola può inoltre essere l'unico mezzo efficace disponibile per indagare e perseguire i reati di cui trattasi e per garantire che i loro autori, al momento ignoti, non restino impuniti. Anche i diritti dei terzi devono essere presi in considerazione» (§ 42), valutando ad esempio, per quanto attiene ai diritti dei terzi – quali le vittime del reato –, se l'accesso ai dati è ristretto nel tempo e se sussistono garanzie processuali nel diritto italiano volte ad assicurare sia la distruzione di tutti i dati che, a seguito dell'accesso, non siano utili al fine dell'individuazione degli autori del furto, sia l'impossibilità di utilizzare i dati acquisiti in violazione dell'art. 132 Cod. Privacy.

Ne deriva, pertanto, come il diritto dell'UE non osti a una legge nazionale «che impone al giudice di autorizzare il p.m. ad accedere a dati legittimamente conservati dai fornitori (..) che consentono di trarre precise conclusioni sulla vita privata di un utente, qualora i dati siano rilevanti per l'accertamento dei reati e sussistano sufficienti indizi della commissione di un reato grave, come definito dal diritto nazionale, punito con la pena della reclusione non inferiore nel massimo a 3 anni. Prima di concedere l'accesso, il giudice nazionale deve effettuare una valutazione individuale della questione se l'ingerenza nei diritti fondamentali (..) sia proporzionata, alla luce, segnatamente, della gravità del reato in discussione e dei fatti del caso di cui trattasi», § 44.

Se, in definitiva, viene confermata la legittimità della scelta del legislatore italiano quanto alle condizioni e alla soglia di gravità individuata, viene al contempo lasciato un margine di valutazione al giudice che deve svolgere le proprie considerazioni quanto alla proporzionalità dell'ingerenza, indipendentemente – e quindi non esclusivamente – dal raggiungimento della soglia di gravità del reato. Ne emerge un rafforzamento del potere attribuito ai giudici, perché l'autorizzazione all'accesso resta comunque subordinata al

controllo di proporzionalità svolto dai giudici stessi. Una interpretazione del diritto dell'UE e della previa giurisprudenza della CGUE che lascia quindi un significativo margine di azione ai giudici nel controllo *ex ante* e che consente di limitare la rigidità della scelta del legislatore nazionale nella definizione di gravità del reato.

4. Tante tappe ma quale meta? La difficoltà di scorgere un punto di arrivo

Nella decisione qui analizzata sono presenti senza dubbio forti elementi di continuità con la giurisprudenza elaborata dalla CGUE, soprattutto con riferimento alle pronunce *Ministerio Fiscal* e *HK v. Prokuratuur*: il parallelismo tra gravità dell'ingerenza e gravità del reato viene riaffermato con chiarezza e viene individuato come il primo necessario vaglio da effettuare nella fase di accesso ai metadati. Solo in caso di ingerenza grave, che è da riscontrarsi qualora la quantità e qualità dei metadati richiesti siano tali da rivelare informazioni precise sulla vita dell'utente, si renderà necessaria la sussistenza di un reato grave.
L'Avvocato Generale Collins, tuttavia, sembra aggiungere un ulteriore tassello a questa già nota ricostruzione: verrebbe meno, infatti, la correttezza assoluta dell'equazione "gravità dell'ingerenza + gravità del reato = concessione dell'autorizzazione all'accesso". In altri termini, ciò che viene messo in discussione è quell'automatismo che vedrebbe il giudice obbligato ad assicurare l'accesso ai metadati sulla base del mero raggiungimento della soglia di gravità del reato perseguito. Se il carattere di gravità predeterminato dal legislatore è certamente una delle condizioni necessarie alla concessione dell'accesso, esso non dovrebbe essere il solo ed unico: va sommato, piuttosto, ad un controllo individuale del giudice – o dell'autorità amministrativa indipendente – volto a determinare la proporzionalità dell'ingerenza rispetto all'obiettivo di interesse generale, con riferimento allo specifico caso concreto e considerati tutti gli elementi di fatto e gli interessi in gioco.
In questo senso, le Conclusioni dell'Avvocato Generale valorizzano certamente il ruolo del giudice e la profondità del vaglio preventivo, consentendo di raggiungere esiti diversi: concedere l'acquisizione dei metadati di localizzazione e ubicazione – determinanti quindi una ingerenza grave – anche per reati che, pur superando la soglia di gravità determinata per legge, non destino particolare allarme sociale, qualora l'ingerenza sia proporzionata all'interesse perseguito; o, al contrario, negare l'accesso, anche in presenza di reato grave, nel caso in cui non sussista un interesse pubblico tale da giustificare l'ingerenza nella sfera personale. Questo ulteriore vaglio potrebbe allora risultare in un approccio maggiormente garantista dei diritti fondamentali, permettendo di prendere in considerazione i fatti concreti e determinando così la possibilità di limitare l'accesso ai metadati anche quando il legislatore nazionale abbia individuato una soglia estremamente bassa di gravità. In questa situazione, l'ulteriore e aggiuntivo vaglio di proporzionalità del giudice potrebbe contribuire a correggere le distorsioni derivanti dall'utilizzo del criterio di gravità quale unico e vincolante elemento di valutazione ai fini dell'acquisizione. Ovviamente un simile esito in senso maggiormente garantista, dipenderebbe in ogni caso dal livello di approfondimento e attenzione dedicato al vaglio di proporzionalità ulteriore. Le Conclusioni dell'Avvocato Generale finiscono, pertanto, col limitare il valore della scelta normativa generale ed astratta del decisore politico, per riconoscere un aggiuntivo livello di tutela rappresentato dal controllo *ex ante*.

Nulla viene detto, invece, quanto alla determinazione dei criteri che i legislatori dovrebbero considerare per individuare la soglia di gravità del reato: questo profilo, del resto, non era stato toccato nemmeno nel caso *Ministerio Fiscal*, nel quale pure il giudice del rinvio aveva espressamente promosso un quesito sul punto. In quel caso l'Avvocato Generale Saugmandsgaard Øe si era spinto a fornire alcune indicazioni in merito[52], poi non riprese tuttavia nella decisione della CGUE. Nelle Conclusioni in esame, invece, viene solo ribadito come la determinazione della gravità non possa risultare nel tramutare l'eccezione in regola, determinando cioè una soglia così bassa da includere *de facto* tutti i reati previsti dall'ordinamento e facendo venir meno il significato stesso del requisito di gravità. In assenza di disposizioni a livello sovranazionale che forniscano una definizione di "reato grave", tale onere viene poi riconosciuto in capo agli Stati membri che, per tale determinazione, possono tenere conto di diversi fattori, in misura variabile, tra i quali certamente emerge con evidenza la gravità della sanzione prevista[53].
Dinnanzi a tali considerazioni derivanti dalla lettura delle presenti Conclusioni, è possibile ora trarre due ordini di riflessioni: una prima riferita specificamente all'ordinamento italiano e una seconda, più ampia, sul possibile futuro della *data retention* nell'UE.
Partendo dal primo profilo, non si può che rilevare come le Conclusioni dell'Avvocato Generale, qualora confermate dalla CGUE, possano rappresentare l'occasione per rivitalizzare il dibattito nostrano in materia di conservazione e accesso ai metadati. In particolare, il riconoscimento della facoltà, in capo ai giudici, di effettuare un vaglio capace anche di slegarsi dalla valutazione della mera soglia di gravità imporrebbe di ripensare il novellato art. 132 Cod. Privacy, con specifico riferimento alla prevista obbligatorietà della concessione dell'acquisizione dei metadati in base alla mera sussistenza dei requisiti definiti nella disposizione. Una tale riflessione dovrebbe condurre ad una interpretazione – o una riscrittura – della normativa stessa in grado di affermare con chiarezza una maggiore discrezionalità del giudice e un margine valutativo ampio quanto alla proporzionalità dell'accesso nel caso concreto. Ciò andrebbe peraltro a corroborare talune critiche, inizialmente avanzate da parte della dottrina, che mettevano in guardia quanto alla correttezza e compatibilità con il diritto dell'UE di valutazioni e controlli unicamente fondati sui criteri astratti determinati dal legislatore e che rivendicavano quindi il potere del giudice di vagliare anche le circostanze del caso concreto[54] ai fini della concessione o meno dell'autorizzazione.
Se simili analisi potranno certamente promuovere un dibattito futuro e una possibile

[52] Nel caso CGUE, C-207/16, *Ministerio Fiscal* (2018), la CGUE, riformulando il quesito posto dal giudice del rinvio, non era giunta ad affrontare la questione attinente alla individuazione dei criteri di gravità dei reati. L'Avvocato Generale, invece, aveva svolto valutazioni in tal senso, affermando innanzitutto come non fosse possibile fissare una soglia di gravità così bassa «da far diventare principio l'eccezione», § 114, negando poi la natura di nozione autonoma del diritto dell'UE della definizione di "reato grave" e quindi fornendo solo in subordine alcune indicazioni e criteri sulla base dei quali fondare la valutazione di gravità (§ 105). Secondo l'Avvocato Generale, quest'ultima non dovrebbe comunque basarsi unicamente sul *quantum* della pena e dunque su un criterio meramente formale (§ 121); veniva infine evidenziato come la soglia suddetta non dovesse essere determinata in via giurisprudenziale: «poiché una simile determinazione richiede una valutazione complessa e potenzialmente soggetta a evoluzione, occorre a mio avviso restare prudenti a questo proposito e riservare tale operazione alla valutazione dei legislatore dell'Unione, nella sfera delle competenze conferite a quest'ultima, o alla valutazione del legislatore di ciascuno Stato membro, entro i limiti dei requisiti derivanti dall'Unione», § 117.

[53] «La durata di una pena detentiva può riflettere l'analisi di una serie di fattori tra i quali la gravità intrinseca percepita di un reato e la sua gravità relativa rispetto ad altri reati», § 29.

[54] Sul punto si rinvia alle riflessioni critiche di F. Zani, *L'ingerenza nel diritto fondamentale alla vita privata ed alla riservatezza alla luce della recente sentenza della Corte di Giustizia 2 marzo 2021 tra principi dell'Unione europea e principi costituzionali*, cit.

riforma della disciplina nazionale vigente in materia di acquisizione dei metadati, non può non essere evidenziato come tale disamina critica sia unicamente limitata al profilo dell'accesso. Il giudice del rinvio, infatti, nulla ha detto – né ha interrogato la CGUE – quanto alla fase previa di conservazione e alla disciplina che la regola: nessun profilo di problematicità, insomma, è stato identificato con riferimento ad un obbligo di conservazione che rimane generalizzato e indiscriminato e che rappresenta, quindi, a parere di molti, la «violazione più grave»[55] operata dalla normativa italiana rispetto al diritto dell'UE, tanto sotto il fronte della estensione della *retention* – tutto fuor che targettizzata –, quanto della durata, macroscopicamente sproporzionata e lontana dalle soluzioni normative adottate – o in corso di discussione – in altri ordinamenti[56].

Un commento delle Conclusioni dell'Avvocato Generale Collins nel caso analizzato non può, in tal senso, esimersi da una considerazione più approfondita del contesto italiano e delle problematicità riguardanti la normativa attuale in materia di *data retention*: se l'intervento riformatore del 2021 ha senza dubbio il pregio di aver – per la prima volta – osservato con serietà la giurisprudenza della CGUE[57], esso è nondimeno caratterizzato da modifiche "selettive", riguardanti solo un aspetto determinato – quello dell'accesso. Ignorando i moniti del Garante per la Protezione dei Dati Personali[58], la scelta del Governo, prima, e del Parlamento, poi, è stata quella di avviarsi per un sentiero ancora significativamente lontano da quello segnalato dalla giurisprudenza dei giudici di Lussemburgo. Sebbene la direzione di tale ultimo percorso sia ancora difficile da determinare con chiarezza, come si dirà a breve, il compito del legislatore nazionale dovrebbe nondimeno essere quello di promuovere – grazie anche all'impulso della società civile e delle corti – un dibattito attento, capace di considerare quei principi e requisiti già indicati dalla CGUE e verso i quali sempre più Stati membri – certo, non senza difficoltà – stanno cercando di tendere. Stimolare una riflessione più ampia e complessiva sulla disciplina della *data retention* e dell'acquisizione dei metadati, che prescinda da interventi emergenziali, a tratti confusi e sovrapposti[59], rappresenterebbe senza dubbio il primo importante segnale di un cambio non solo di passo ma anche di strada. Una tale riflessione dovrebbe muovere dalla comprensione piena della delicatezza e complessità del corretto contemperamento tra libertà e potere, diritti fondamentali e tutela della sicurezza dinnanzi al proliferare di strumenti di sorveglianza massiva quali da conservazione generalizzata; del resto, come già evidenziato dall'Avvocato Generale Campos-Sánchez Bordona nelle Conclusioni riferite alla causa *La Quadrature du Net*, la garanzia delle esigenze securitarie deve trovare un confine chiaro nelle necessità di «assoggettamento del potere e della forza ai limiti del diritto e, in particolare, a un

[55] R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit., 53.

[56] Come rilevato da gran parte della dottrina, tra cui si ricordano L. Lupária, *Data retention e processo penale*, cit.; L. Scaffardi, *La data retention va in ascensore*, cit.; R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit.

[57] Sotto questo profilo, interessanti sono le considerazioni di A. Malacarne, *commento a prima lettura del DL 132/21 in materia di tabulati telefonici*, in *Sistema Penale*, 8 ottobre 2021.

[58] Oltre ai moniti già richiamati, mossi dal Garante per la Protezione dei Dati Pasquale Stanzione nel documento *Segnalazione sulla disciplina della conservazione* (cit.), anche il già Garante, Antonello Soro, non aveva mancato di esprimere perplessità e preoccupazioni quanto alla disciplina italiana in materia di *data retention*, sin dalla discussa adozione della Legge Europea 2017 (sul punto si leggano le dichiarazioni di Soro durante il Convegno *Privacy digitale e protezione dei dati personali tra persona e mercato*, reperibili sul sito web del Garante, nonché il Parere 8005333/2018).

[59] Taluni studiosi definiscono infatti la disciplina italiana in materia di *data retention* come frutto di una «tormentata stratificazione» (E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, cit.).

ordinamento giuridico che trova nella difesa dei diritti fondamentali la ragione e il fine della sua esistenza»; se così non fosse «nulla potrebbe assicurare che, dotando il potere pubblico di strumenti esorbitanti per il perseguimento dei reati (..) la sua azione incontrollata e totalmente libera non si risolverebbe in definitiva in un pregiudizio alla libertà di tutti», § 135[60].

Venendo infine al secondo ambito di approfondimento, le Conclusioni e la prossima decisione della CGUE nel caso qui analizzato rappresentano una ulteriore importante tappa di quel viaggio che, nella dimensione sovranazionale e nazionale, continua ad essere costellato di mete intermedie ma che pare essere, ancora oggi, privo di un punto di arrivo chiaro e definitivo. Il rinvio del giudice italiano, infatti, si inserisce in un percorso ancora in evoluzione, rispetto al quale diversi protagonisti stanno ancora concorrendo a determinarne la direzione e – forse – il traguardo finale.

Innanzitutto, non si può che mettere in luce come, nell'attuale immobilismo del legislatore europeo e nella spesso diversa interpretazione e posizione assunta da governi e Parlamenti nazionali quanto alla disciplina della *data retention*, i giudici di Lussemburgo siano nel frattempo chiamati a pronunciarsi in un altro rilevante rinvio promosso questa volta dal Consiglio di Stato francese. Il caso *La Quadrature du Net et al. c. Premier Ministre, Ministère de la Culture*, C-470/12, recentemente riassegnato alla Grande Sezione, è infatti osservato con grande attenzione e le Conclusioni dell'Avvocato Generale Szpunar del 27 ottobre 2022 hanno già iniziato a far discutere. Tale rinvio ha ad oggetto, nel limitato e specifico ambito della lotta alle violazioni dei diritti di proprietà intellettuale commesse online, la disciplina della *data retention* e accesso agli indirizzi IP attribuiti all'origine di una connessione Internet. La questione, che qui si vuole solo brevemente richiamare, prende avvio dalla normativa francese – il Decreto del 5 marzo 2010 – che consente la conservazione generalizzata, l'acquisizione e il trattamento – da parte di una particolare autorità – dei dati di connessione a scopi di lotta ai reati lesivi del diritto d'autore; questa disposizione, tuttavia, non prevede il controllo preventivo di un giudice o di un'autorità indipendente.

Nelle sue Conclusioni, l'Avvocato Generale Szpunar pare proporre un ripensamento della giurisprudenza della CGUE relativamente all'interpretazione dell'art. 15 Direttiva *e-Privacy* e, per quanto qui ci interessa maggiormente, muove considerazioni di rilievo anche sulla nozione di "forma grave di criminalità": questa deve «essere interpretata autonomamente. Essa non può dipendere dalle concezioni di ciascuno Stato membro, salvo permettere un'elusione dei requisiti di cui all'art. 15, par. 1, della direttiva 2002/58/CE a seconda che gli Stati membri adottino una concezione estensiva o meno della lotta alle forme gravi di criminalità», § 74. Una lettura, questa, che trova evidenti profili di contrapposizione con le Conclusioni dell'Avvocato Generale Collins nel caso sin qui esaminato, che giungono, sul punto, a negare il carattere di nozione autonoma di diritto dell'UE al concetto di "reato grave".

L'Avvocato Generale Szpunar, poi, seppure a condizioni ben determinate e unicamente con riferimento ai dati relativi all'identità civile corrispondenti ad indirizzi IP, rilancia una lettura del diritto dell'UE volta a consentire una conservazione generalizzata e un accesso non vincolato al controllo preventivo di un giudice o di una entità amministrativa indipendente; ciò però solo qualora lo scopo perseguito sia quello di permettere l'intervento e l'indagine da parte dell'autorità amministrativa incaricata di proteggere i diritti d'autore su Internet e unicamente nel caso in cui tali dati rappresentino il solo strumento di indagine in grado di consentire l'identificazione della persona alla quale l'indirizzo era attribuito al momento della commissione del reato.

Rispetto alla lettura qui sinteticamente riportata delle Conclusioni nel caso C-470/12,

[60] Si fa riferimento alle Conclusioni dell'Avvocato Generale Campos-Sánchez Bordona nel caso *La Quadrature du Net*, § 135.

alcune critiche e perplessità sono già state sollevate[61], rilevando nelle posizioni espresse dall'Avvocato Generale Szpunar i segni di un preoccupante *revirement* rispetto alla previa giurisprudenza della CGUE e di una interpretazione del diritto dell'UE maggiormente pro-securitaria, col rischio di "annacquare" e via via restringere i requisiti e i principi indicati dalla *case law* eurounitaria. Le visioni discordanti e le critiche, in direzioni differenti, già emerse a seguito della apertura a forme di *bulk data retention* per scopi di garanzia della sicurezza nazionale, sembrano quindi destinate a riproporsi nel prossimo futuro.

Le decisioni dei giudici di Lussemburgo in quest'ultimo caso – senza dubbio molto particolare e circoscritto quanto alla natura dei dati e dei reati perseguiti – e in quello esaminato nel presente lavoro determineranno l'evoluzione del dibattito europeo in materia non solo di *data retention* ma anche, più ampiamente, di tutela dei diritti fondamentali dinnanzi all'emergere di sempre più sofisticate tecniche di sorveglianza massiva e raccolta di dati. Il vivace e mai sopito confronto – e scontro – tra torsioni regolatorie securitarie e approcci maggiormente garantisti di diritti e libertà trova infatti ormai sempre nuova concretizzazione: si pensi al ricorso a sistemi innovativi di c.d. *predictive policing*, fondati su decisioni automatizzate, o ancora a strumenti massivi di riconoscimento facciale[62], che già hanno iniziato a mettere alla prova legislatori e corti, anche nell'UE[63], testimoniando così come la nota e antica contrapposizione – o

[61] In questo senso si è espressa la ONG EDRi (*Advocate General recklessly calls for watering down privacy protections*, 16 novembre 2022). In particolare, gli attivisti criticano la posizione dell'Avvocato Generale che ritiene i dati relativi agli indirizzi IP come meno invasivi della sfera privata e non in grado di consentire una ricostruzione della vita e delle preferenze degli utenti: «*in doing so, the AG plays down the level of privacy intrusion that identifying the person who has viewed certain online files may entail. Files including photos, videos or text are susceptible to reveal the person's sexual orientation, political, religious or philosophical opinion. There is no need to reconstruct the entire clickstream of the user in order to deduce very intimate information on their life*».

[62] Entrambi i sistemi di *predictive policing* e di riconoscimento facciale sono basati sull'impiego di strumenti di Intelligenza artificiale e sono impiegati – anche ma non solo – da *law enforcement authorities* o agenzie di *intelligence* al fine di anticipare la soglia del pericolo e svolgere analisi predittive di dati o immagini. Su questi strumenti innovativi – peraltro oggetto di attenzione anche nel dibattito normativo sovranazionale con riferimento alla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale –, si legga, *ex multis*, B. Perego, *Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori*, in *BioLaw Journal*, 2, 2020, 447 ss.; G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in questa *Rivista*, 1, 2021, 204 ss.; E. Carpanelli, *Il ricorso all'Intelligenza artificiale nel contesto di attività di law enforcement e di operazioni militari: brevi riflessioni nella prospettiva del diritto internazionale*, in *DPCE Online*, 1, 2022, 383 ss.; M. Lo Monaco - J. Scipione, *Anatomia legale del riconoscimento facciale*, in *Fondazione Leonardo. Civiltà delle macchine*, 16 marzo 2022; S. Lonati, *Predictive policing: dal disincanto all'urgenza di un ripensamento*, in questa *Rivista*, 2, 2022, 302 ss.

[63] In materia di riconoscimento facciale, di grande rilievo è certamente la pronuncia dei giudici inglesi della Court of Appeal, Civil Division, 11 agosto 2020, *R(OTAO) Bridges v. The Chief Constable of South Wales Police and Others*, EWCA Civ 1058,; ma pensiamo anche al dibattito italiano, che ha visto l'intervento del Garante per la Protezione dei Dati con riferimento al sistema SariReal Time e Clearview AI e che ha conosciuto con d.l. 51/2023 l'approvazione di una proroga legislativa della moratoria sui sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico estesa sino al 31 dicembre 2025 (già determinata dall'art. 9, c. 9, del d.l. 139/2021, convertito dalla l. 205/2021). In tema di *predictive policing*, di particolare interesse è la recente sentenza del Tribunale costituzionale federale tedesco del 16 febbraio 2023 che ha dichiarato l'incostituzionalità delle normative adottate dai Land di Hesse e Hamburg riguardanti l'implementazione di "automated data analysis for the prevention of criminal acts" (si rinvia sul punto alla Press Release No. 18/2023 del *Bundesverfassunsgericht* tedesco); anche la CGUE è attualmente chiamata a pronunciarsi su sistemi di *automated decision-making* fondati su strumenti di Intelligenza artificiale, nel caso C-634/21 (su tale caso e sullo stato di avanzamento del processo: A. Hauselmann, *The ECJ's first landmark case on automated decision-making. A Report from the oral hearing before the First Chamber*, in *European Law Blog*, 20 febbraio 2023).

rapporto – tra sicurezza e diritti fondamentali sia continuamente rinnovata dinnanzi al progresso tecnologico[64].

Ebbene, in tale ottica generale, il futuro di sistemi di sorveglianza massiva, tra cui la *data retention*, nell'UE e, in particolar modo, in Italia risulta ancora difficile da stabilire, soprattutto con riferimento a specifici e diversi profili regolatori, quali il ruolo delle autorità giurisdizionali nel controllo preventivo o il diverso vaglio di proporzionalità da svolgere in considerazione di finalità e tipologia di dati conservati[65]. Come si è avuto modo di vedere dall'analisi del caso in esame, molti sono gli interrogativi interpretativi da risolvere, concernenti soprattutto un vaglio di proporzionalità[66] divenuto sempre più centrale ma altrettanto complesso da determinare dinnanzi a posizioni spesso divergenti[67].

Attraverso i prossimi interventi giurisprudenziali, a livello nazionale e sovranazionale, nonché mediante le scelte normative interne o europee, le corti e i legislatori dovranno assumere il difficile ma improrogabile compito di identificare la meta finale di un percorso ancora in divenire e a tratti incerto; con un monito che dovrebbe muovere le decisioni – anche legislative – in tale complessa materia e che aiuta a comprendere la grande delicatezza della posta in gioco: «*it is to be hoped that the Court [la CGUE in questo caso] will succeed in disregarding the polarisation trap and fostering the adoption and development of new technologies that are compliant with fundamental rights*»[68].

[64] Il progredire delle tecnologie e l'affermarsi della società algoritmica, infatti, risultano in grado sì di ampliare potenzialità di controllo e prevenzione in ambito securitario, ma anche di incrementare rischi e minacce alle libertà su cui le nostre società democratiche e lo Stato di diritto si fondano. Per riflessioni approfondite sul tema, si veda, tra i molti, G. De Minico - O. Pollicino (eds.), *Virtual freedoms, terrorism and the law*, Torino-Londra, 2020; H-W. Micklitz - O. Pollicino - A. Reichman - A. Simoncini (eds.), *Constitutional challenges in the algorithmic society*, Oxford, 2021; G. De Gregorio, *Digital constitutionalism in Europe. Reframing rights and powers in the algorithmic society*, Cambridge, 2022; M. Ienca - O. Pollicino - L. Liguori - E. Stefanini - R. Andorno (eds.), *The Cambridge handbook of information, technology, life sciences and human rights*, Cambridge, 2022; E. Celeste, *Digital constitutionalism. The role of Internet Bills of Rights*, Londra, 2022.

[65] Come affermato da Albers, del resto, «*Retention of data generated in telecommunications in order to enable security agencies at a later point in time to gain access to and make use of this data for security purposes is an illustrative example of how the Internet impacts the forms surveillance takes and creates new challenges for fundamental rights*», M. Albers, *Surveillance and Data Protection Rights: Data Retention and Access to Telecommunications Data*, in M. Albers - I.W. Sarlet (eds.), *Personality and data protection rights on the Internet*, Cham, 2022, 69.

[66] De Vergottini evidenzia la necessità di respingere l'idea di un bilanciamento tra sicurezza e diritti fondamentali «perché il bilanciamento presuppone equivalenza di posizioni di partenza. Piuttosto, tenendo ferma la precedenza per i diritti si ammette in casi particolarmente gravi e meritevoli di ottenere una limitazione dei diritti ma a condizione che l'intervento limitativo sia giustificato e soprattutto proporzionato al fine che si deve conseguire con la misura», G. de Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 4, 2019, 85.

[67] Ciò emerge con tutta chiarezza dal dibattito normativo in corso sulla proposta di regolamento *e-Privacy*, già richiamato.

[68] V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 36.