BlogDUE

Can data collected to combat serious crime be used in subsequent administrative investigations pursuant to the *e-privacy* Directive? Some thoughts on the *Lietuvos Respublikos generalinė prokuratūra* judgment

Federico Ferri (Senior Assistant Professor of EU Law, *Alma Mater Studiorum* – University of Bologna) – 13 November 2023

SUMMARY: 1. Legal background. – 2. Facts of the case and findings of the Court. – 3. Putting the Court's conclusions into context. – 4. Has the circle been squared?

1. On 7 September 2023, the Court of Justice of the European Union (CJEU) handed down its decision on the C-162/22 case *Lietuvos Respublikos generalinė prokuratūra*. This First Chamber's judgment fuels the Court's case law on data retention in the framework of the well-known "*e-privacy* Directive", namely Directive 2002/58/EC.

Predictably, the case revolved around Art. 15, para. 1, of the Directive which allows Member States to adopt legislative measures to derogate from core data protection rights safeguarded by EU secondary law. More precisely, Art. 15, para. 1, states that such measures may be adopted to retain data, even though some cumulative conditions must be respected. First, only temporary measures are admissible. Second, they must comply with "the general principles of Community law". Third, restrictions are lawful only as far as they are necessary, appropriate and proportionate "within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system (…)".

The point is that the judicial "data retention saga" keeps evolving within a complex legal scenario. The cornerstone of the legal framework on data retention at EU level should have been Directive 2006/24/EC, but the CJEU declared it invalid in the *Digital Rights Ireland* judgment (8 April 2014, Joined Cases C-293/12 and C-594/12) and the EU legislator failed to fill this gap over years. Furthermore, in terms of data protection, Directive 2002/58/EC contains various references to legal instruments that are no longer applicable; for example, Directive 95/46/EC represented a sort of benchmark for the criteria established by the abovementioned Art. 15, para. 1, and was repealed by the General Data Protection Regulation (Regulation (EU) 2016/679). Not to mention that data retention has long constituted a testing ground for the potential of some provisions of the EU Charter of Fundamental Rights: above

all, Arts. 7, 8, and – at times – 11, aimed at protecting, respectively, private and family life, personal data, and the freedom of expression and information (besides *Digital Rights Ireland*, some of the main reference judgments are: *Tele2 Sverige*, 21 December 2016, Joined Cases C-203/15 and C-698/15; *Ministerio Fiscal*, 2 October 2018, Case C-207/16; *Privacy International*, 6 October 2020, Case C-623/17; *La Quadrature du Net*, 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18; *HK v. Prokuratuur*, 2 March 2021, Case C-746/18; *Commissioner of An Garda Síochána*, 5 April 2022, Case C-140/20; *SpaceNet and Telekom Deutschland*, 20 September 2022, Joined Cases C-793/19 and C-794/19).

Against this background, the role played by the Court has often proved crucial. Accordingly, the *Lietuvos Respublikos generalinė prokuratūra* case may have had the potential to complicate matters further.

2. In the present case, a Lithuanian public prosecutor was dismissed from service by the Prosecutor General's Office. The main reason of the disciplinary penalty was the unlawful provision of relevant information to a suspect and his lawyer during a pre-trial investigation. Evidence of the misconduct in office was collected during an internal administrative investigation. To this end, also traffic and location data about the communications between all three subjects were used. Nevertheless, those relevant data had been obtained during previous intelligence operations, as they had been collected and retained through providers of electronic communications services and for the purpose of combating serious crimes.

The public prosecutor initiated an administrative trial to challenge the dismissal decision; after the issuance of the first instance decision, the Supreme Administrative Court of Lithuania was ultimately seized. The main argument of the applicant was that access by the intelligence bodies, in connection with a criminal intelligence operation, to traffic data and the actual content of electronic communications constituted a serious interference with his rights, having regard to Directive 2002/58/EC and the Charter. The central issue was represented by the possibility that such data may be lawfully and subsequently used to investigate not only serious criminal offences, but also administrative misconduct related to acts of corruption. Indeed, this option was permitted by the Lithuanian Law on criminal intelligence that had been adopted to implement Art. 15, para. 1, of the *e-privacy* Directive.

The Supreme Administrative Court of Lithuania decided to stay the proceedings and activate a preliminary ruling. The CJEU was then asked whether Art. 15, para. 1, of Directive 2002/58/EC, read in the light of Articles 7, 8, 11 and 52, para. 1, of the Charter, must be interpreted as precluding such a form of use of the data already collected in the context of criminal intelligence operations.

Drawing at least in part from the opinion of Advocate General Campos Sánchez Bordona and its latest case law, the CJEU confirms the doubts of the referring Court and answers the preliminary question in the affirmative.

The CJEU first explains that the access and retention of traffic and location data must respect the requirements indicated in Art. 15, para. 1, of Directive 2002/58/EC. This provision sets forth an exception to the obligation of principle to ensure the confidentiality of electronic communications and data and, in particular, to the prohibition on storage data. The Luxembourg Judges (re)affirm that the provision at stake does not preclude legislative measures that, for the purposes of combating serous crime and preventing serious threats to public security, provide for the following situations: "the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended; the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary; the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers".

Then, the CJEU stipulates that the list of objectives contained in Art. 15, para. 1, of the Directive can be relied on to justify derogatory measures, but it is exhaustive; what is more, that there is a hierarchy amongst these objectives. The most important is safeguarding national security; it means that only this objective is capable, at least theoretically, to ensure the legitimacy of measures entailing more serious interferences with fundamental rights. The fight against serious crime and the prevention of serious threats to public security are, instead, of lesser importance, even though in certain cases also these grounds can be invoked to bring about serious interferences to fundamental rights. On the contrary, this is not possible if the objectives are fighting crime generally and preventing non-serious threats to public security. Based on the Court's reasoning, traffic and location data retained by providers may, in principle, be validly accessed only to pursue the public interest objective invoked to impose the (first) retention. That (second) access may be eventually justified by other objectives only if they are of greater importance, keeping in mind the hierarchy mentioned above.

Finally, the Court declares that these considerations on Art. 15, para. 1, of the *e-privacy* Directive apply *mutatis mutandis* to the subsequent use of traffic and location data retained by providers for the purpose of combating serious crime. As regards the main proceedings, internal investigations into disciplinary misconduct or misconduct in office related to acts of corruption are not meant to refer, genuinely and strictly, to the objectives indicated in Art. 15, para. 1, of the *e-privacy* Directive, including the prosecution and punishment of criminal offences.

3. The main findings of the *Lietuvos Respublikos generalinė prokuratūra* judgement do not appear surprising if considered in light of the pre-existing case-law of the Court. This is true precisely because – paradoxically – the reasoning of the CJEU deviates from the textual interpretation of Art. 15, para. 1, of Directive 2002/58/EC. In fact, when interpreting this provision, the Court has almost always broken off the potential constraints resulting from the meaning of the terms to examine. This is the outcome of a virtuous approach aimed at safeguarding the bulk of the fundamental rights connected with digital privacy individual prerogatives. Also for this reason, some scholars referred to the EU as a "fortress of digital privacy" (for instance, L. P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems*, in L. VIOLINI, A. BARAGGIA (eds.), *The Fragmented Landscape of Fundamental Rights Protection in Europe*, Cheltenham-Northampton, 2018, p. 134; O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Oxford, 2021, p. 137 et seq.). Some examples may help to better understand this point.

In the first place, in previous judgments (starting with *Tele2 Sverige AB*, point 102) the Court narrowed the scope of Art. 15, para. 1, of the *e-privacy* Directive. Basically, even if one of the potentially derogatory grounds is the prevention, investigation, detection and prosecution of criminal offences, the Court held that only "serious" criminal offences may be relevant to validly invoke – at least in principle – exceptions to the rule (see also L. WOODS, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*, in *EU Law Analysis*, 21 December 2016).

Moreover, the fact that all the objectives indicated in Art. 15, para. 1, are equal – but some are more, was confirmed in *La Quadrature du Net* (and reiterated in *Commissioner of An Garda Síochána* and in *SpaceNet and Telekom Deutschland*), where the Court clarified that the goal of protecting national security is to be prioritized due to Art. 4, para. 2, TEU, according to which this sector remains the sole responsibility of each Member State. The Court explained that such responsibility "corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities" (*La Quadrature du Net*, point 135). Threats to national security are thus different and, in any event, more serious than general risks of tensions or disturbances affecting public security. In other words, the need to safeguard national security is apt, compared with other Art. 15, para. 1, grounds and in light to Art. 52, para. 1, of the Charter, to justify measures entailing more serious interferences with fundamental rights. This, however, does not leave the Member States free to refrain from respecting the law of the EU when taking measures for the purpose of protecting national security (e.g. *La*

Quadrature du Net, point 99; see also F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited*, in *European Foreign Affairs Review*, No. 4, 2023, p. 323 et seq.).

This jurisprudence was particularly important also for the clarification of the measures that can be considered legitimate under Art. 15, para. 1, of Directive 2002/58/EC to – *inter alia* – combat serious crime. Again, reference has to be made to *La Quadrature du Net* (in particular, point 168), which can be seen as a pioneer judgment in this respect. Among other things, in *La Quadrature du Net* the Court triggered a more nuanced approach to surveillance, thereby opening the door for even bulk data retention measures in certain cases (the judgment was criticized by some scholars: e.g. M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze* Privacy International *e* La Quadrature du Net *della Corte di giustizia UE*, in *Il diritto dell'Unione europea*, No. 1, 2021, p. 93 et seq.; M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?*, in *European Public Law*, No. 1, 2022, p. 123 et seq.). Such approach has some similarities with recent judgments of the European Court of Human Rights Grand Chamber about data retention in the framework of Arts. 8 and 10 of the European Convention of Human Rights (in particular: *Big Brother Watch and Others v. the UK*, 25 May 2021, Applications Nos. 58170/13, 62322/14 and 24960/15; *Centrum för rättvisa v. Sweden*, 25 May 2021, Application No. 35252/08. See also M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa*, in *EJIL: Talk!*, 26 May 2021; B. VAN DER SLOOT, *Big Brother Watch and others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?*, in *European Data Protection Law Review*, No. 2, 2021, p. 319 et seq.).

Put it briefly, with the *Lietuvos Respublikos generalinė prokuratūra* decision the CJEU basically stays the course indicated by *La Quadrature du Net*. The added value of *Lietuvos Respublikos generalinė prokuratūra* is to extend beyond retention activities the safeguards previously introduced by the Court itself. In other words, it seems that the CJEU has completed the reasoning developed in *La Quadrature du Net* (especially point 165) and *Commissioner of An Garda Síochána* (point 98), where it ruled that access to traffic and location data retained by providers pursuant to a measure taken under Article 15, para. 1, of Directive 2002/58/EC may, in principle, be justified only by the same public interest objective for which retention was ordered to those providers; at most, the new access can be based on a new ground if its importance is greater than that of the objective which justified retention.

The judgment at hand suggests that Art. 15, para. 1, of Directive 2002/58/EC, alongside Arts. 7, 8, 11 and 52, para. 1, of the Charter, cover a long legality chain of activities that does not end with – although is centred on – retention (see also L. DRECHSLER, *Re-using retained personal data under*

the ePrivacy Directive: Court of Justice clarifies limits in Case C-162/22 A.G. v Lietuvos Respublikos generalinė prokuratūra, in *EU Law Live*, 27 September 2023). No matter if Art. 15, para. 1, of the *e-privacy* Directive fails to consider subsequent use of data, this is for sure a necessary corollary of the hierarchy test established and repeated by the Court to foster the protection of the fundamental rights concerned. To conclude otherwise would undermine the effectiveness of these rights, in light of the legal contours gradually designed by the CJEU.

4. Bearing in mind the above, has the CJEU squared the circle of data retention with its case law, from *Digital Rights Ireland* to *Lietuvos Respublikos generalinė prokuratūra* (and through *La Quadrature du Net* and *Commissioner of An Garda Síochána*)? Maybe it is too soon to take this stand, at least for two reasons.

On the one hand, it should not be forgotten that the Member States keep enjoying a certain leeway when it comes to the interpretation (and the implementation) of the key concepts at the heart of Art. 15, para. 1, of Directive 2002/58/EC, including the notion of "serious crime". Suffice here to recall that the CJEU had a chance to clarify this concept, but refrained from doing it; that happened especially in the *Ministerio Fiscal* judgement, where the preliminary question was slightly reshaped so to shift the focus from the seriousness of the crime to the seriousness of the impact on the fundamental rights to be protected.

On the other hand, Directive 2002/58/EC is expected to be repealed soon by the forthcoming *e-privacy* Regulation, whose proposal was tabled almost seven years ago. Since the beginning, it was clear that the Commission's proposal was not seeking to harmonize national laws on data retention and access criteria to data related to electronic communications by public authorities, with the result that the legal landscape was likely to remain fragmented at the national level (G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal, in *Associazione italiana dei costituzionalisti – Osservatorio costituzionale*, n. 3, 2018, p. 474). The main reference text so far is the Council's mandate of 10 February 2021. Among its most controversial provisions is Art. 7, para. 4, which runs as follows: "Union or Member state law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as the safeguarding against and the prevention of threats to public security, for a limited period (…)". Now, as noted by the European Data Protection Board, this provision appears to derogate the core of the *La Quadrature du Net* judgment (European Data Protection Board, *Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021*). If this specific regime is confirmed, that would result both in different national

criteria and standards flourishing across the EU, as well as in Arts. 7, 8, 11, and 52, para. 1, of the Charter being jeopardized. Therefore, as already pointed out, this issue shall be addressed and solved, "so that the pronouncements of the CJEU do not become dead letter in lieu of retaining national mass surveillance regimes" (V. MITSILEGAS, E. GUILD, E. KUSKONMAZ, N. VAVOULA, *Data retention and the future of large-scalesurveillance: The evolution and contestation ofjudicial benchmarks*, in *European Law Journal*, 12 May 2022, p. 27).