insights

Volume: 24 Issue: 28

By: **Monika Zalnieriute**

November 5, 2020

The Future of Data Retention Regimes and National Security in the EU after the *Quadrature Du Net* and *Privacy International* Judgments

Introduction

On October 6, 2020, the Grand Chamber of the Court of Justice (CJEU) delivered two long-awaited judgments on data retention, national security and fundamental rights: Joined Cases C-511/18 *La Quadrature Du Net and Others*, C-512/18 *French Data Network and Others,* and C-520/18 *Ordre des Barreaux Francophones et Germanophone and Others* (hereinafter *Quadrature Du Net*)[1] and Case C-623/17 *Privacy International (Privacy International)*.[2] In both judgments, the Court ruled that the EU Privacy and Electronic Communications Directive (2002/58) (e-Privacy Directive)[3] and the EU Charter of Fundamental Rights[4] generally prevent national law from enabling bulk data retention of traffic and location data. However, EU law does not preclude indiscriminate data retention measures if member states can demonstrate the existence of legitimate and serious threats to national security. In such cases, bulk data can only be retained during a strictly necessary period, and the decision must be subject to review by a court or independent administrative body.

National Security, Data Retention, and the Division of Competence in the EU

Quadrature Du Net and *Privacy International* involved proceedings brought before the Investigatory Powers Tribunal in the United Kingdom (UK) and the Conseil d'État in France and the Constitutional Court in Belgium, concerning the lawfulness of national legislation requiring communications service providers to forward users' traffic data and

location data to a public authority or to retain such data in a general or indiscriminate way. The national courts referred the cases to the CJEU to clarify whether: (1) the activities of national security agencies—as opposed to general law enforcement agencies—fall within the scope of EU law, and (2) whether indiscriminate data retention for national security purposes is compatible with EU law.

The positive answer to the first question in all four cases shows that the CJEU has become an important actor in regulating national security and intelligence activities in EU member states. The emergence of an EU actor capable of seriously influencing national powers of surveillance is relatively new. Only with the end of the Cold War have the activities of intelligence agencies become gradually regulated by statutory laws, rather than being shielded behind secretive executive decrees.

This relative novelty is reflected in the EU legal framework, where national security, despite European integration, has explicitly remained the responsibility of member states. Under the Treaty of the European Union (TEU), the EU only exercises competences that have been expressly or impliedly delegated to the EU by the member states.[5] The TEU also provides that "the Union shall respect the . . . Member States' essential State functions, including safeguarding national security . . . national security remains the sole responsibility of each Member State."[6]

However, national security intersects and overlaps with internal EU security, where the EU does have shared competence to adopt legislative measures under Title V of Treaty on the Functioning of the European Union (TFEU),[7] which establishes an area of Freedom, Security, and Justice. It provides for EU competence to adopt legislation on police cooperation[8] and fighting organized crime and terrorism[9]—matters closely related to national security. The TFEU further stipulates that the EU's competence in justice and security "shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."[10] Shared competence means that the EU member states can also act in this area, but they have to comply with the EU legal framework.

The Origins and Controversy of Data Retention Regimes

Contemporary data retention regimes date back to the post-9/11 era, when many governments adopted new legislative measures granting wide-ranging powers to law enforcement agencies in the fight against the "war on terror." The EU entered into numerous international agreements on data retention and sharing. In 2006, the EU adopted a Data Retention Directive which required communications service providers to

store traffic and location data for a period between six months and two years, and maintain a surveillance database for law enforcement purposes.[11] Between 2009 and 2012, the Czech and Romanian Constitutional Courts and German Federal Constitutional Court opined that national laws implementing the Data Retention Directive encroached on fundamental rights and were incompatible with the national constitutional laws in those member states.[12]

Following the Snowden revelations in 2013, the CJEU has been very vocal on the constitutional significance of data protection in the EU legal framework, and that has often intersected with national security concerns. First, in the ground-breaking decision in *Digital Rights Ireland*, the CJEU invalidated the Data Retention Directive because it represented a disproportionate and unjustified interference with the European Charter of Fundamental Rights provisions guaranteeing the rights to private life and data protection. [13] Soon after, in the *Schrems I* case, the CJEU invalidated the EU Commission's decision on adequacy of data protection provided by the Safe Harbour agreement, which had facilitated EU-US data-sharing between 2000 and 2015.[14] In the subsequent *Tele2 Sverige*,[15] the CJEU confirmed that indiscriminate data retention for the purposes of combatting crime interfered seriously with the right to a private life, and extended the *Digital Rights Ireland* ruling to national data retention regimes in member states. *Tele 2 Sverige* has caused unease among member states, which felt that the CJEU has deprived them of a tool of indiscriminate data retention which they see as crucial in safeguarding national security and combatting crime.

Legitimizing Bulk Data Retention for National Security

The CJEU's decisions in *Quadrature Du Net* and *Privacy International*, legitimizing indiscriminate data retention for national security, are not surprising even though they contrast sharply with the Court's post-Snowden approach, which the CJEU has cemented in its most recent ruling in *Schrems II* case, delivered just two months earlier, on July 16, 2020.[16] In that case, the CJEU invalidated the EU-US Privacy Shield agreement for lack of safeguards in the national surveillance system of the US. Yet, the CJEU was under a lot of pressure to soften its wide-ranging stance developed after the Snowden revelations. Praised by the NGOs, the Court's progressive post-Snowden approach, has been criticised as "hyper-constitutionalization," and even as a "largely self-congratulatory exercise . . . that uses a strategy of 'othering' in order to build a specific European identity upon the very idea of privacy."[17]

In *Quadrature du Net* and *Privacy International* the Court demanded procedural safeguards, yet this approach is very different from that in *Tele 2 Sverige* where the CJEU

had insisted that to be proportionate, data retention had to be targeted. In their restraint, the *Quadrature du Net* and *Privacy International* pronouncements are similar to the modest approach of the European Court of Human Rights, which oversees the interpretation of the European Convention on Human Rights (ECHR). The Convention covers surveillance activities for national security purposes, and which is part of the national law of all EU member states, and part of EU law. The EU Charter of Fundamental Rights explicitly recognizes that some rights protected therein and by the ECHR overlap, and therefore, "the meaning and scope of those rights shall be the same as those laid down by the ECHR."[18]

In the recent cases of *Centrum för Rättvisa v. Sweden,* and *Big Brother Watch v. UK,* the European Court of Human Rights accepted that the bulk collection of communications data is a matter within each states' margin of appreciation.[19] Both of these judgments focused on the safeguards applying to these two states' systems of signals intelligence, yet both of them were appealed to the Grand Chamber of the European Court of Human Rights, with final judgments expected in 2021. While in the post-Snowden era, the CJEU regarded the European Court of Human Rights' jurisprudence as a minimum standard from which it can diverge by imposing stricter data protection standards, *Privacy International* and *Quadrature Du Net* suggest that the approaches of these two courts are converging. This convergence points towards the EU where indiscriminate data retention is, just like in pre-Snowden era, acceptable, provided certain safeguards are in place.

The Future of Data Retention in the EU

Overall, the EU Commission, EU Parliament, and CJEU are institutionally inclined to define 'national security' narrowly, to increase their own role in the area. The member states, on the other hand, have an institutional interest in keeping the EU institutions out of national security. At the same time, the member states cannot avoid the growing European interdependence in security matters. This struggle of competence is particularly visible in the data retention policy, considered in *Quadrature Du Net* and *Privacy International* cases.

The decisions come at a time when data retention regimes are back on the agendas of the member states and EU institutions. In May 2019, the Council of the EU concluded the data retention reflection process, and called on the EU Commission to consider a future EU regime on data retention, emphasizing that the fragmentation of national data retention practices can hinder law enforcement efforts, particularly in cross-border cases.[20] The EU Commission is also preparing an e-Privacy Regulation,[21] set to repeal the e-Privacy Directive and complete the EU's data protection framework alongside the

General Data Protection Regulation[22] and Law Enforcement Directive.[23] The Council's reflection process revealed that member states prefer to establish a more favorable environment for data retention, foreshadowing the potential of introducing a data retention obligation through the back door.

About the Author: Monika Zalnieriute is Senior Lecturer at Macquarie Law School, Macquarie University, Sydney, Australia (monika.zalnieriute@mq.edu.au) and a Visiting Fellow, UNSW Law Sydney.

---

[1] ECLI:EU:C:2020:791, http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6166350.

[2] ECLI:EU:C:2020:790, http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6063852.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002 O.J. (L 201) 37.

[4] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 2.

[5] Treaty on European Union, 2012 O.J. (C 326) 15, art. 5 [hereinafter TEU].

[6] *Id*. art. 4.

[7] Treaty on the Functioning of the European Union, 2012, O.J. (C 3262) 47–390 [hereinafter TFEU].

[8] *Id*. art.

[9] TFEU art. 88.

[10] *Id.* art. 72.

[11] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 O.J. (L 105) 54.

[12] *See* the Czech Republic Constitutional Court judgment of 2011/03/22, Pl. ÚS 24/10 94/2011; Romanian Constitutional Court 08/10/2009 Decision No 1258, and German decision in 1 Bvr 256/08 Vom 02/03/2010.

[13] Joined Cases C-293/12 and C-594/12, Digital Rts Ireland Ltd. V. Minister Commc'ns, Marine & Natural Resources, Minister Just., Equality & L. Reform, Comm'er of the Garda Síochána, Ireland, The Attorney General, 2014 E.C.R. 238.

[14] C-311/18 Data Protection Comm'er v. Facebook Ireland Ltd. & Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020).

[15] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post -och telestyrelsen; Sec'y State Home Dept. v. Tom Watson, Peter Brice, Geoffrey Lewis, ECLI:EU:C:2016:970 (Dec. 21, 2016).

[16] Schrems I, *supra* note 14.

[17] Thomas Wischmeyer, *"Faraway, So Close!" – A Constitutional Perspective on Transatlantic Data Flow Regulation*, *in* OBAMA'S COURT: RECENT CHANGES IN U.S. CONSTITUTIONAL LAW IN TRANSATLANTIC PERSPECTIVE, 8–10 (Anna-Bettina Kaiser, Niels Petersen, & Johannes Saurer eds., 2018), at 15.

[18] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 2, art. 52.

[19] *Centrum För Rättvisa v. Sweden,* App. No. 35252/08, 112 (2018), http://hudoc.echr.coe.int/fre?i=001-183863;

Big Brother Watch and Others v. The United Kingdom, App. Nos. 58170/13, 62322/14 and 24960/15, 314 (2018), http://hudoc.echr.coe.int/fre?i=001-186048.

[20] Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime, 1–7 5, 9 (2019), https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf.

[21] *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)* COM (2017) 10 final (Jan. 10, 2017).

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[23] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89.