Case C-817/19, Ligue des Droits Humains v. Council of Ministers (C.J.E.U.)

C-817/19, *Ligue des Droits Humains* v. *Council of Ministers*

Introduction

On 21 June 2022, the Court of Justice of the European Union (CJEU) sitting as a Grand Chamber rendered its decision in the preliminary ruling procedure C-817/19, *Ligue des Droits Humains* v. *Council of Ministers*.[i] In its ruling, the CJEU held that the surveillance regime established by the Passenger Name Record Directive 2016/681[ii] (PNR Directive) was compatible with the Charter of Fundamental Rights of the European Union (CFREU/EU Charter).[iii] Nevertheless, the CJEU strictly circumscribed the Directive's transposition within EU Member States' domestic laws. While restricting permissible interpretations of the PNR Directive's provisions and imposing strict limitations on its scope to ensure its conformity with the EU Charter, the Court upheld for the first time an instrument of indiscriminate surveillance as compatible with EU primary law. This represents a significant development in the CJEU's case-law on privacy rights, which is likely to affect the negotiation and development of future PNR agreements with third countries, as well as the development of the ePrivacy Regulation, discussions surrounding the regulation of AI, and negotiations for international instruments aiming to address serious crimes. Further, the ruling confirms the CJEU's increasing convergence with the European Court of Human Rights' (ECtHR) case-law on the matter, thus inscribing national security as a legitimate exception to the general prohibition of indiscriminate bulk data collection and retention in Europe.

Background

Since its original 2014 pronouncement in *Digital Rights Ireland,*[iv] the CJEU has grappled with a number of instruments and domestic laws concerning indiscriminate data collection and retention. Originally extremely protective of privacy rights, the Court has slowly evolved towards a stance more deferential to states' national security concerns.

In *Digital Rights Ireland*, the CJEU rejected a model of mass surveillance based on the general and indiscriminate retention of communication metadata as incompatible with the EU Charter. As a result, it annulled the Data Retention Directive.[v] In this landmark judgment, the CJEU thus rejected the possibility that indiscriminate data retention could constitute a proportionate interference with the right to respect for private and family life (Article 7 CFREU) and to the protection of personal data (Article 8 CFREU). The Court's principled opposition to mass surveillance was reaffirmed in further cases concerning EU Member States' data retention regimes;[vi] international data sharing;[vii] and the transfer of Passenger Name Record data.[viii]

This principled position was, however, undermined in October 2020. In *La Quadrature du Net and Others*,[ix] concerning the compatibility with EU law of French and Belgian laws on data processing, the Court held for the first time that bulk retention of communications data could be justified on national security grounds. The Court was careful to mandate strong procedural safeguards. Nevertheless, *La Quadrature du Net* resulted in the principled acceptance of bulk data retention (and thus bulk data collection as a necessary prior step) as a proportionate interference with fundamental rights when the objective of general interest pursued is the protection of national security. The national security exception was reaffirmed in a later decision, a preliminary ruling concerning Germany's telecommunications data retention law (*SpaceNet AG* and *Telekom Deutschland*).[x]

Unlike *La Quadrature du Net* and *SpaceNet AG* and *Telekom Deutschland*, the Belgian court's referral for a preliminary ruling in *Ligue des Droits Humains* pertained not only to the conformity of national legislation with EU law but also to the validity of an EU instrument, namely the PNR Directive. The PNR Directive requires the systematic processing of PNR data relating to air passengers on extra-EU flights entering and leaving the EU for the purposes of combating terrorist offenses and serious crime, and authorizes similar measures for intra-EU

flights. The CJEU therefore had to pronounce itself on the validity of the PNR Directive with regard to EU primary law, in this case the EU Charter.

Ruling

In its ruling, the CJEU found the PNR Directive to be compatible with the EU Charter. While noting the seriousness of the Directive's interferences with the rights to privacy and to the protection of personal data,[xi] the Court provided a detailed analysis of the justification for these interferences.[xii] In particular, the CJEU found that the interferences are necessary and proportionate to the objective of legitimate interest that the Directive seeks to achieve, namely "to ensure the internal security of the European Union and thus protect the life and safety of persons".[xiii] Hence, despite the Directive seeking to introduce "a surveillance regime that is continuous, untargeted and systematic, including the automatic assessment of the personal data of everyone using air transport services",[xiv] the CJEU ultimately concluded that the Directive is consistent with the Charter.

Nevertheless, in doing so, the Court strictly circumscribed the transposition of the PNR Directive by Member States. The CJEU thus imposed numerous limitations and restrictive interpretations, many of which derived from Opinion 1/15 in which it had invalidated the proposed PNR agreement between the EU and Canada.[xv] First, as regards the material scope of the PNR regime, the CJEU limited the information that can be collected to the data listed in Directive's Annex I.[xvi] It also specified that this regime can only be applied for the purpose of combating serious crime and should not be extended to ordinary crime.[xvii] Further, despite Article 2 of the Directive unreservedly allowing Member States to apply the PNR regime to intra-EU flights, the Court held that this regime may only apply to intra-EU flights and/or other means of transport in the presence of "a genuine and present or foreseeable threat".[xviii]

Then, with regard to the processing of PNR data, the CJEU held that Member States may not add processing purposes other than those exhaustively listed in Article 1(2) of the Directive.[xix]

Nor can they empower their Passenger Information Units (PIUs) to authorize the disclosure of PNR data after the 6-month period provided for in the Directive.[xx] Then, in direct contradiction with the text of Article 12(1) of the Directive mandating a five-year retention period for all PNR data, the Court held that Member States may not set a general retention period for data for all air passengers regardless of whether they pose a terrorist risk or present no risk at all.[xxi]

The Court also specified limitations concerning the means and methods used to process PNR data. It thus stated that, to compare PNR data with existing databases, PIUs may only use databases "on persons or objects sought or under alert".[xxii] Furthermore, the Court excluded the possibility to use self-learning AI technologies to process PNR data if these technologies can modify their processing methods without human intervention or control.[xxiii] In addition, the results of any automated processing of PNR data must be thoroughly and effectively reviewed by a PIU official.[xxiv] Hence, while AI processing is authorized, human oversight remains mandatory.

Conclusion

The CJEU's ruling in *Ligue des Droits Humains* is part of a broader judicial movement legitimating bulk data collection and retention for national security purposes in Europe. Aligning itself with ECtHR's case-law on mass surveillance regimes,[xxv] the CJEU confirms that the protection of national security constitutes an objective capable of rendering bulk data collection and retention necessary and proportionate under the EU Charter. Nevertheless, the ruling presents itself as a complex balancing exercise. On the one hand, the Court finds the PNR Directive compatible with the EU Charter. On the other hand, and through the same reasoning, the Court imposes extremely restrictive interpretations of the Directive's provisions to EU Member States to ensure such compatibility. By so doing, the Court adopts a rule-creating role. Indeed, these restrictive interpretations are sometimes in direct contradiction with the text of the Directive (for instance concerning the retention period for PNR data or the limitations on

EU Member States' competence to apply the PNR regime to intra-EU flights). Since Member States' transposition laws will need to reflect these interpretations, their lack of textual basis is likely to trigger further litigation.

The development and confirmation of a national security exception to the general prohibition of indiscriminate bulk data collection and retention by the CJEU is its recent case-law also has the potential to influence law-making efforts at both EU and international levels. In the EU, future agreements, directives, and regulations will necessarily take into account the CJEU's latest case-law to ensure conformity with the EU Charter. Discussions on AI and PNR agreements with third countries will be directly affected by the ruling. *Ligue des Droits Humains* could also affect the new ePrivacy Regulation,[xxvi] currently being developed to replace the ePrivacy Directive[xxvii] and with regard to which the Council of the European Union had already proposed to exclude national security activities from its scope.[xxviii] Beyond Europe, the ruling might have consequences in multilateral negotiation fora, for instance in the UN Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes.[xxix] Indeed, European courts' principled acceptance of indiscriminate data collection and retention as compatible with fundamental rights when national security is at stake could further hinder civil society's efforts to bring privacy rights to the forefront of discussions.

---

[i] Case C-817/19, Ligue des Droits Humains v. Council of Ministers, ECLI:EU:C:2022:491.
[ii] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
[iii] Charter of Fundamental Rights of the European Union (2007/C 303/01).
[iv] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others (C-293/12) and Kärntner Landesregierung and Others (C-594/12) [2014] ECLI:EU:C:2014:238.
[v] 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 of public communications networks and amending Directive 2002/58/EC,OJ L105/54, 13.4.2006 (Data Retention Directive).
[vi] Joined Cases C-203/15 and C-689/15, Tele2 Sverige AB v. Postoch telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Tom Watson and Others (C-689/15) [2016] ECLI:EU:C:2016:970.

[vii] C-362/14 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650 and C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559.
[viii] Case Opinion 1/15, ECLI:EU:C:2016:656.
[ix] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier Ministre and Others, ECLI:EU:C:2020:791.
[x] Joined Cases C-793/19 (SpaceNet AG) and C-794/19 (Telekom Deutschland), ECLI:EU:C:2022:702.
[xi] Para 111.
[xii] Paras 112-128.
[xiii] Para 121.
[xiv] Para 111.
[xv] Case Opinion 1/15, ECLI:EU:C:2016:656.
[xvi] Paras 131-139.
[xvii] Para 152.
[xviii] Paras 173-174.
[xix] Paras 236-237.
[xx] Para 247.
[xxi] Para 262.
[xxii] Paras 187-188.
[xxiii] Paras 193-201.
[xxiv] Paras 202-213.
[xxv] See, in particular, *Big Brother Watch and Others* v. *The United Kingdom* [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021; *Centrum för Rättvisa* v. *Sweden* [GC], Application No 35252/08, 25 May 2021.
[xxvi] *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/2017/010 final - 2017/03 (COD).
[xxvii] 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 (Directive on privacy and electronic communications).
[xxviii] *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)—Mandate for negotiations with the European Parliament*, ST 6087 2021 INIT (10 February 2021).
[xxix] See: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.