20 Years Anniversary of the Tampere Programme

Europeanisation Dynamics of the EU Area of Freedom, Security and Justice

Sergio Carrera, Deirdre Curtin and Andrew Geddes

European University Institute
Robert Schuman Centre for Advanced Studies
Department of Law
Migration Policy Centre
EU2019.FI
CEPS

Published by

European University Institute (EUI)

Via dei Roccettini 9, I-50014

San Domenico di Fiesole (FI)

Italy

ISBN:978-92-9084-882-0

doi:10.2870/66646

QM-04-20-173-EN-N

With the support of the Erasmus+ Programme of the European Union

20 YEAR ANNIVERSARY OF THE TAMPERE PROGRAMME

Europeanisation Dynamics of the EU Area of Freedom, Security and Justice

EDITED BY

Sergio Carrera

Deirdre Curtin

Andrew Geddes

European University Institute, Florence, Italy

European University Institute
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES
DEPARTMENT OF LAW
MIGRATION POLICY CENTRE
EU2019.FI Finland's Presidency of the Council of the European Union
CEPS

Table of Contents

22. TARGETED SURVEILLANCE: CAN PRIVACY AND SURVEILLANCE BE RECONCILED?

Edoardo Celeste & Federico Fabbrini

1. Introduction

Striking the balance between the protection of fundamental rights and the need to protect national security has been a challenge for all liberal democracies in times of emergency. The same is true also for the European Union (EU). In fact, since the launch 20 years ago of the 1999 Tampere programme, implementing the 1997 Treaty of Amsterdam, the EU has developed a common policy in the area of Freedom, Security and Justice (AFSJ), which led to the adoption of important pieces of legislation also concerning the fight against crime and international terrorism. At the same time, however, since 2000, the EU has been endowed with an advanced and comprehensive Charter of Fundamental Rights, which was given full primary law status by the 2009 Treaty of Lisbon.

As a result, in the last decade, the European Court of Justice has been faced repeatedly with the question of how to reconcile security and justice, contributing to the constitutionalisation of

the AFSJ.[1] This is particularly true in the field of privacy and data protection, where the ECJ has taken a leading role in reviewing EU and national legislation empowering law enforcement agencies to undertake surveillance. In fact, in comparative perspective, the ECJ has become the most important jurisdiction world-wide in limiting security overreach in the field of mass surveillance to adequately protect human rights. Hence, it is not an overstatement to claim that in this field the ECJ has progressively become a "human rights court."[2]

This Chapter summarizes the ECJ case law prohibiting mass data collection and retention and discusses its legacy for the future. The contribution is structured as follows. Section 2 contextualises the emergence of mass surveillance in Europe in the early 2000s and maps the relevant legislation adopted by the EU. Section 3 examines the ECJ's decisions in *Digital Rights Ireland* and *Schrems*, explaining why the ECJ deemed EU surveillance measures to be incompatible with EU fundamental rights. Section 4 examines instead the ECJ's decision in *Tele2 Sverige & Watson*, and explains how the case law of the ECJ reverberated on surveillance measures adopted at the national level. Finally, section 5 concludes by reflecting on the potential consequences of the ECJ jurisprudence on future cases.

2. The Emergence of Mass Surveillance in Europe

The first years of the twenty-first century were characterised by a radical revolution in terms of intelligence and law enforcement authorities' practices. In the aftermath of the 9/11 terrorist attacks, the urgent need to contrast international terrorism led to a transition to a system of pre-emptive security and mass surveillance.[3]

1 See K. Lenaerts (2010), 'The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice' 59 International and Comparative Law Quarterly 255.

2 F. Fabbrini (2015), 'The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court' in S. de Vries, U. Bernitz and S. Weatherill (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument* (Hart).

3 See V. Mitsilegas (2014), 'Transatlantic Counterterrorism Cooperation and European

Significant advancements in the technological sector offered for the first time the possibility to collect and process huge amount of data for speculative purposes.[4]

In Europe, several member states enacted legislation requiring internet and telephone service providers to retain and further make accessible to national law enforcement authorities electronic communications' meta-data, i.e. information about the time, location, source and addressees of phone calls, texts or emails.[5] These statutes were adopted as derogations to EU data protection law, which allowed member states to introduce exceptions to data protection rules in, *inter alia*, the domains of public security, defence and criminal investigations.[6]

In 2006, however, after the terrorist attacks in Madrid and London, the EU institutions saw a window of opportunity to advance legislation to harmonize member states' action in the field. As a result, the Data Retention Directive, Directive 2006/24/EC, was adopted to harmonise the patchwork of laws emerged in Europe. The Data Retention Directive did not require internet and service providers to retain the content of electronic communication, but allowed for the retention of all types of meta-data for a fixed period of time.[7]

In 2013, the entire world was shocked by the revelations of a former contractor of the US Central Intelligence Agency, Edward Snowden. In a series of interviews, Snowden disclosed the existence of various intelligence programmes pre-emptively collecting in bulk communications content and meta-data from major

Values' in D. Curtin and E. Fahey (eds), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders* (Cambridge University Press).

4 See Marieke de Goede, *Speculative Security* (Minnesota University Press 2012).

5 See F. Fabbrini (2015), 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' Harvard Human Rights Journal, Vol. 28: 65-95.

6 Directive 2002/58/EC, Article 15; Directive 95/46/EC, Article 13.

7 See Fabbrini (2015).

US telecommunications operators and internet companies.[8] In Europe, this news received unprecedented attention both at institutional and civil society level. Data of millions of Europeans using US internet services providers had been affected. UK intelligence agencies were discovered to have been involved too.[9] In March 2014, a resolution of the European Parliament strongly condemned the systematic and indiscriminate collection of personal data carried out by the intelligence programmes of the US National Security Agency.[10] However, less than a month later, in the case *Digital Rights Ireland*, the ECJ invalidated the EU Data Retention Directive for failing to limit the width of data collection involved.[11] The EU, too, started removing the beam out of its own eye.

3. EU Legislation and Fundamental Rights

The legal regime introduced by the Data Retention Directive had already been subject to judicial scrutiny at domestic level before *Digital Rights Ireland*. The constitutional courts of Romania, Czech Republic and Germany found the national statutes implementing the Directive in their respective countries to be incompatible with the respect of the right to privacy and data protection of individuals.[12] However, it was only in *Digital Rights Ireland* that the validity of the Directive itself was called into question.

In this case, the ECJ recognised that both the blanket collec-

8 D. Cole, F. Fabbrini and S.J. Schulhofer (eds.) (2017), Surveillance, Privacy, and Transatlantic Relations, Hart Publishing.

9 See S. Schulhofer (2017), 'A Transatlantic Privacy Pact? A Sceptical View', in D. Cole, F. Fabbrini and S.J. Schulhofer (eds.), Surveillance, Privacy, and Transatlantic Relations, Hart Publishing.

10 European Parliament, Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 12 March 2014, P7_TA(2014)0230.

11 *Digital Rights Ireland* [2014] ECJ Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

12 Curtea Constitutionala [Constitutional Court of Romania], decision No. 1258, 8 October 2009; Nález Ustavniho soudu ze dne 22.5.2011 [Decision of the Constitutional Court of the Czech Republic of 22 March 2011], Pl.U S24/10; Bundesverfassungsgericht [German Constitutional Court, 2 March 2010, 125 BVerfGE 261.

tion of meta-data by internet and telephone service providers and the further access to those data operated by national law enforcement authorities represented a "broad ranging" and "particularly serious" interference with the rights to privacy and to data protection, enshrined in Article 7 and 8 of the EU Charter of Fundamental Rights,[13] since a similar system of data retention would enhance people's feeling to be constantly under surveillance.[14] While the ECJ ruled that the Directive did not violate the essence of Articles 7 and 8, and that the regime put in place by the Directive met the first tier of the proportionality test, being suitable to pursue an objective of general interest, such as the fight against crime, the ECJ concluded that the Directive could not pass scrutiny under the necessity test.

In fact, according to the ECJ, the interference with the rights to privacy and data protection went beyond "what is strictly necessary".[15] The ECJ identified five main faults in the Directive, and in particular observed with concern that the Data Retention Directive "entail[ed] an interference with the fundamental rights of practically the entire European population".[16] The Directive did not require to retain exclusively meta-data of individuals who might have a link with a crime, but essentially affected "all persons using electronic communications services".[17] Moreover, the Directive did not set objective criteria to regulate the subsequent access and use of personal data by national authorities as well as did not foresee any prior mechanisms of judicial authorisation.[18]

In 2015, in the *Schrems* case, the ECJ reiterated its condemnation of the model of blanket surveillance.[19] In the aftermath of the Snowden revelations about the existence of US mass surveillance programmes, an Austrian activist, Max Schrems, filed a complaint

13 *Digital Rights Ireland* (n 11) para 37.

14 *Digital Rights Ireland* (n 11) para 37.

15 *Digital Rights Ireland* (n 11) para 51 ff.

16 *Digital Rights Ireland* (n 11) para 56.

17 *Digital Rights Ireland* (n 11) para 58.

18 *Digital Rights Ireland* (n 11) para 62.

19 *Schrems* [2015] ECJ C-362/14, ECLI:EU:C:2015:650.

to the Irish Data Protection Commission. As a Facebook's user, he was concerned about the possibility of his personal data being transferred from Ireland to the US, and potentially being accessed by US national security authorities with no form of scrutiny or remedy offered to European citizens. Article 25 of the Data Protection Directive allowed EU member states to transfer personal data only to third countries ensuring an "adequate level of protection", which, as the ECJ explained, means a level that is "essentially equivalent to that guaranteed within the European Union".[20]

Following a request for a preliminary ruling made by the Irish High Court, the ECJ analysed the compatibility with EU law of the so-called Safe Harbour regime, which allowed for the transfer of personal data from the EU to US corporations. Eventually, the ECJ ruled that the Commission adequacy Decision 2000/520/EC, which, pursuant to the Data Protection Directive, certified the adequacy of the level of safeguards offered by the Safe Harbour agreement, was invalid and struck it down.

The ECJ did not directly examine US surveillance law nor did it explicitly affirm that the US do not offer an "adequate level of protection". However, it pointed out that nothing in the Safe Harbour agreement prevented US national security agencies to access and use all EU personal data on a generalised basis, without establishing preliminarily and clearly the categories of data susceptible to be involved. The ECJ reiterated that a similar derogation to the protection of personal data is not limited to "what is strictly necessary".[21] Moreover, the ECJ went further by affirming that such a model of bulk surveillance, which, in contrast to the case of Data Retention Directive, did not only involve meta-data, but all kinds of personal data, "must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter".[22] The ruling of the ECJ therefore forced

20 *Schrems* (n 19) para 73.

21 *Schrems* (n 19) para 93.

22 *Schrems* (n 19) para 94; on the point, see T. Ojanen (2017), 'Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union', in D. Cole, F. Fabbrini and S.J. Schulhofer (eds.), Surveillance, Privacy, and Transatlantic Relations, Hart Publishing.

the EU to renegotiate an agreement with the US to allow transatlantic data transfer.

4. National Legislation and EU Fundamental Rights

Digital Rights Ireland and *Schrems* focused on two specific regimes, the Data Retention Directive and the Safe Harbour Agreement, both of which were adopted at EU level. Yet, the judgments had a lasting effect also on national legislation. In fact, as the ECJ had the chance to show in *Tele2 Sverige & Watson*, these judgments *de facto* established a series of general criteria to ensure the compatibility of surveillance programmes with EU fundamental rights.[23]

In *Tele2 Sverige & Watson*, the ECJ examined the Swedish and British statutes implementing the Data Retention Directive. Such statutes had formally remained in place even after the invalidation of the Directive. At that time, national legislators and courts were reluctant to interpret *Digital Rights Ireland* as if the ECJ had definitively banned the model of mass data retention and surveillance.[24] In *Tele2 Sverige & Watson*, however, the ECJ ruled that the Swedish and British statutes were implementing Article 15(1) of Directive 2002/58/EC, the so-called e-Privacy Directive, which allows member states to derogate from the obligation of confidentiality of electronic communications if necessary to protect a series of interests, including public and national security.

The ECJ found that, in terms of scope, the domestic data retention statutes under consideration, by requiring a blanket retention of meta-data, essentially mirrored the EU Data Retention Directive.[25] The ECJ observed that similar data retention systems not only represent an interference with Article 7 and 8 of the Charter

23 *Tele2 Sverige* [2016] ECJ Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970; see E. Celeste (2019), 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (European Constitutional Law Review, Vol. 15: 134.

24 See *Secretary of State for the Home Department v Davis MP & Ors* [2015] EWCA Civ 1185.

25 *Tele2 Sverige* (n 23) para 97.

of Fundamental Rights, enshrining the rights to privacy and to data protection, but also with Article 11, protecting the right to freedom of expression, due to the potential chilling effects that a feeling of constant surveillance may generate on individual free speech.[26]

Following *Digital Rights Ireland*, the ECJ then reiterated that a data retention model requiring the collection of personal data in a generalised way, involving all users and any methods of communication, with no differentiation, goes beyond the limits of what can be considered as a necessary and justified interference with the fundamental rights of individuals.[27]

However, in *Tele2 Sverige & Watson*, the ECJ did not limit itself to certify the incompatibility of the bulk data retention models incorporated in the Swedish and British legislation with EU fundamental rights. The ECJ also offered national legislators a pragmatic solution to the issue of data retention. A bulk system of data retention could never be tolerable, even if paired with a set of stringent criteria regulating access by national authorities.[28] However, the ECJ clearly pointed out that a *targeted* system of data retention and subsequent use of data by national authorities would represent an admissible compression of individual rights justified by the legitimate interest of combating serious crimes and terrorism.[29]

The ECJ explained that surveillance should be "the exception", and not "the rule".[30] For this reason, member states should limit the categories of data, means of communications and persons concerned by data retention measures to "what is strictly necessary".[31] The ECJ then stressed that national legislation should circumscribe the number of individuals affected by data retention programmes by requiring the presence of an objective link between the public

26 *Tele2 Sverige* (n 23) paras 92–93.

27 *Tele2 Sverige* (n 23) para 105 ff.

28 Cf. *Secretary of State for the Home Department v Davis MP & Ors* (n 24) paras 48 and 65.

29 *Tele2 Sverige* (n 23) para 108.

30 *Tele2 Sverige* (n 23) para 104.

31 *Tele2 Sverige* (n 23) para 108.

concerned and the crime or risk to be prevented.[32] Lastly, with high sense of pragmatism, the ECJ suggested that this condition could be fulfilled by a domestic legislation restricting data retention practices to one or more geographical areas with a significant level of risk.[33]

5. Conclusion

The case law in *Digital Rights Ireland*, *Schrems*, and *Tele2 Sverige & Watson* shows that the ECJ has increasingly struck the balance between privacy and security in favour of data protection. Despite the efforts by EU and national authorities to adopt surveillance measures in the aftermath of the terrorist attacks of 9/11, the ECJ has step by step invalidated measures such as the Data Retention Directive or national laws implementing it, which created a system of mass surveillance to the detriment of the protection of fundamental rights. Moreover, the ECJ has annulled the Safe Harbour Agreement since it allowed the transfer of data to the US in the absence of adequate privacy protection, and thus with no limits to the ability of US law enforcement authorities to access EU citizens' data. As such, the ECJ has embraced a standard of human rights protection in the field of national security which is arguably the most advanced in comparative perspective, by holding that human rights cannot be sacrificed on the altar of national security.

On the one hand, this has relevance in the short term. A number of cases are in fact currently pending before the ECJ. In October 2017, in the case *Privacy International*, the UK Investigatory Powers Tribunal, which is the British jurisdiction with competence on cases of alleged human rights violations perpetrated by national law enforcement and intelligence agencies, has asked the ECJ to ascertain whether UK's domestic legislation establishing a blanket system of data retention for national security purposes is compatible with the obligation of confidentiality of electronic

32 *Tele2 Sverige* (n 23) para 110.

33 *Tele2 Sverige* (n 23) para 111.

communications provided by the e-Privacy Directive.[34] The preliminary conclusion of the British Tribunal is that bulk collection and processing of data are an "essential necessity […] to protect national security", and that the principles established in *Tele 2 Sverige & Watson* would not be applicable.[35] However, there seems to be no reason why the ECJ should depart from its approach and admit the compatibility of a bulk data retention regime with EU fundamental rights.

Moreover, in May 2018, in the so-called *Schrems II* case, the Irish High Court has referred to the ECJ a further question related to the data transfer between EU and US corporations.[36] The original complaint to the Irish Data Protection Commissioner was filed again by Mr Schrems, this time contesting Facebook Ireland's practice of relying on standard contractual clauses to transfer personal data to its mother company in the US. Standard contractual clauses are one of the mechanisms for transferring EU personal data outside the EU, and consist of model contracts approved by the European Commission. In *Schrems II*, the ECJ will be asked to clarify if the use of these clauses to transfer data to the US is permitted in light of US surveillance laws and practices. After the first *Schrems* case, in US law there have been limited improvements allowing for more transparency and accountability of intelligence and law enforcement authorities, in particular vis-à-vis foreign citizens. Some critical points, however, still persist, making *de facto* very hard to ensure that EU personal data transferred to the US enjoy "essentially equivalent" safeguards.

---

34 *Reference for a preliminary ruling from the Investigatory Powers Tribunal - London (United Kingdom) made on 31 October 2017 – Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (ECJ, Case C-623/17); see *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2017] UK IPT IPT/15/110/CH; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Ors* [2016] IPT/15/110/CH (UK IPT); see Celeste (n 23).

35 *Reference for a preliminary ruling from the Investigatory Powers Tribunal - London (United Kingdom) made on 31 October 2017 – Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (n 34).

36 *Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (ECJ, Case C-311/18).

On the other hand, the case law of the ECJ also has longer term implications. Twenty years ago, in Tampere, member states laid down the strategic objectives of a European area of freedom, security and justice, where police and judicial authorities of different nations could cooperate in order to enhance the protection of individual rights. Achieving that objective required maintaining a high and even level of human rights protection across the EU.

While many challenges in this area remain – including the threatening dynamics of rule of law backsliding in several member states, and not to mention the risks connected to Brexit (the UK decision to leave the EU) in this field – the ECJ has confirmed through its case law on mass surveillance and privacy that it will carefully police this space, to make sure that integration in the field of AFSJ does not result in a limitation of human rights.

References

Celeste, E. (2019), The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios. *European Constitutional Law Review* 15: 134-157.

Cole, D., F. Fabbrini and S. Schulhofer (eds.) (2017). *Surveillance, Privacy, and Transatlantic Relations*, Hart Publishing: Oxford, UK-Portland.

De Goede, M. (2012), *Speculative Security: The Politics of Pursuing Terrorist Monies*, Minnesota University Press: Minneapolis.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002,

Directive 95/46/EC Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

European Parliament (2014). Resolution on the US NSA sur-

veillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 12 March 2014, P7_TA(2014)0230.

Fabbrini, F. (2015a), The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court. In: de Vries S, Bernitz U and Weatherill S (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument*. Hart Publishing: Oxford, UK-Portland.

Fabbrini, F. (2015b), Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States. *Harvard Human Rights Journal* 28: 65-95.

Lenaerts, K. (2010), The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice. *International and Comparative Law Quarterly* 59: 255-301.

Mitsilegas, V. (2014), Transatlantic Counterterrorism Cooperation and European Values. In Curtin D and Fahey E (eds.), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders*, Cambridge University Press: Cambridge.

Ojanen, T. (2017), Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In: D. Cole, F. Fabbrini and S. Schulhofer (eds.), *Surveillance, Privacy and Transatlantic Relations*, Hart Publishing: Oxford, UK-Portland.

Schulhofer, S. (2017), A Transatlantic Privacy Pact? A Sceptical View. In: D. Cole, F. Fabbrini and S. Schulhofer (eds.), *Surveillance, Privacy and Transatlantic Relations*, Hart Publishing: Oxford, UK-Portland.

Case law

Bundesverfassungsgericht [German Constitutional Court, 2 March 2010, 125 BVerfGE 261.

Curtea Constitutionala [Constitutional Court of Romania], decision No. 1258, 8 October 2009.

Digital Rights Ireland (2014). ECJ Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (ECJ, Case C-311/18).

Nález Ustavniho soudu ze dne 22.5.2011 [Decision of the Constitutional Court of the Czech Republic of 22 March 2011], Pl.U S24/10.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Ors [2016] IPT/15/110/CH (UK IPT).

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2017] UK IPT IPT/15/110/CH.

Reference for a preliminary ruling from the Investigatory Powers Tribunal – London (United Kingdom) made on 31 October 2017 – Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (ECJ, Case C-623/17).

Schrems (2015). ECJ C-362/14, ECLI:EU:C:2015:650.

Secretary of State for the Home Department v Davis MP & Ors [2015] EWCA Civ 1185.

Tele2 Sverige (2016). ECJ Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.