Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust (JUD-IT)

Compilation of case notes from relevant EU judgements

JUD-IT Compilation of Case Notes / October 2018

Abstract

As part of the JUD-IT project, Maastricht University has compiled the following set of jurisprudential case notes. The notes focus on specific landmark judgments held by the Court of Justice of the European Union, and scrutise key rulings through which the Court of Luxembourg addressed questions related to the processing of EU data in the prevention, detection, investigation and prosecution of crime and terrorism. The notes help clarifying the conditions that must be met in order for the gathering, accessing and sharing of electronic information by law enforcement authorities to be considered legal under EU law.

The following cases are hereby analyzed:

- Patrick Breyer v Bundesrepublik Deutschland (2016)
- Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ("Tele2") (2016)
- Opinion 1/15, Canada-EU PNR (2017)

This report has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this report are attributable solely to the authors in a personal capacity and not to any institution with which they are associated, nor can they be taken in any way to reflect the views of the European Commission.

Case Note No. 1:

Patrick Breyer v Bundesrepublik Deutschland

Subject of the case

This case considered the definition of 'personal data', the scope of the exception for the activities of the State in areas of criminal law and the relationship between national law and the 'legitimate interests' legal ground for the processing of personal data.

1. Case info

Court/tribunal: Court of Justice of the European Union (CJEU)
Date of judgement: 19 October 2016
Case number: Case C-582/14
European Case Law Identifier: EU:C:2016:779 (CJEU) and EU:C:2016:339 (AG)

2. Case note

2.1. Background of the case

The applicant Mr Breyer is a German politician and activist who consulted various websites of the German federal institutions. These websites kept a log of accesses, including the name of the web page or file accessed, the date and time when a site was accessed, the terms entered in the search fields, the quantity of data transferred, an indication of whether access was successful, and the IP (*internet protocol*) addresses of the devices from which the websites were visited.

An IP address consists of a series of digits assigned to a networked computer to facilitate its communication over the internet. IP addresses may be 'static' or 'dynamic.' Some large internet users will have a 'static' IP address permanently assigned to their devices, which remain the same whenever they access the internet. However, most internet users have a 'dynamic' IP address, which is temporarily assigned to a single connecting client or end-node and which changes each time there is a new connection to the internet. The internet service provider (ISP) concerned keeps a record of which particular dynamic IP address has been assigned to which particular device at a particular time.

As a result, a dynamic IP address does not *per se* identify a specific computer when it accesses the internet. Only the ISP has the additional information linking a dynamic IP address to the specific internet connections which make it possible to identify a visitor to a website.

In this case, the German federal institutions maintained access logs of visitors to their websites with the aim *inter alia* of preventing cyber-attacks and to make it possible to bring criminal prosecutions against the 'pirates' who commit such attacks.

Mr Breyer brought an action before the German courts seeking an injunction to prevent the German federal institutions' websites from registering and storing this information about his visits to their websites.

On appeal, the *Bundesgerichtshof* (Federal Court of Justice, Germany) decided to refer a number of questions to the CJEU.

First it asked whether so-called 'dynamic' IP addresses constitute personal data and hence benefit from the protection provided for such data.

Second, the *Bundesgerichtshof* asked whether the operator of a website must, at least in principle, have the possibility to collect and subsequently use visitors' personal data not only to facilitate and charge for the specific use of the telemedium by the user concerned but also to ensure the general operability of its website and guarantee its security and continued proper functioning.

These questions required the CJEU to consider a third issue, the exception to the scope of Directive 95/46/EC for the activities of the State in areas of criminal law, in view of the websites' aim of processing visitors' data for the purpose of criminal proceedings against 'pirates' and the question of the status of the German federal institutions which provided access to their websites.

2.2. Issues at stake/positions defended by the parties

a) The definition of personal data

Personal data is defined in Article 2(a) of Directive 95/46/EC:

> "Personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

This is further explained in Recital 26 of the Directive 95/46/EC:

> Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.

For present purposes the analysis of Article 2(a) and Recital 26 of the Directive in this case correspond to Article 4(1) and Recital 26 GDPR.

The CJEU first noted that it had already held in *Scarlet Extended*[1] that dynamic IP addresses of internet users were protected personal data because they allow users to be precisely identified. However, the situation in that case was different because both the collection and the identification

[1] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, EU:C:2011:771, para. 51.

of the IP addresses of internet users were carried out by the same entity, the ISPs.[2] Thus from the perspective of the ISP, the IP addresses were personal data. In the present case, however, the federal institutions registered the IP addresses of the users of their websites, but they did not have the additional data necessary in order to identify those users, which is normally held by the ISP concerned.

The CJEU therefore had to decide whether the German federal institutions (the data controllers) should treat the IP addresses as personal data even if they were not in possession of this additional information.

The Court first noted that a dynamic IP address does not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer.

The Court then considered whether an IP address may be treated as data relating to an 'identifiable natural person' where the additional data necessary in order to identify the user are held by a third party, the user's ISP. Under Article 2(a) of the Directive, an identifiable person is one who can be identified indirectly as well as directly, and Recital 26 explains that, in order to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by *any other person* to identify the said person (emphasis supplied). On this basis, the Court concluded that the information enabling the identification of the data subject does not all have to be in the hands of one entity, so that the fact that the necessary information was split between the websites and Mr Breyer's ISPs did not preclude the dynamic IP addresses from being personal data.

However, the Court stressed that the possibility to combine a dynamic IP address with the additional data held by the ISP had to be a *means likely reasonably to be used* to identify the data subject. In this respect it agreed with Advocate General Campos Sánchez-Bordona that this would not be the case if the possibility of the identification of the data subject was insignificant in reality, for example, if it was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power.[3]

On the basis of the facts in the order for reference, the Court found, first, that national law did not allow the ISP to provide the additional identification information directly to the websites providers. However, the Court noted that, subject to verification by the referring court, legal channels exist in certain circumstances, in particular in the event of cyber-attacks, so that a website provider would able to contact the competent authority to bring criminal proceedings, and in that context for the authority to obtain the additional information from the visitor's ISP. As a result, the means existed which could reasonably be used in order to identify an individual, so that the information collected by the website constituted personal data within the definition in Article 2(a) of the Directive.

b) The exception relating to activities of the State in areas of criminal law

[2] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, EU:C:2016:779, para. 33-34.

[3] Opinion of Advocate-General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, EU:C:2016:339, para. 68.

Since the maintenance of the operability of the websites and the prevention of cyberattacks might ultimately lead to criminal proceedings against the perpetrators, the CJEU considered, before considering the answer to the second question, whether the processing of IP addresses in such circumstances is not excluded from the Directive altogether.

This is because of the exception under Article 3(2), first indent, of Directive 95/46, which provides that:

> This Directive shall not apply to the processing of personal data … in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law (…).

The Court has consistently stressed that this exception must be interpreted strictly and should be applied only to the activities which are expressly listed there or which can be classified in the same category (*ejusdem generis*). In this respect, the Court has characterised them as activities of the State or of State authorities and thus unrelated to the fields of activity of individuals.[4]

On this basis, the Court considered the nature of the activities of the German federal institutions in providing information on their websites and concluded that, in spite of their status as public authorities, they were acting as individuals *sine imperio* and outside the activities of the State in the area of criminal law. As a result, the exception did not apply.[5]

c) Compatibility of a restriction under national law with Article 7(f) of Directive 95/46/EC

The national law governing the collection and use of personal data to make telemedia available is laid down in the *Telemediengesetz* (Law on telemedia) of 26 February 2007 (BGBl. 2007 I, p. 179, 'TMG'). Paragraph 12(1) of the TMG provides:

> A service provider may collect and use personal data to make telemedia available only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

Paragraph 15(1) of the TMG provides:

> A service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use).

The national court restrictively interpreted the TMG to authorise the collection and use of personal data relating to a user of those services, without his consent, only to the extent that is it is necessary to facilitate and charge for the specific use of the website by the user concerned. The CJEU noted

---

[4] Case C-582/14 *Patrick Breyer v Bundesrepublik* Deutschland, para. 52, referring to the CJEU judgments Case C‑101/01 *Lindqvist*, EU:C:2003:596, para. 43, and Case C‑73/07 *Satakunnan Markkinapörssi and Satamedia*, EU:C:2008:727, para. 41.

[5] See the Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 82-92.

that this restrictive interpretation did not extend to the objective of protecting the website against cyber-attacks.

The question was whether this restriction was compatible with Article 7 of Directive 95/46/EC. This provision sets out an 'exhaustive and restrictive list' of six principles which permit the lawful processing of personal data. The Court has held that 'Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article.'[6]

Under Article 5 of the Directive the Member States have a margin of discretion to specify the conditions under which the processing of personal data is lawful. However, this cannot exceed the limits of Article 7 and the objective of the Directive.

In this respect, Article 7(1)(f) provides that:

> (…) personal data may be processed only if (…) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).

The Court noted that the restrictive interpretation of the national legislation by the national court would only permit the processing of personal data by the websites to the extent that it is necessary to facilitate and invoice the specific use of services by visitors, and would preclude the continued storage of personal data in order to ensure the general operability and continued functioning of those websites. However, under Article 7(1)(f) of the Directive, the processing of personal data is lawful if it is necessary to achieve a legitimate objective pursued by the controller, or by the third party to which the data are transmitted, provided that the interest or the fundamental rights and freedoms of the data subject does not override that objective.

In this respect, the German Federal institutions which provided the websites had a legitimate interest in ensuring the continued functioning of their websites which goes beyond each specific use of their publicly accessible websites, and this interest should be balanced with the interests of data subjects.

The Court concluded that the national legislation reduced the scope of the principle laid down in Article 7(1)(f) of Directive 95/46/EC by excluding the possibility of balancing the objective of ensuring the general operability of the websites against the interests or fundamental rights and freedoms of data subjects. In consequence Article 7(1)(f) precluded the legislative restriction under national law.

2.3. Explanation of the Court decision

The reasoning in *Breyer* follows the consistent case law of the Court in applying a broad interpretation to the scope of the data protection rules under the Directive and a strict approach to the exceptions to its scope.

---

[6] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 57-58, referring to the CJEU judgment Joined Cases C‑468/10 and C‑469/10 *ASNEF and FECEMD*, EU:C:2011:777, para. 30, 32-34 and 36.

a) The definition of personal data

The ruling is consistent with the broad approach by the Article 29 Working Party in its Opinion on Personal Data.[7] This states unequivocally that IP addresses are regarded as data relating to an identifiable person, and specifically refers to cases where the IP address is processed with the intention of identifying the user of a computer, where the controller anticipates that the "means likely reasonably to be used" to identify the persons will be available, e.g. through the courts appealed to.[8]

The GDPR has kept essentially the same wording of the definition of personal data in Article 4(1) and the same explanations in Recital 26, so this line of case law will remain applicable. With regard to the specific issue of IP addresses, Recital 30 GDPR further clarifies that '(n)atural persons may be associated with online identifiers (…) such as internet protocol addresses'.

At national level there was a debate between two schools of thought. Under the 'objective/absolute' approach, a user is identifiable when it is feasible to identify him or her by combining their dynamic IP address with data provided by a third party. Under the 'subjective/relative approach', information held by a third party is irrelevant and a person is identifiable only in terms of the information actually held by the putative controller.[9]

The CJEU did not address this issue as such but followed a middle line, which did not limit the scope of identifiability only to data held by the putative controller (subjective/relative approach) but required a case-by-case analysis of whether the information held by a third party was reasonably likely to be available, a "means likely reasonably to be used", to identify the user (in effect, a restricted objective/absolute approach).[10] While the Court interpreted its approach quite widely, it affirmed that there may be situations where identification is not feasible because "the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant."[11]

This discussion of identifiability illustrates the difference between *anonymization* and the new concept of *pseudonymisation* introduced in the GDPR and defined in Article 4(5) thereof:

> the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

---

7 Opinion 4/2007, WP136 of 20 June 2007.

8 Ibid., Example No. 15, p. 16-17.

9 See Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 25, and the Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 52 and 53.

10 See F. Niemann and L. Schüßler, 'CJEU decision on dynamic IP addresses touches fundamental DP law questions', *Bird & Bird*, 21 October 2016, available at: https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions.

11 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 46; Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 68.

The GDPR treats pseudonymous data as personal data relating to an identifiable person and hence subject to its rules. Pseudonymisation is recommended as an extra safeguard for protecting personal data, for example as a part of data protection by design under Article 25(1) GDPR.

In contrast, if personal data is *anonymised*, and there is no reasonable scope for combining that data with third party data to identify a data subject, then the data protection rules will not apply at all.

b) The criminal proceedings exception

Neither the Court nor the Advocate General saw any room for the criminal proceedings exception, under Article 3(2), first indent, of the Directive, to apply in the present case, because the German Federal institutions were not acting in their capacity of public authorities when they processed the IP addresses. The judicial policy is clear, that the criminal proceedings exception should only apply to public authorities carrying out the activities of the State in the area of criminal law. This issue is further discussed in Case Note No. 2 on *Tele2 Sverige and Watson*.

However, the question arises whether it is appropriate to extend the meaning of 'individual' to cover public authorities generally. Normally the term "individual" is used as a synonym for "natural person", as in the full titles of earlier data protection instruments which refer to the protection of *individuals* with regard to the processing of personal data, including Directive 95/46/EC, Regulation 45/2001/EC and Council of Europe Convention No. 108 (though the GDPR now refers to the protection of *natural persons*).

This might be important in the context of another exclusion under the Data Protection Directive, the exception under Article 3(2), second indent, of Directive 95/46/EC. This provides that:

> This Directive shall not apply to the processing of personal data (…) by a natural person in the course of a purely personal or household activity.

This exception is plainly intended for natural persons and it would be inappropriate for a public authority to invoke it on the basis that it is acting as an 'individual' qua 'natural person.' Whilst legal persons fall within the scope of the right to privacy, Recital 14 GDPR clarifies that the Regulation does not cover the processing of personal data which concerns legal persons. Moreover the CJEU has confirmed in Ryneš[12] that the "household purposes" exemption is strictly limited to purely personal activities (e.g., personal correspondence or personal use of social networking services).

c) The scope of the legitimate interests ground for processing

Having received the interpretation of an EU instrument by the Court, a national court should, first, interpret the national legislation consistently with the wording and the purpose of the Directive.[13] This general principle of consistent interpretation (*interprétation conforme*)[14] requires the national court to interpret the national legislation consistently with the provisions of the Directive "as far as possible",[15] if necessary in light of national law as a whole.[16] "In order to perform conform

---

[12] Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů, Judgment*, EU:C:2014:2428.

[13] Case 14/83 *Von Colson and Kamann v. Land Nordrhein-Westfalen*, EU:C:1984:153, para. 26.

[14] See A. Dashwood et al. (eds.), *Wyatt and Dashwood's European Union Law* (6th edition, Hart Publishing, 2011), p. 239-244.

[15] Case C–106/89 *Marleasing*, EU:C:1990:395, para. 8.

[16] Joined Cases C-397/01 and C-403/01 *Pfeiffer*, EU:C:2004:584.

interpretation with EU law, national judges must use the room available under national law (as a whole) in order to achieve the purpose of the EU act."[17] The interpretation may go beyond what is semantically possible so long as it does not unavoidably contradict the intended purpose of the national legislation (*contra legem*)[18] or extend the scope of liability under national criminal law.[19]

In the present case both the Court and the Advocate General found that the national legislation, "if it were interpreted in the strict manner" put forward by the national court, reduced the scope of the legitimate interests ground for processing laid down in Article 7(f) of the Directive.[20] As a result, the Court found that EU law precluded the restriction to processing solely for facilitating or charging for the use of the websites.[21] The Advocate General noted that the national court was "required to interpret the national legislation in a manner consistent with Directive 95/46," so that the legitimate interest of the federal institutions in ensuring the continued functioning of their websites could be taken into account and balanced, on a case-by-case basis, against the user's interests or fundamental rights.[22]

3. Main implications

There are three main implications of this ruling.

First, the CJEU has confirmed that the definition of 'personal data' is very wide. Even where it is not possible for the putative data controller to identify an individual on its own, the data being processed will be personal data if they can be combined with additional data held by another party which makes it reasonably possible to identify the individuals concerned. This will be the case even when the additional information can only be obtained as a result of independent legal action by a completely different public authority. Note, however, that the analysis must be done case by case and in view of local law. Rather than an absolute approach, the Court followed the relative approach subject to the test that the means of combining the data held by the putative controller with the data necessary to identify the individual concerned must be "likely reasonably to be used to identify" the individual. This approach has been praised as "more flexibility and (...) more leeway for certain anonymisation and Big Data practices that 'help' actors to stay out of the scope of data protection law."[23]

Second, the exceptions to the scope of the data protection rules must be narrowly interpreted. In particular, if data are collected and recorded merely as a preventive measure, in case they may be used to support a complaint to the criminal law enforcement authorities at some stage in

[17] See *Consistent interpretation*, European University Institute, Centre For Judicial Cooperation, available at: http://judcoop.eui.eu/data/?p=data&fold=1&subfold=1.1.1.

[18] Case C-105/03 Pupino, EU:C:2005:386, para. 47.

[19] Case 80/86 *Kolpinghuis Nijmegen BV*, EU:C:1987:431.

[20] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 59.

[21] Ibid., para. 62-64.

[22] Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 102.

[23] P. De Hert, 'Foreword: Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer', 1 *EDPL* 3 (2017), p. 27.

the future, such processing does not fall within the "criminal law enforcement" exception.[24] Only the processing of the data for law enforcement purposes by a criminal law authority, or specifically for such an authority, will fall within the exception.[25]

Third, national legislation which purports to govern the legitimate grounds for lawful processing must be interpreted so far as possible not to reduce the scope of the grounds laid down in the EU data protection legislation, and otherwise must not be applied by the national court. The level of harmonisation under the Directive has been strictly enforced by the CJEU in its *ASNEF* and *Breyer* rulings. Harmonisation has now been greatly increased under the GDPR, and it is the duty of national courts to enforce it.

[24] Opinion of Advocate General Sánchez-Bordona in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, para. 88-92.
[25] Joined Cases C-317/04 and C-318/04 *Parliament v Council and Commission* EU:C:2006:346, para. 58.

Case Note No. 2:

Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ("Tele2")

Subject of the case

In this case, the CJEU balanced the fundamental rights of privacy, data protection and freedom of information with the needs of the State to ensure security and criminal law enforcement.

1. Case info

Court/tribunal: Court of Justice of the European Union (CJEU)
Date of judgement: 21 December 2016
Case number: Joined Cases C-203/15 and C-698/15
European Case Law Identifier: EU:C:2016:970 (CJEU) and EU:C:2016:572 (AG)

2. Case note

2.1 Background of the case

Directive 2002/58 (the ePrivacy Directive)[26] lays down privacy and data protection obligations, relating to electronic communications, specifying and complementing those under Directive 95/46/EC (the Data Protection Directive).[27] In particular the fundamental right to confidentiality of communications enshrined in Article 7 of the Charter of Fundamental rights of the European Union (the Charter) is specified in Article 5(1) of the ePrivacy Directive. This reiterates the obligation to ensure confidentiality of communications, and prohibits the interception of electronic communications without the consent of the user concerned, with the sole exception

[26] 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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ 2009 L 337, p. 1).

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, p. 31.

of interception authorised by national legislation adopted in accordance with Article 15(1) of the ePrivacy Directive. Similarly Articles 6 and 9 of the ePrivacy Directive specifically protect the processing of related traffic data and location data subject to restrictions under Article 15(1).

Article 15(1) of the ePrivacy Directive permits Member States to adopt legislative restrictions on, inter alia, the rights and obligations laid down in Articles 5, 6 and 9, when any such restriction 'constitutes a necessary, appropriate and proportionate measure 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'.

This *option* for Member States to derogate from the ePrivacy Directive was transformed into an *obligation* on service providers to retain the metadata of electronic communications under the Data Retention Directive 2006/24/EC.[28] However the Court of Justice of the European Union (CJEU) declared that directive invalid in its *Digital Rights* ruling because the general obligation to retain traffic data and location data constituted an interference with the fundamental rights to respect for privacy and the protection of personal data which was not limited to what was strictly necessary. [29] The Court laid down a number of minimum mandatory safeguards which had to be complied with in order to limit the interference with the rights enshrined in the ePrivacy Directive and Articles 7 and 8 of the Charter to what is strictly necessary.[30]

As a result of the invalidation of the Data Retention Directive, Member States were no longer *required* to retain telecommunications metadata but they still had the possibility to *derogate from* the obligations imposed under the ePrivacy Directive by virtue of Article 15 thereof.

On the day after the ruling in *Digital Rights*, the Swedish operator Tele2 Sverige informed the Swedish Post and Telecom Authority (PTS) that it would no longer retain personal data and would erase the personal data retained prior to that date. A commission of inquiry was set up which concluded that the Swedish data retention legislation met the standards laid down in the *Digital Rights* ruling.[31] In consequence, the PTS adopted a decision requiring Tele2 to continue retaining the information, and Tele2 challenged that decision (Case C-203/15 *Tele2*).

In the UK, the government rapidly adopted fresh legislation, the Data Retention and Investigatory Powers Act (DRIPA) 2014. The DRIPA enabled the government to require public telecommunications operators to retain all the data relating to communications for a maximum

[28] 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, OJ 2006 L 105, p. 54.

[29] Joined Cases C-293 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, EU:C:2014:238. See the case comment by O. Lynskey, 'The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*', 51 *CML Rev.* 6 (2014), p. 1789.

[30] See Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, EU:C:2016:572, para. 216-226.

[31] See I. Cameron, 'Balancing data protection and law enforcement needs: Tele2 Sverige and Watson', 54 *CML Rev.* 5 (2017), p. 1471-1473.

period of 12 months, with the exception of the content of those communications. This new legislation was challenged by Members of the UK Parliament (Case C-698/15 *Watson*).

As a result, the Administrative Court of Appeal in Stockholm and the Court of Appeal in London referred a number of questions to the CJEU concerning these challenges. These questions between them raised three issues of interpretation of Article 15(1) of the ePrivacy Directive, read in the light of Articles 7, 8 and 52(1) of the Charter:

1. whether national rules that impose on providers a general obligation to retain data are compatible with EU law (the first question in *Tele2*)
2. whether national rules are compatible with EU law that prescribe an obligation to retain data and make provision for access by the competent national authorities but (i) do not restrict that access solely to the objective of fighting serious crime, (ii) do not subject that access to prior review by a court or an independent administrative authority, and (iii) do not require that the data concerned should be retained within the EU (the second question in *Tele2* and the first question in *Watson*); and
3. whether the Court interprets Articles 7 and 8 of the Charter in such a way as to expand the scope conferred on Article 8 ECHR by the ECtHR (the second question in *Watson*).

Following the Opinion of Advocate General Saugmandsgaard Øe of 19 July 2016, the CJEU ruled as follows:

1. Article 15(1) of Directive 2002/58/EC (…) read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (…) must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.
2. Article 15(1) of Directive 2002/58 (…) read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (…) must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.
3. The third issue, in the second question referred by the Court of Appeal in London, was held to be inadmissible.

2.2. Issues at stake/positions defended by the parties

The positions taken by the intervening governments on data retention for intelligence and law enforcement purposes differed: the Belgian, Danish, German, Estonian, Irish and Dutch governments considered that the issue was within EU law. The Czech Government considered

that it was not. The UK Government took the position that national law dealing with retention fell within the scope of EU law, but not national laws on access.[38] A similar position to that of the UK Government was taken by the Commission, which nonetheless considered that the national laws on access could be taken into account in assessing the compatibility with EU law of the national laws on retention.

2.3. Explanation of the Court decision

In its Press Release, the Court effectively summarised the main elements of its ruling as follows:

The Member States may not impose a general obligation to retain data on providers of electronic communications services

EU law precludes a general and indiscriminate retention of traffic data and location data, but it is open to Members States to make provision, as a preventive measure, for targeted retention of that data solely for the purpose of fighting serious crime, provided that such retention is, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the chosen duration of retention, limited to what is strictly necessary. Access of the national authorities to the retained data must be subject to conditions, including prior review by an independent authority and the data being retained within the EU.

The Court first explained the difference between the *scope* of the EU data protection rules, as enshrined in the ePrivacy Directive and the Data Protection Directive, now the GDPR, and the *possibility to derogate* from those rules. When a security or law enforcement authority processes personal data for the purpose of State activities such as national security or law enforcement, Article 3(1) of the ePrivacy Directive specifies that that processing falls outside its scope.[32] National security processing falls outside the scope of the Treaties, per Article 4(2) TFEU, and law enforcement falls within the scope of the separate Law Enforcement Directive.[33]

In contrast, when a private operator or public authority processes personal data for its own purposes within the scope of EU law, Article 15(1) of the ePrivacy Directive permits Member States to derogate from certain obligations under the data protection rules for the purposes of the same State activities of, inter alia, national security and law enforcement.[34]

The Court noted that the objectives under Article 15(1) 'overlap substantially with the objectives pursued by the activities referred to in Article 1(3)'. However it reasoned that the legislative measures referred to in Article 15(1) cannot be excluded from the scope of the directive, 'for otherwise that provision would be deprived of any purpose' and indeed that

[32] See also Article 3(2) of the former Data Protection Directive 95/46 and Article 2(a), (b) and (d) of the GDPR.
[33] Directive (EU) 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, OJ 2016 L 119, p. 89.
[34] See also Article 13(1) of the Data Protection Directive and Article 23(1) of the GDPR.

'Article 15(1) necessarily presupposes that the national measures referred to therein' fall within the scope of the ePrivacy Directive.[35]

Thus, the processing of personal data by private operators, including its retention and affording access to it by security or law enforcement, falls under the ePrivacy Directive and the GDPR, whereas the subsequent processing of that data by the security or law enforcement authorities themselves is outside the scope of these instruments, either under national competence or under the Law Enforcement Directive.

Second, the Court considered Article 15(1) in light of Articles 7 and 8 of the Charter and the obligations laid down in the Directive. The general obligation under Article 5(1) to ensure the confidentiality of communications, as well as the corresponding obligations under Articles 6 and 9 of the Directive, which protect traffic and location data, require Article 15(1) to be interpreted strictly. This principle of confidentiality of communications implies, inter alia, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised by national law in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication. Such national laws, restricting the obligations under the ePrivacy Directive, cannot be allowed to become the general rule, otherwise the general obligation of confidentiality would be 'rendered largely meaningless'.[36]

The Court further noted that Article 15(1) should not only be considered in light of the rights to privacy and protection of personal data enshrined in Articles 7 and 8 of the Charter but also in light of the right to freedom of expression enshrined in Article 11 of the Charter. It declared that freedom of expression 'constitutes one of the essential foundations of a pluralist, democratic society'.[37]

In this context, the Court proceeded to consider the national laws in Sweden and the UK in the light of the principles of necessity and proportionality. It noted that these principles must be applied under Article 52(1) of the Charter, under the specific provisions of the ePrivacy Directive, and by its own settled case law to the effect that 'derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary'.[38]

The Court applied these principles in two respects: the mass retention of data by operators, and access to that data by the authorities.

a) The mass retention of data

The Court noted that the national legislation "provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all

[35] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 72 and 73.
[36] Ibid., para. 82-89.
[37] Ibid., para. 93.
[38] Ibid., para. 96 and case law cited therein.

means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions."[39]

The Court found that metadata can be as revealing as content. Taken as a whole, it allows "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[40]

This was not only a particularly serious and far-reaching interference with the rights to privacy and data protection. It could also affect the use of means of electronic communication and, consequently, "the exercise by the users thereof of their freedom of expression".[41]

In *Digital Rights*, the Advocate General had referred to 'the vague feeling of surveillance' which is 'capable of having a decisive influence on the exercise (...) of their freedom of expression and information.'[42] The Court in that case agreed that the data retention was 'likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[43] However, this aspect was regarded as merely ancillary to the interference with privacy and data protection and it did not figure in the operational part of the judgment.

In contrast, this additional element of serious interference with freedom of expression served to reinforce the Court's ruling in the present case. It found that even the important societal interest of combating serious crime, in particular organised crime and terrorism, cannot in itself justify a general and indiscriminate retention of all traffic and location data. The Court did not follow the Advocate General on this point, who had advised that the general retention of data may be acceptable if it respects all the necessary limits and safeguards.

The Court recalled that under the national legislation in question the retention of metadata was the rule rather than the exception, and the data of wholly innocent people would be retained, including the data of persons whose communications are protected by professional secrecy.[44] This would include, for example, judicial secrecy, legal professional privilege,[45] medical secrecy and journalism.

---

[39] Ibid., para. 97.
[40] Ibid., para. 99.
[41] Ibid., para. 101.
[42] Opinion of Advocate General Cruz Villalón in Joined Cases C-293 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, EU:C:2013:845, para. 52.
[43] Joined Cases C-293 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, para. 37.
[44] Joined Cases C-203/15 and C□698/15 *Tele 2 and Watson*, para. 104-105.
[45] ECtHR, *Michaud v France* (app no. 12323/11), 6 December 2012; ECtHR, *RE v The United* Kingdom (app no. 62498/11), 27 October 2015. See M. Galic, 'Covert Surveillance of Privileged Consultations and the Weakening of the Legal Professional Privilege', 2 *EDPL* 4 (2016), p. 602.

Furthermore, the national legislation did not require any specific relationship between the data retained and a threat to public security. In particular, it was "not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime".[46]

The Court concluded that such legislation exceeded the limits of what is strictly necessary and could not be justified under the Directive or the Charter.

The Court then proceeded to explain what type of narrow approach to data retention *would* be justifiable under these criteria. A *targeted* retention of traffic and location data could be acceptable as a preventive measure for the purpose of fighting serious crime "provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary". That is, the retention of data must still meet objective criteria, that establish a connection between the data to be retained and the objective pursued. For example, "such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences".[47]

In any event, there must be "clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse".[48]

The Court therefore concluded, with regard to the first question referred in Case C-203/15 (*Tele2*) that "Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."[49]

b) Access to that data by the authorities

The Court then considered the second question in Case C-203/15 (*Tele2*) and the first question in Case C-698/15 (*Watson*), whether the access of the competent national authorities to retained data compatible with Article 15(1) of the ePrivacy Directive, read in the light of Articles 7, 8 and Article 52(1) of the Charter, where three alternative conditions applied:

- such access was not restricted solely to the objective of fighting serious crime,
- it was not subject to prior review by a court or an independent administrative authority,

[46] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 106.
[47] Ibid., para. 108-111.
[48] Ibid., para. 109.
[49] Ibid., para. 112.

- there was no requirement that the data concerned should be retained within the European Union.

The Court applied the same criteria limiting the retention of data to access to that data.

First, applying the principle of proportionality to the area of prevention, investigation, detection and prosecution of criminal offences, the Court reiterated that only the objective of fighting serious crime is capable of justifying access to the retained data.[50]

Applying the principle of necessity, it found that a general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary. To the contrary, "access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime."[51] In this respect, the Court cited the ECtHR ruling in *Zakharov v Russia*, where the ECtHR underlined the need for there to be a "reasonable suspicion" against the persons concerned.[52]

The Court accepted however that access to the data of other persons might also be granted in particular situations, where vital security or defence interests are threatened by terrorist activities, "where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities."[53]

Second, in order to ensure that these conditions are fully respected, the Court required that access to retained data should be subject to a prior review carried out either by a court or by an independent administrative body on the basis of a reasoned request by the investigating authorities.[54] The Court specifically referred to the ruling of the ECtHR in *Szabó and Vissy v Hungary* that "in this field, control by an independent body, normally a judge with special expertise, should be the rule"[55], except in cases of urgency.[56]

The Court stressed that the legislation should provide that the competent national authorities should notify the persons affected "as soon as this is no longer liable to jeopardize the investigations being undertaken by those authorities." Such notification is necessary to enable these persons to exercise their right to a legal remedy.[57]

Finally, the Court laid down requirements relating to the security of the retained data and supervision by an independent authority. It noted that Article 15(1) of the ePrivacy Directive did not provide for any derogation to the obligation to ensure the security of the retained data, and

[50] Ibid., para. 115.
[51] Ibid., para. 119.
[52] ECtHR, *Roman Zakharov v Russia* (application no. 47143/06), 4 December 2015, para. 260.
[53] Joined Cases C-203/15 and C-698/15, *Tele 2 and Watson*, para. 119.
[54] Ibid., para. 120.
[55] ECtHR, *Szabó and Vissy v Hungary* (Application no. 37138/14), 12 January 2016, para. 80.
[56] Ibid., para. 77.
[57] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 121.

concluded that this required service providers to guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In this respect, the Court stressed, first, that national legislation should provide for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period. The Court did not follow the suggestion by the Advocate General that a Member State could reasonably go further and require that the data be stored within the national territory, especially in the absence of coordination of national authorities within the European Union.[58]

Second, the Court stressed the need to ensure review of compliance by an independent supervisory authority, as required under Article 8(3) of the Charter. This constitutes, in accordance with the Court's settled case law, an "essential element" of the right to protection of personal data and makes it possible for persons whose personal data was retained to complain to the national supervisory authority seeking the protection of their data.[59]

The Court concluded that "Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."

c) The scope of Articles 7 and 8 of the Charter compared to Article 8 ECHR

The second question in *Watson* was whether the Court gave Articles 7 and/or 8 of the Charter a wider scope than Article 8 ECHR, as interpreted by the ECtHR. The Court concluded that since giving an answer to this question was not necessary for the national court to decide the issue in accordance with EU law, it would therefore not answer it.

d) The reaction of the national courts to the preliminary ruling

On 22 December 2016, immediately following the preliminary ruling by the CJEU, the Administrative Court of Appeal in Stockholm found that the Swedish data retention legislation was invalid and annulled the decision of the PTS requiring Tele2 to retain information of data flows for law enforcement purposes.[60]

---

[58] Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 241.

[59] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 122 and 123.

[60] See Kammarrätten bifaller överklagandet och upphäver Post-och telestyrelsens beslut den 27 juni 2014 att förelägga Tele2 Sverige AB att lagra trafikuppgifter m.m. för brottsbekämpande ändamål.

On 30 December 2016, following an independent review,[61] the UK adopted new legislation, the Investigatory Powers Act,[62] which replaced the DRIPA, the subject of the reference in *Watson*. On 30 January 2018, the Court of Appeal in London declared that the earlier legislation was incompatible with EU law to the extent that it permitted access to retained data where the purpose of such access was not limited solely to fighting serious crime and where such access was not subject to prior review by a court or an independent administrative authority.[63] The Court did not address other matters in the ruling, which are the subject of a fresh request for a preliminary ruling by another UK court, the Investigatory Powers Tribunal.[64]

3. Main implications

This ruling is the third in a series of four rulings by the CJEU that address the increasing resort by national authorities to the mass processing of personal data. It was preceded by the rulings in *Digital Rights* and *Schrems*[65] and followed by the ruling in Opinion 1/15 *EU-Canada PNR* (see JUD-IT Case Note No. 3). In this line of cases the Court can be seen as imposing a balance between the interests of the State and the fundamental rights of those whose privacy and personal information are affected by such processing. In the present case the Court has specifically balanced the interests of effective law enforcement and national security with the need to protect the fundamental rights of privacy, data protection and, for the first time, freedom of expression.

In this respect, the European Bar in particular has underlined the dangers to individual liberty when State authorities can process personal data of everybody, including independent advocates defending their clients. The same threat exists of course for independent judges hearing their cases. The CCBE has stated that "this kind of mass surveillance goes beyond risking specific human rights between private persons, and is a threat to the rule of law as recognised in modern democracies."[66] The CCBE has intervened on this issue in the *Prakken d'Oliveira* case, where the Court of Appeal in The Hague ordered the Dutch State to stop all surveillance of lawyers' communications until it provided for independent oversight. Otherwise interception of privileged communications was a violation of the right to a fair trial and undermined the rationale behind professional secrecy.[67]

---

[61] *Report of the Bulk Powers Review* by David Anderson QC, Independent Reviewer of Terrorism Legislation, Command 9326, August 2016.

[62] See the review of the compatibility of the Investigatory Powers Act with EU law following the *Tele2* ruling in W.R. Mbioh, 'Post-Och Telestyrelsen and Watson and the Investigatory Powers Act 2016', 3 *EDPL* 2 (2017), p. 278-282

[63] [2018] EWCA Civ 70.

[64] Case C-623/17 *Privacy International*, pending. See C. Kuner et al., 'An unstoppable force and an immoveable object? EU data protection law and national security', 8 *IPDL* 1 (2018), p. 1.

[65] Case C-362/14 *Schrems v Data Protection Commissioner*, EU:C:2015:650.

[66] CCBE Statement on mass electronic surveillance by government bodies (including of European lawyers' data) 14/10/2013.

[67] Case 200.174.280-01, judgment of 27 October 2015, ECLI:NL:GHDHA:2015:2881.

The ruling therefore establishes that bulk surveillance is only acceptable according to certain conditions: it must be targeted rather than generalised, it must be objectively justified, and it cannot be carried out, in principle, unless it has first been checked and authorised by an independent judicial or equivalent administrative body. The private individuals whose data is being processed by the authorities must be given the opportunity to know that such processing is taking place, at least later on when there is no threat to the investigation as a result, the data must be stored within the jurisdiction of the European Union, and private individuals must have the possibility of lodging a complaint with an independent supervisory authority.

It has been argued that the ruling is of greater benefit in Member States where control over the police and intelligence services is unsatisfactory, than in those Member States where such control is effective and where, it is argued, the ruling may actually hinder the effective pursuit of criminal investigations and "flings a large spanner into the effective works of criminal investigations."[68] From this point of view, the main impact of the ruling is that it precludes the possibility of imposing a general duty of retention of location and traffic data. This challenges the policy by Member States of mass surveillance of the whole population, so as to have communications data available for the identification of hitherto unknown criminals and terrorists. Unless the data of everybody is retained, it is argued, the data of criminals and terrorists who are as yet unknown will not be available when the authorities need to find it.

A number of points may be made concerning the argument that the ruling makes it more difficult to ensure public safety. First, the ruling only refers to *preventive* data retention. It is still possible for the authorities to *preserve* data being held immediately after the commission of an offence, and to retain data generated after the event on the basis of a specific investigation.[69]

Second, traffic metadata are in any event retained by operators, for billing purposes. They are authorised to retain such under Article 6(2) of the ePrivacy Directive up to the end of the period during which the bill may lawfully be challenged or payment pursued (which may range in many cases between four weeks and six months, depending on the operator concerned). In consequence, as in the case of PNR flight data, discussed in Case Note No. 3 on Opinion 1/15 *EU-Canada PNR*, the State may rely on personal data that private operators are processing for their own purposes. So in any event there will be "historic" data available to investigations, in addition to data which is "frozen" when an investigation commences. Access to this retained data will be possible so long as the Court's criteria are respected, that is, that the objective of access is limited to fighting serious crime, that access is subject in principle to prior review by a court or independent administrative authority, and that the persons affected by the granting of such access should be notified about it as soon as such notification is no longer liable to jeopardise the investigations being undertaken by those authorities.[70]

---

[68] I. Cameron, supra, p. 1481.
[69] See the Council of Europe Convention on Cybercrime, ETS 185, 23 November 2001, Articles 16 -17.
[70] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 120- 121.

Third, the Court included within its definition of "targeted" retention the possibility of retaining data within a specific group or geographical zone. This is possible in cases of "objective evidence that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences"[71] or to cases of a "group of persons likely to be involved, in one way or another, in a serious crime."[72]

It is interesting to compare these criteria with the Court's ruling in Opinion 1/15 on the draft *EU-Canada PNR* Agreement. In that case, the Court permitted the general retention of the flight data of a large group of people, the travellers flying from the EU to Canada. The collection of this data was necessary for the border control purposes of the recipient country (as recognised by multinational treaty), it did not include the data of privileged groups *per se*, nor was it permitted by the Court to include the collection of sensitive data. The extent of the interference with the rights of privacy, data protection and freedom of expression was thus more limited, especially in view of the restrictions imposed by the Court on processing such data after air travellers had arrived in Canada.[73]

In another case, *Ministerio Fiscal*, the police had requested access to personal data held by a telecoms operator and the interference with fundamental rights was relatively small. The request for access was targeted at a very small group of persons specifically connected in some way to the theft of a mobile phone (the persons telephoned by that stolen mobile phone), was limited to a very short period (twelve days after the theft of the phone), concerned only limited categories of personal data (surnames, forenames and possibly the addresses of the individuals targeted by the investigation), and concerned access to data generated after the event on the basis of a specific investigation.[74]

In the present case, the Court did not follow the normally influential Opinion of its Advocate General. Advocate General Saugmandsgaard Øe had suggested that mass surveillance is acceptable so long as it follows the strict requirements of EU law, in particular, so long as it is satisfies strict requirements.[75] In adopting its stricter approach, the Court seems to have been influenced by a number of factors.

---

[71] Ibid., para. 111.

[72] Ibid., para. 106. This evidence-based approach has been characterised as a necessary limitation in view of the 'ethical and social issues such profiling may entail', O. Lynskey, 'Tele2 Sverige AB and Watson et al: Continuity and Radical Change', *European Law Blog*, 12 January 2017, available at http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/).

[73] For more information, please see the discussion of Opinion 1/15 in Case Note No. 3.

[74] Opinion of Advocate General Saugmandsgaard Øe in Case C-207/16 *Ministerio Fiscal*, EU:C:2018:300.

[75] Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 *Tele 2 and* Watson, para. 116. The data must be strictly necessary for and proportionate to the objective limited to the fight against serious crime.

First, the information that may be obtained from metadata is potentially a much greater invasion of privacy now than in the past, facilitating, per the Advocate General, "the almost instantaneous cataloguing of entire populations."[76]

Second, the Court noted that not only privacy and data protection but also freedom of expression are affected. This point did not decisively influence either the Court or the Advocate General in the earlier *Digital Rights* case, but it does seem to have played an important role in the present case, reinforcing both the exclusion of general and indiscriminate surveillance and data retention and the Court's insistence on limiting both retention and access to cases of serious crime.

Third, statistics submitted to the Court by Tele2 and Mr. Watson underlined the high possibility of abusive or illegal access by the authorities.[77] In view of these risks of actual harm, both the Court and the Advocate General laid down a high standard to be observed by national legislation on data retention. The Advocate General followed the Court's earlier case law and proposed a very high standard of proportionality, balancing "the advantages associated with giving the authorities whose task it is to fight serious crime a certain ability to examine the past" with "the serious risks which, in a democratic society, arise from the power to catalogue the private lives of individuals and to catalogue a population in its entirety." The Advocate General added that even if national law respected all the mandatory requirements laid down in *Digital Rights*, it might still be disproportionate in light of the serious risks referred to.[78] In this context, the Court went further, but only to the extent of confirming that a totally broad brush approach, permitting general and indiscriminate data retention, is unacceptable.

Finally, the mutual influence of the CJEU and the ECtHR is clear. The ECtHR, which has itself developed a substantial case law on surveillance,[79] specifically referred to the CJEU case law on surveillance, in particular *Digital Rights*,[80] and in turn the CJEU specifically refers in the present case to the ECtHR rulings in *Zakharov* and *Szabó*, albeit only "by analogy" because formally "the ECHR is not a legal instrument formally incorporated into EU law" and hence only the fundamental rights enshrined in the Charter could be applied.[81] The Court was aware of, though it does not specifically refer to, the reasoning of the Grand Chamber of the ECtHR in *Zakharov*, reiterated by the Fourth Chamber in *Szabó,* that "a system of secret surveillance (…) may undermine or even destroy democracy under the cloak of defending it".[82] The ECtHR was concerned that the legislation in question might be interpreted as "paving the way for the

[76] Ibid., para. 259.
[77] Ibid., para. 260.
[78] Ibid., para. 261-262.
[79] ECtHR, *Klass and Others v Germany*, 6 September 1978, Series A no. 28; ECtHR, *Weber and Saravia* (dec.), no. 54934/00, 29 June 2006; ECtHR, *Liberty and Others v the United Kingdom*, no. 58243/00, 1 July 2008; ECtHR, *Kennedy v the United Kingdom* (no. 26839/05), 18 May 2010.
[80] ECtHR, *Szabó and Vissy v Hungary* (Application no. 37138/14), 12 January 2016, para. 15 and 23.
[81] Joined Cases C-203/15 and C-698/15 *Tele 2 and* Watson, para. 127-128.
[82] ECtHR, *Roman Zakharov v Russia* (application no. 47143/06), 4 December 2015, para. 232; ECtHR, *Szabó and Vissy v Hungary* (Application no. 37138/14), 12 January 2016, para. 57.

unlimited surveillance of a large number of citizens".[83] In consequence the ECtHR insisted in *Szabó* that a surveillance measure must be "strictly necessary (…) for the obtaining of vital intelligence in an individual operation" and that the court or independent body authorising the surveillance, as referred to in the present ruling, must "verify whether sufficient reasons for intercepting a specific individual's communications exist in each case." [84]

These dicta strongly militate against general and indiscriminate data retention, and the CJEU was fully aware of them when drafting its ruling in the present case, to the extent that it has been concluded that these judgments "demonstrate an aligning of standards between Luxembourg and Strasbourg".[85] In view of the pending cases before both Courts[86], this strong and protective mutual influence is likely to be continued.

In the meantime the ruling in *Tele2* means in effect that national rules in the Member States need to be re-evaluated in light of this decision to see whether they are compatible with EU law.[87] The national judge confronted with a case of surveillance should apply the mandatory requirements developed in *Digital Rights* and the additional criteria laid down in *Tele2* and recall, in case of doubt, the possibility of referring the question to the CJEU under Article 267 TFEU.[88] Where the national judge feels that the law clearly permits the surveillance in question, he or she should assume that the issue may well be submitted to the ECtHR and analysed in the light of the criteria developed in *Zakharov* and *Szabó*.

[83] ECtHR, *Szabó and Vissy v Hungary* (Application no. 37138/14), 12 January 2016, para. 67.
[84] Ibid., para. 73.
[85] M.D. Cole and A. Vandendriessche, 'From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance', 2 *EDPL* 1 (2016), p. 129.
[86] Pending before the CJEU: Case C-623/17 *Privacy International*. Pending before the ECtHR: ECtHR, *Centrum För Rättvisa v Sweden* (application no. 35252/08); ECtHR, *Tretter and Others v Austria* (application no. 3599/10); ECtHR, *Big Brother Watch and Others v the United Kingdom* (application no. 58170/13); ECtHR, *Bureau of Investigative Journalism and Alice Ross v the United Kingdom* (application no. 62322/14); ECtHR, *10 Human Rights Organisations and Others v the United Kingdom* (application no. 24960/15); and ECtHR, *Association confraternelle de la presse judiciaire v France et 11 autres requêtes* (applications nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15).
[87] C. Etteldorf, 'Higher Administrative Court of Northrhine Westphalia Declares German Data Retention Law Violates EU Law', 3 *EDPL* 3 (2017), p. 396.
[88] And the *obligation* under that Article for the court of last resort to submit the question to the CJEU.

Case Note No. 3:
Opinion 1/15, Canada-EU PNR

Subject of the case

In this Opinion, the CJEU lays down the criteria for the application of the fundamental rights to privacy and data protection under Articles 7 and 8 of the Charter of Fundamental rights of the European Union (the Charter) to transfers of personal data to third country authorities for the purpose of the fight against terrorism and serious transnational crime. It clarifies the appropriate legal bases for international treaties made by the EU on these matters, and it comments on the application of Articles 21 (non-discrimination) and 52(1) of the Charter (limitations on the exercise of the rights and freedoms recognised by the Charter).

4. Case info

Court/tribunal: Court of Justice of the European Union (Grand Chamber)
Date of judgement: 26 July 2017
Case number: Opinion 1/15
European Case Law Identifier: EU:C:2017:592 (CJEU) and EU:C:2016:656 (AG)

5. Case note

5.1. Background of the case [89]

The European Union has negotiated an agreement with Canada, the 'envisaged agreement',[90] which required airlines in the EU flying from to Canada to transfer to the Canadian authorities specific elements of the passenger name record (PNR) data of all their passengers on these flights. These passengers' personal data would then be processed by Canada for the purposes inter alia of border control and combating terrorism and serious international crime.

Airlines routinely collect PNR data from passengers in their automatic reservations systems when booking a flight. This booking information may include the names and addresses of passengers, their payment and credit card details, baggage and seating information, and information on special requirements for meals, which might reveal sensitive data such as health or religion.

The envisaged agreement replaces an earlier agreement of 2006 which had expired in 2009. That agreement required airlines in the EU flying to Canada to transfer on a systematic and continuous basis the PNR data of all their passengers to a Canadian authority with a view to that data being used and retained, and possibly transferred to other authorities and to other non-

[89] Opinion 1/15 Canada-EU PNR, EU:C:2017:592, para. 14-26, 128, 164.
[90] Proposal for a Council Decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, COM(2013) 529 final.

member countries, for the purpose of combating terrorism and forms of serious transnational crime.

The preamble of the envisaged agreement stresses:

> "the importance of sharing PNR data and relevant and appropriate analytical information containing PNR data obtained under this Agreement by Canada with competent police and judicial authorities of Member States of the European Union, Europol and Eurojust as a means to foster international police and judicial cooperation".

Finally the envisaged agreement provides for a data retention period of five years and lays down requirements in relation to PNR data security and integrity, immediate masking of sensitive data, rights of access to and correction and erasure of data, and for the possibility of administrative and judicial redress.

The envisaged agreement was signed in 2014 and the Council requested the European Parliament to approve the agreement to permit its conclusion. The European Parliament referred the envisaged agreement to the Court of Justice in order to ascertain whether it was compatible with EU law and, in particular, with the fundamental rights to respect for private life and the protection of personal data.

The European Parliament's request for an Opinion to the Court was worded as follows:

> "Is the [envisaged agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data] compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to the protection of personal data?
>
> Do point (d) of the second subparagraph of Article 82(1) and Article 87(2)(a)] TFEU constitute the appropriate legal basis for the act of the Council [of the European Union] concluding the envisaged agreement or must this act be based on Article 16 TFEU?"

The Court found in Opinion 1/15 that the envisaged agreement could not be concluded in its current form because it has been proposed on the wrong legal basis and several of its provisions are incompatible with fundamental rights recognised by the EU.

5.2. Issues at stake/positions defended by the parties

The issues raised before the Court may be divided into three categories.

a) Institutional law issues, including the applicability of the Charter to treaties and the legal basis for the envisaged agreement.
b) Horizontal data protection issues such as the categories of data and possible discrimination, other possible uses of that data, and independent supervision.
c) Application of the principles in Article 52(1) of the Charter, including the legal nature of the envisaged agreement and the requirements of necessity and proportionality.

a) Legal basis

The Commission proposed Articles 82(1)(d) TFEU (judicial cooperation in criminal matters in the EU) and 87(2)(a) TFEU (police cooperation among the Member States in criminal matters) as the legal bases of the envisaged agreement.

However, the European Parliament argued that the content of the envisaged agreement is mainly related to the protection of personal data. In consequence the sole appropriate legal basis of the envisaged agreement was Article 16(2) TFEU (protection of personal data), which is capable of applying across all areas of EU law, including those referred to in Title V of Part Three TFEU relating to the area of freedom, security and justice, as recognised in Declaration 21 to the Lisbon Treaty.

In contrast, Bulgaria, Estonia, France, Ireland, the United Kingdom, the Council and the Commission submitted that the principal objective of the envisaged agreement was to ensure the security and safety of the public, as could be seen in its preamble and Articles 1 and 3 of the agreement. The Commission recalled the much-criticised *EC-US PNR* ruling in 2006, where the Court found that the processing of personal data in the context of the first PNR agreement with the United States fell within a framework established by the public authorities that related to public security.[91] The protection of personal data was incidental to this objective, and merely served as a means of achieving the principal objective. In consequence they argued that Article 16 TFEU was not an appropriate legal basis.

b) Necessity and proportionality

The Parliament argued that there was no proof generally that the transfer of PNR data was necessary to ensure security, relying in particular on the doubts expressed in an Opinion of the EDPS of 30 September 2013.[92] More specifically, the Parliament submitted that the envisaged agreement affected all air passengers in a comprehensive manner, without them being in a situation specifically liable to criminal prosecutions and without any specific link between their PNR data and a threat to public security. The Parliament also noted that the envisaged agreement did not subject access to PNR data to a prior review by a court or by an independent administrative body in the framework of procedures of prevention, detection or criminal prosecutions, in order to ensure that the access to and use of such data is limited to that which is strictly necessary for the purposes of attaining the objective pursued. Finally the period of five

[91] Joined Cases C-317/04 and C-318/04 *Parliament v Council and Commission*, EU:C:2006:346, para. 55 to 59. See the discussion in H. Hijmans, 'PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators', 3 *European Data Protection Law Review* 3 (2017), p. 1, 4, and in C. Docksey, 'The European Court of Justice and the Decade of Surveillance', in H. Hijmans and H. Kranenborg (eds.), *Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)* (Intersentia 2014), p. 100-106.

[92] Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data of 30 September 2013, https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf.

years of data retention applied without any distinction to all air passengers and was not based on any objective criteria regarding the choice of such a period.

The Member States intervening and the Council and the Commission submitted that the envisaged agreement was compatible with the requirements of the Charter. They conceded that there was an interference with the fundamental rights of privacy and data protection, but argued that, unlike the *Digital Rights* ruling striking down the Data Retention Directive 2006/24/EC,[93] it was not particularly serious and PNR data do not allow very precise conclusions to be drawn concerning the private life of air passengers. They submitted that the PNR scheme is similar in nature to border checks and is subjected to strict data protection safeguards concerning limits on the use of the PNR data and to supervision by an independent authority. They also submitted that the five-year retention period laid down in Article 16 of the envisaged agreement does not go beyond what is strictly necessary in the light of its public security objective and given the average duration of complex investigations into terrorism and serious transnational crime. In this respect, France and Spain provided a number of specific examples in which the process of checking and cross-checking information has taken around five years and for which the data was or might have been of great use. As to the processing of sensitive data, the UK, the Commission and the Council noted that only one category of data would contain such information, relating to additional services requested by passengers, and that the envisaged agreement limited its use to exceptional circumstances. Finally these intervenors argued that the Court's guidance in *Schrems*,[94] relating to the application and interpretation of the Charter, was either inapplicable or would lead to a different result in the present case.

5.3. Explanation of the Court decision

a) Institutional law issues

(i) *applicability of the Charter to treaties*

This was the Court's first ruling on the compatibility of a draft international agreement with the fundamental rights enshrined in the Charter. The Court found that an international agreement must be entirely compatible with the EU Treaties and with the constitutional principles stemming therefrom.[95]

The ruling will therefore serve as a benchmark for similar bilateral agreements with third states which facilitate data transfers in name of public security, notably the PNR Agreements with Australia[96] and the United States,[97] and elements of the US Privacy Shield.[98]

---

[93] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, EU:C:2014:238.

[94] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, EU:C:2015:650, judgment of 6 October 2015.

[95] Opinion 1/15, para. 67

[96] Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ 2012 L 186, p. 4.

(ii) *Legal basis*

The Court resolved the legal basis required for an EU instrument which governs how personal data collected by private operators for commercial purposes may be further used for the purposes of security and law enforcement. It recalled that the choice of the appropriate legal basis has constitutional significance, since, having only conferred powers, the European Union must link the acts which it adopts to provisions of the Treaty which actually empower it to adopt such acts.

The Court examined for the first time the scope of Article 16(2) TFEU, introduced by the Lisbon Treaty, and its interaction with Treaty provisions on freedom, security and justice. It first recalled that in accordance with its settled case-law, the choice of the legal basis must rest on objective factors amenable to judicial review, which include the aim and the content of that measure. If a European Union act pursues a twofold purpose or comprises two components and one of these is identifiable as the main one, whereas the other is merely incidental, the act must be based on the single legal basis required by the main or predominant purpose or component. Only exceptionally, where the EU act simultaneously pursues a number of objectives or has several components which are inextricably linked without one being incidental to the other, the measure will have to be founded on the various corresponding legal bases.[99]

The Court noted that Article 1 of the envisaged agreement, entitled "Purpose of Agreement", states that "the Parties set out the conditions for the transfer and use of [PNR data] to ensure the security and safety of the public and prescribe the means by which the data is protected". It pointed out a number of preambles and clauses referring to both the objective of protecting public security and to the objective of ensuring an adequate level of data protection. These showed that the content of the envisaged agreement largely consists of detailed rules to ensure that the transfer of PNR data to Canada for the purposes of the protection of public security and safety in that non-member country and in the EU takes place under conditions consistent with the protection of personal data. It therefore found that security and data protection were two equal components of the envisaged Agreement, inextricably linked to each other, and each requiring its own legal basis.[100]

First, Article 16 TFEU is an appropriate and necessary legal basis because the envisaged agreement "(…) relates, in particular, to the establishment of a system consisting of a body of rules intended to protect personal data and with which Canada has undertaken to comply (…)."[101]

---

[97] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ 2012, L 215, p. 5.

[98] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), OJ 2016 L 207, p. 1.

[99] See Case C-263/14 *Parliament* v *Council*, EU:C:2016:435, para. 44 and the case-law cited therein

[100] Opinion 1/15, para. 90-94.

[101] Ibid., para. 89.

Second the envisaged agreement must also be based on Article 87(2)(a) TFEU (police cooperation) because it establishes rules governing the transfer of PNR data to the Canadian authority responsible for combating terrorist offences or serious transnational crime and governing the use of that data by that authority. [102]

However, the Canadian authority did not constitute a judicial authority nor do any of the provisions of the envisaged agreement refer to facilitating judicial cooperation in criminal matters, and so the Court found that it could not be based on Article 82(1)(d) TFEU (judicial cooperation in criminal matters in the EU). [103]

As a result, Articles 16(2) (the right to data protection) and 87(2)(a) TFEU (police cooperation among the Member States in criminal matters) constitute the appropriate legal bases for the act of the Council concluding the envisaged agreement.[104]

b) Compatibility of the envisaged agreement with Articles 7 and 8 of the Charter

The Court assessed the compatibility of the envisaged agreement with, in particular, the right to respect for private life and the right to the protection of personal data. With regard to the right to protection of personal data, which is enshrined in both Article 16(1) TFEU and Article 8 of the Charter, the Court referred solely to Article 8 of the Charter because Article 8(2) lays down in a more specific manner the conditions under which such data may be processed.[105]

i) *Interference with fundamental rights*

The Court observed that PNR data transferred prior to departure, together with systematic analysis by automated means before arrival in Canada, may reveal considerable information about passengers' private lives, such as a complete travel itinerary, travel habits, financial situation, dietary habits or their state of health and relationships and may even provide sensitive information about those air passengers. Furthermore, the PNR data transferred is intended to be analysed systematically by automated means, based on pre-established models and criteria, before the passengers' arrival in Canada. Such analyses may provide additional information on the private lives of passengers. These analyses are carried out without there being reasons based on individual circumstances that would permit the inference that the persons concerned may present a risk to public security. Finally, since the period during which PNR data may be retained

[102] Ibid., para. 98-101.
[103] Ibid., para. 102-103.
[104] Both the Court and the Advocate General found the procedures laid down in Article 16(2) TFEU and Article 87(2)(a) TFEU were compatible with each other and provided for the use of the same legislative procedure, and thus it was possible to rely on the dual legal basis. They also found that neither Protocol 21 TFEU with regard to Ireland and the UK, nor Protocol 22 TFEU with regard to Denmark changed this result. See ibid., para. 105-118.
[105] Ibid., para. 120.

may last for up to five years, the envisaged agreement makes it possible for information on the private lives of passengers to be available for a particularly long period of time.[106]

The Court found that this processing of personal information of identified individuals entailed an interference with the fundamental rights to respect for private life under Article 7 and data protection under Article 8 of the Charter.[107] In consequence, the Court subjected the envisaged agreement to a detailed review of compliance with the strict requirements laid down in the Charter and specifically indicated in what respects the envisaged agreement would have to be amended to ensure that it does not exceed what is strictly necessary in order to achieve its security objective.

ii) *Justification for the interferences*[108]

The Court recalled that the right to the protection of personal data requires that the high level of protection of fundamental rights and freedoms conferred by EU law continues where personal data is transferred from the European Union to a non-member country, where the data must enjoy a level of protection essentially equivalent to that guaranteed within the European Union.[109]

In this respect, the first sentence of Article 52(1) of the Charter requires that any limitation on the exercise of these rights must be 'provided for by law and respect the essence' of these rights.

Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The observance of the principle of proportionality requires, in accordance with settled case-law of the Court,[110] that derogations from and limitations to the protection of personal data should apply only in so far as is strictly necessary.

In order to satisfy that requirement, the legislation which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards to protect effectively personal data against the risk of abuse. The need for such safeguards is all the greater where sensitive data are at stake and where personal data are subject to automated processing. [111]

---

[106] Ibid., para. 121, 122, 128 and 132.
[107] Ibid., para. 124-126.
[108] Ibid., para. 133 et seq.
[109] See, by analogy, Case C-362/14 *Schrems*, para. 72 to 74.
[110] Case C-73/07 *Satakunnan Markkinapörssi and Satamedia*, judgment of 16 December 2008 EU:C:2008:727, para. 56; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others*, EU:C:2014:238, para. 51 and 52; Case C-362/14 *Schrems*, para. 92; and Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson*, EU:C:2016:970, para. 96 and 103.
[111] Opinion 1/15, para. 141.

(1) provided by law[112]

The CJEU settled the issue whether international agreements may be used to determine adequacy. The Parliament had argued that the envisaged agreement was not a "legislative act" and hence was incapable of being regarded as a "law" for the purposes of satisfying the first requirement of Article 52(1) of the Charter. However, the Court found, following the Advocate General, that such an agreement may be regarded as being the equivalent, externally, of that which is a legislative act internally. It is noteworthy, however, that the use of an international agreement to recognise adequacy is not foreseen in the exhaustively-negotiated GDPR.[113]

(2) objective of general interest[114]

The envisaged agreement was intended, inter alia, to ensure public security by means of a transfer of PNR data to Canada and the use of that data within the framework of the fight against terrorist offences and serious transnational crime. The Court confirmed that this is an objective of general interest of the European Union which is indeed capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter. The Court added that the protection of public security also contributes to the protection of the rights and freedoms of others, referring to the right not only to liberty but also to security of the person under Article 6 of the Charter.

(3) respect for the essence of the fundamental rights in question[115]

The Court noted that the information revealed was limited to air travel between Canada and the EU, thus respecting the essence of Article 7 and of the Charter, and that there were safeguards to ensure the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing, thus respecting the essence of Article 8 of the Charter.

(4) necessity and proportionality[116]

The Court assessed whether the interferences entailed by the envisaged agreement were limited to what was strictly necessary and, in that context, whether it laid down clear and precise rules governing the scope and application of the measures provided for.

(4.1.) specification of data[117]

The Court found that the envisaged agreement was not sufficiently precise as regards the nineteen headings of PNR data to be transferred. Headings five and seven use the words "etc" and "all available contact information", which were too open-ended. Most problematic was

---

[112] Ibid., para. 145-147.

[113] 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) (Text with EEA relevance), OJ 2016 L 119, p. 1.

[114] Opinion 1/15, para. 148-149 and 152-153.

[115] Ibid., para. 150.

[116] Ibid., para. 140-141 and 154 *et seq*.

[117] Ibid., para. 164-167.

heading seventeen, which heading refers to "general remarks" and constituted an entirely open "free text" heading, as shown by the use of the term "including", which could even encompass information entirely unrelated to the purpose of the transfer of PNR data.

(4.2.) sensitive data[118]

The Court found that the parties had agreed that sensitive data could be processed under the envisaged agreement on the basis that Articles 8 and 16 thereof dealt with the processing of sensitive data and that it was defined under Article 2(e) thereof as any information that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership", or concerning "a person's health or sex life".[119]

In contrast the EU PNR Directive (EU) 2016/681[120] specifically prohibits the processing of sensitive data, and many of the categories of sensitive data are included in the prohibition of discrimination under Article 21 of the Charter.

In view of Articles 7 and 8 of the Charter, read in the light of Article 21 thereof, the Court concluded that there would have to be a precise and particularly solid justification for such processing, based on grounds other than the protection of public security against terrorism and serious transnational crime. Since no such specific justification existed the Court found that the provisions of the Charter precluded the processing of sensitive data under the envisaged agreement.

(4.3.) automated processing[121]

The Court pointed out that there was a significant margin of error built into the automated analyses of PNR data before the arrival of air passengers in Canada, due to the use of pre-established models and criteria and of unverified personal data provided by airlines. In order to be acceptable, the Court required such processing to be non-discriminatory, reliable and up to date, making it possible to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime. In addition the results should be subject to an individual re-examination by non-automated means before an individual measure adversely affecting an air passenger concerned were adopted.

(4.4.) purposes

The Court found that the envisaged agreement had sufficiently defined the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime. Both the terms "terrorist offences" and "serious transnational crime" were defined in a

---

[118] Ibid., para. 145-147.

[119] These are the same criteria as Article 8 of Directive 95/46, to which the definition in Article 9 of the GDPR adds genetic and biometric data and sexual orientation.

[120] 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, OJ 2016 L 119, p. 132.

[121] Opinion 1/15, para. 168-174.

clear and precise manner.[122] However, the envisaged agreement also authorised Canada to process PNR data "on a case-by-case basis" in order to "ensure the oversight or accountability of the public administration" and to "comply with the subpoena or warrant issued, or an order made, by a court", respectively. The Court found that these other purposes were too vague and general to meet the requirements as to clarity and precision and were not therefore limited to what is strictly necessary to attain the objective pursued by that agreement.[123]

(4.5.) transfer, storage and use of PNR data

The Court's analysis of the transfer, storage and use of PNR data may be divided into three distinct time frames:

i) processing of PNR data of all passengers before and upon entry to Canada[124]

The transfer and storage of PNR data of all passengers for the purpose of entering Canada was judged not to exceed the limits of necessity. Although this affected all passengers entering Canada generally and without exception, the automated processing of PNR data before the arrival of the passengers in Canada would facilitate and expedite security checks, in particular at borders, in order to identify persons liable to present a risk to public security from amongst all air passengers. The Court noted in this respect that the Chicago Convention[125] requires all air passengers to comply with the laws as to admission to and departure from the territory of the country to where they fly, and the identification, by means of PNR data, of passengers liable to present a risk to public security forms part of border control, to which air passengers are subject if they wish to enter and spend time in Canada. This extends the approach of the Court in the earlier *Tele2* ruling, discussed in Case Note No. 2, that the scope of the surveillance cannot be "general and indiscriminate" and must be limited to what is shown to be necessary and proportionate.[126]

In the present case the processing of flight data was limited to a specific albeit large group of air travelers to Canada, not the whole population, and that data was necessary for border control purposes recognized by international treaty. Moreover personal information was limited to the flight data collected by the airline on which passengers were travelling, and there was no obligation to collect all the possible data fields, simply an obligation to transfer the flight data that was collected in practice by each airline to the Canadian authorities. In addition, there was no interference *per se* with protected categories of information, e.g. relating to legal

[122] Ibid., para. 175-178.
[123] Ibid., para. 179-181.
[124] Ibid., para. 186-189.
[125] Convention on International Civil Aviation, signed at Chicago on 7 December 1944 (United Nations Treaty Series, Volume 15, No 102).
[126] The Court held in that case that surveillance may extend to a geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, see Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson*, para. 106. Kuner feels that the Court has "pulled back" from this approach in the present case, see C. Kuner, 'International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR', 55 *Common Market Law Review* 3 (2018), p. 857, 871-872.

professional privilege or judicial secrecy, as in the earlier case of *Tele2* where general and indiscriminate retention of all electronic communications was required.

ii) processing of PNR data of all passengers during their stay in Canada[127]

The Court specified that PNR data could only be *stored* under the envisaged agreement for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime. The *use* of any of this data during or after their stay in Canada was not strictly necessary for these purposes. Any further processing of these data would require a specific justification, for example where there is objective evidence from which it may be inferred that the PNR data of one or more air passengers might make an effective contribution to combating terrorist offences and serious transnational crime. And it would require the development of specific rules on the conditions of use and access, in particular providing that the use of these data should be normally only permitted after prior review by a court or an independent authority.

iii) processing of PNR data of certain passengers after leaving Canada[128]

The Court considered that retention of PNR data after air passengers leave Canada was not strictly necessary, as these persons have already been checked on entry and departure and they should not be regarded as presenting a risk as regards terrorism or serious transnational crime. In consequence the further retention and use of PNR data would only be considered acceptable in those cases where a traveller presented a specific risk based on objective evidence relating to the fight against terrorism or serious transnational crime. Once again, the use of PNR data should be normally only permitted after prior review by a court or an independent authority. Subject to these conditions, the Court found that the retention period of five years from the date of receiving the PNR DATA did not exceed the limits of what is strictly necessary.

(4.6.) disclosure of PNR data to authorities in third states[129]

The envisaged agreement provided that the Canadian authorities could assess the level of protection guaranteed in third countries when deciding whether to disclose PNR data to the government authorities of those countries. However the Court recalled that a transfer of personal data from the EU to a third country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. As a result the Canadian authorities should only be able to transfer PNR data to authorities in other third countries where the EU itself had established that there was an essentially equivalent level of protection, either in an agreement with the third country concerned or following a decision by the Commission finding that the third country ensures an adequate level of protection.

(iii) Information to data subjects[130]

[127] Opinion 1/15, para. 197-203.
[128] Ibid., para. 204-209.
[129] Ibid., para. 212-214.

The envisaged agreement did not require air passengers to be notified of the transfer of their PNR data to Canada and of its use, in particular whether their data have been used by the Canadian authorities for more than the entry checks. That information is necessary to enable travellers to exercise their rights to request access to PNR data concerning them, to rectification of that data, if appropriate, and to an effective remedy before a tribunal. Consequently, in situations where there is objective evidence justifying use of the PNR data for specific investigations which requires the prior authorisation of a judicial authority or an independent administrative body, and where PNR data is disclosed to other government authorities or to individuals, it is necessary to notify air passengers individually. This may be delayed during the investigations, but the information should be provided once it is no longer liable to jeopardise those investigations.

(iv) Independent supervision - the oversight of PNR data protection safeguards[131]

Under Article 8(3) of the Charter, compliance with the data protection rules is subject to control by an independent authority. Under the settled case law of the Court this independent supervision is an essential element of the right to protection of personal data.[132] The envisaged agreement provided for oversight in part by an independent supervisory authority, the Privacy Commissioner of Canada. However, an "impartial" administrative authority with a "proven record of autonomy" was responsible for oversight of the cases of non-resident foreigners, not the Privacy Commissioner of Canada. The Court did not accept that this second form of supervision was adequate to ensure the strict standard of independent supervision required under Article 8(3) of the Charter.

6. Main implications

This ruling is the latest in a series of four rulings by the CJEU, following the rulings in *Digital Rights, Schrems* and *Tele2* (see JUD-IT Case Note No. 2), that address the increasing resort by national authorities to the mass processing of personal data. In this line of cases the Court can be seen as developing and imposing a balance between the interests of the State with the fundamental rights of those whose privacy and personal information are affected by such processing. The ruling marks a further consolidation of the work of the CJEU in establishing the Charter as a constitutional benchmark and the role of the Court in prioritising the protection of fundamental rights, in particular the rights to privacy and data protection.[133] In the present case the Court has applied the principle of necessity to a treaty and explained its consequences in detail.

There are a number of significant implications for national judges.

---

[130] Ibid., para. 218-225.
[131] Ibid., para. 228-231.
[132] Case C-518/07 *Commission v Germany*, EU:C:2010:125, para. 25; Case C-288/12 *Commission* v *Hungary*, EU:C:2014:237, para. 48; and Case C-362/14 *Schrems*, para. 41
[133] V. Skouris, 'After 12 Years…', 23 *Maastricht Journal of European and Comparative Law* 2 (2016), p. 219, 220.

First, data processing authorised by a treaty must be scrutinised as closely as data processing authorised by EU or national legislation in view of its compatibility with the fundamental rights enshrined in the Charter. The ruling will therefore serve as a benchmark for similar bilateral agreements with third states which provide for data transfers in the name of public security and law enforcement, notably the PNR Agreements with Australia and the United States, and elements of the US Privacy Shield.

Second, the standards for judicial scrutiny laid down in Article 52(1) of the Charter must be applied. The detailed prescriptions by the Court provide in effect a case manual for the analysis to be applied, first by the Council and Commission in negotiating agreements, and then by the CJEU and by national judges in cases before them.[134] In particular, the CJEU has confirmed and consolidated its recent case law on mass surveillance,[135] which it has developed in parallel with that of the ECtHR.[136]

The present ruling establishes that a treaty satisfies the first requirement in the first sentence of Article 52(1) of there being a 'law.' However, the national judge should assess whether the provisions of the treaty satisfy the other requirements of Article 52(1) first sentence of the Charter, namely the existence of an objective of general interest and respect for the essence of the rights concerned. If these requirements have been respected the national judge should assess whether the requirements of necessity and proportionality in the second sentence of Article 52(1) have been satisfied.

In this respect, the national judge should check whether these standards have been respected with regard to the fundamental rights to privacy (Article 7 of the Charter) and data protection (Article 8 of the Charter), as well as other fundamental rights such as non-discrimination (Article 21 of the Charter) and effective judicial remedy (Article 47 of the Charter).

Most importantly, in case of doubt, the CJEU should be consulted under the preliminary ruling procedure enshrined in Article 267 TFEU.

---

[134] See, *contra*, Kuner argues that the Court has in effect performed a 'redline revision' of the envisaged agreement which poses difficulties for negotiators in the future in terms of not knowing whether specific clauses in an agreement will pass the test of compatibility . See C. Kuner, 'Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15', *VerfBlog* (2017), http://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/) and that the detail of the prescriptions "makes a poor fit with the give-and-take of international negotiations" (see C. Kuner, 55 *CML Rev.* 3 (2018), p. 874).

[135] For a review of the case law, see EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 11 April 2017.

[136] ECtHR, *Roman Zakharov v Russia*, Judgment of 4 December 2015, Application no. 47143/06; ECtHR, *Szabó and Vissy v Hungary*, Judgment of 12 January 2016, Application no. 37138/14.