Data Retention in the European Union

Legal analysis of telecommunication data retention

Felix Mikolasch

Bachelor Thesis 2018/2019

Bachelor in Law

Faculty of Law - Universitat Autònoma de Barcelona

Directed by Antoni Roig Batalla

10th May 2019

Abstract

Data retention is a relatively new phenomena. Due to the impact of 9/11 data retention became an important tool, according to governments, against terrorists and other criminals. Telecommunication service providers are obliged to retain non content data about the communications of its clients for a certain period of time. Law enforcement authorities may access this data after complying with certain requirements. However, data retention strongly interferes with fundamental rights, mainly the respect for private and family life and protection of personal data. The Court of Justice of the European Union (CJEU) has declared that existing data retention schemes are contrary to EU law. This analysis tries to clarify how data retention could be carried out in accordance with fundamental rights. It assesses the relevant case law from the CJEU, the applicable legal framework and data retention systems of other jurisdictions in order to determine parameters which are important for the future development of this investigation tool.

Keywords:
Data retention - European Union regulation - Data preservation - Quick freeze - Data protection
Palabras clave:
Retención de datos - Regulación en la Unión Europea - Preservación de datos - Quick freeze - Protección de datos
Stichworte:
Vorratsdatenspeicherung - Regulierung in der Europäischen Union - Anlassdatenspeicherung - Quick freeze - Datenschutz

Contents

Introduction

0.1 From Beccaria to Data Retention

> «Falsa idea di utilità è quella che sacrifica mille vantaggi reali per un inconveniente o immaginario o di poca conseguenza, che toglierebbe agli uomini il fuoco perché incendia e l'acqua perché annega, che non ripara ai mali che col distruggere.»
>
> Cesare Beccaria, *Dei delitti e delle pene* (1764)

In the 18th century, Cesare Beccaria, in his most famous work *Dei delitti e delle pene*, stated how a modern, rational criminal law would look like. Everyone should be guaranteed a due process of law, punishments ought to be proportionate and everyone should be treated innocent until proven guilty.

Sure enough Beccarias work had great influence on criminal law in continental Europe and beyond. Nowadays, a great number of jurists defend a humanistic point of view when it comes to criminal law: Offenders should be reintegrated into society and should spend their prison time preparing for it. Also, laws ought to be proportional and not draconian, as everyone could face a criminal trial. However, apart from legal scholars, lawyers, judges and other jurists, these ideas from the age of Enlightenment were not received in the same way.

All kind of media, for example, preaches ideas directly opposed to the values Beccaria established. Frequently, we read headlines suggesting that a robber, a thief, a murderer and others should face heavier jail sentences, ought to be locked up for the maximum time possible, some even calling for the reintroduction of the death penalty. Politicians, too, praise this mantra as it seems to be a promising strategy to gain votes in the next elections and to establish themselves as someone who guarantees security.

Theses considerations are essential for understanding how anti-terror legislation unfolded after 9/11. When, back in September 2001, the twin towers fell, a new era of military and security policies began. The United States legislators approved of the *Patriot Act* and the United States Government went as far as installing camps like Guantánamo where, according to some reports, torture was commonplace. The *War on Terror* had begun.

The Madrid Bombings of 2004 and the London Bombings of 2005 were to reassure European countries that they are facing international terrorism, too. Under these impressions, in 2006 the European Union adopted the *Data Retention Directive*, an instrument which had to be transposed into the national legislation of every Member State of the European Union.

Its objective was to prevent and to help investigating serious crimes, such as terrorism. To achieve this goal, the text set out that the operators of telecommunication services[1] had to retain the traffic data for a certain period of time. Traffic data generally means all data except for the content of the communication. For example, the data retained from a cellphone call would be the duration of the connection, which phones (identified by a unique serial number called IMEI) are communicating, the cellphone numbers, its owners and the location of the two phones. The content of the conversation would not be recorded.

Data retention also applied to other services such as internet access or SMS, and in general to every type of telecommunication service. Law enforcement authorities could then request access to the withheld data. Various Constitutional or Supreme Courts of European States declared that their national legislation, implementing the Data Retention Directive, fell short of respecting fundamental rights.

In 2014, the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland* declared that the Data Retention Directive from 2006 did not comply with other European Union law and was in breach of the Charter of Fundamental Rights of the European Union. The Directive was declared invalid. Two years later, in 2016, the Court of Justice also found that the *national* legislation, regarding data retention in Sweden and England, were not respecting the provisions of European Union (EU) law, referring once again to fundamental rights as a justification.

The judges followed the argument that data retention as foreseen in the Data Retention Directive of 2006 is a method were every single person using telecommunications services is placed under constant surveillance. This approach was rejected as it does not conform to fundamental rights. However, the Court of Justice of the European Union left the door open for data retention if it complies with the requirements set out in its decisions.

Usual arguments against data retention are that placing everyone under sur-

[1]This text uses *telecommunication service providers* and *communication service providers* indistinctly.

veillance is interfering with the rights to intimacy, privacy, data protection and consequently the unhindered development of human personality. It would also have a chilling effect on freedom of speech. Finally, it could harm democratic institutions, as a result of limiting or interfering with fundamental rights, such as freedom of speech.

Arguments brought forward for data retention are usually more utilitarian: This is to say that these arguments are focussing on specific goals and that data retention is a mean to achieve these goals. The end justifies the means, one may say. From this perspective data retention is necessary for the fight against serious crime, for example, terrorism, child pornography or narcotrafficking. This would legitimate data retention, as society is striving for security and is not tolerating these offences.

This brings us back to Cesare Beccaria. When he, back in his days, stated that laws should not be draconian, but should be proportionate and tried to convince his fellows that living in liberty is the best condition for human beings, he most surely, I may argue, would have been astonished on how we treat our liberties today. Hence, the aim of this thesis is to clarify how data retention could be carried out in accordance with fundamental rights.

0.2 Research questions

In this thesis we will address telecommunication data retention, focussing mainly on its public aspect and regulation in the European Union. Telecommunication data retention for private purposes will also be mentioned, although only briefly.

1. How is data retention and access to retained data shaped and conditioned by the jurisprudence of the Court of Justice of the European Union?

2. Beyond the jurisprudence of the Court of Justice of the European Union and the applicable legal framework: which options and models for data retention and access are plausible?

3. Have any of the suggested options for question two or any alternative system proved anywhere to fulfil the principle of proportionality and to respect fundamental rights?

0.3 Structure

The first chapter will be dedicated to data retention[2] and access by authorities to this data from a negative perspective. We will discuss the now invalidated Data Retention Directive and what data was retained, for how long, as well as some applicable guarantees. Furthermore, we will review the *Digital Rights Ireland*, the *Tele2* and the *Ministerio Fiscal* judgements from the Court of Justice of the European Union and the following limitations for national and European Union legislation. This implies exploring the underlying discussion between surveillance and fundamental rights.

In the second chapter we will focus on data retention and access by authorities from a positive perspective. This is to say that the second chapter outlines how future data retention could be realised, taking into account all the necessary limitations set out in the decisions of the Court of Justice of the European Union as explained in the first chapter. Also, we will refer to the principles of the European Union General Data Protection Regulation. Further, we will discuss the notion of the «quick freeze» system, which has been discussed as an alternative to the classical approach of data retention.

In the third chapter we take a look at some specific jurisdictions: the United States, Australia, Austria and Canada. We will compare the systems of data retention operating in these states, focussing on the legal framework in each jurisdiction, its principles and possible criticism. The purpose of this analysis is to assess the systems by the standards found to be relevant in the foregoing chapter in order to identify practical problems, alternatives and undesirable attributes of data retention schemes.

Finally, we will conclude answering the research questions, trying to summarize how data retention would ideally work in view of the test of proportionality. We will also state some questions that remain unanswered and need further analysis in the future.

[2]The term *data retention* is used in a broad sense in this text. It does also cover *data preservation*.

Chapter 1

The Limits of Data Retention

1.1 The Data Retention Directive

1.1.1 Origin

As outlined in the introduction (see *supra* 0.1) the European Union Data Retention Directive[1] was adopted as a part of new security policies against international terrorism, due to the impact of the terrorist attacks suffered in New York, London and Madrid.[2] As stated in the recitals of the directive, the use of electronic communication was growing significantly, making it, therefore, necessary to gain access to data related to electronic communications for «[...]the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime»,[3] especially citing the fight against terrorism.[4]

1.1.2 Content and Traffic Data

The Data Retention Directive's core provision was the obligation of «providers of publicly available electronic communications services or of a public communications network»[5] to retain traffic data for a period between six months and two years.[6] This traffic data of telephone and internet connections consists of data necessary to identify the source, the destination, date, time, duration and type of a communication, as well as the users' equipment and the users location.[7] Content data, however,

[1]Directive 2006/24/EC of the European Parliament and of the Council. Available at: `https://data.europa.eu/eli/dir/2006/24/oj`, visited on 1st February 2019.

[2]Møller Pedersen, Anja, Udsen, Henrik and Sandfeld Jakobsen, Søren (2018). "Data retention in Europe—the Tele 2 case and beyond". In: *International Data Privacy Law* 8 (2). Available at: `http://dx.doi.org/10.1093/idpl/ipx026`, visited on 27th November 2018, p. 160.

[3]Directive 2006/24/EC of the European Parliament and of the Council, recital 7.

[4]Ibid., recitals 8-10.

[5]Ibid., article 3.

[6]Ibid., article 6.

[7]Ibid., article 5(1).

should not be retained.[8] The scope of application of this provisions is broad: the directive applies to data of both natural and legal persons,[9] «[...]without distinguishing between criminal suspects and ordinary citizens»[10] and extends data retention to all communication service providers in the European Union.[11] However, the data gained through this retention may only be used «[...]for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.»[12]

1.1.3 Retention and Access

The Data Retention Directive distinguished the logging of traffic data, known as retention, and the access by authorities to this logged data. The Directive imposed the obligation to retain traffic data: this should be regulated in a similar way in the whole European Union.[13] Access by authorities to the retained data, however, needed to be regulated by each Member State.[14]

The Court of Justice of the European Union also applies this difference and treats retention and access as two different subjects (see *infra* 1.2).

1.1.4 Controversies

The Data Retention Directive has been described as a directive which «[...]met with significant controversy[...]»[15] from the beginning of its existence.[16] Unsurprisingly,

[8] Ibid., article 5(2).

[9] Ibid., article 1(2).

[10] Vedaschi, Arianna and Lubello, Valerio (2015). "Data Retention and its Implications for the Fundamental Right to Privacy". In: *Tilburg Law Review* 20(1). Available at: `http://booksandjournals.brillonline.com/content/journals/10.1163/22112596-02001005`, visited on 27th November 2018, p. 20.

[11] Ibid., p. 19.

[12] Directive 2006/24/EC of the European Parliament and of the Council, article 1(1).

[13] Ibid., article 3(1).

[14] Ibid., article 4.

[15] Fennelly, David (2018). "Data retention: the life, death and afterlife of a directive". In: *ERA Forum*. ISSN: 1863-9038. Available at: `https://doi.org/10.1007/s12027-018-0516-5`, visited on 27th November 2018, p. 2.

[16] González Pascual, Maribel (2014). "El TJUE como garante de los Derechos en la UE a la luz de la sentencia Digital Rights Ireland". In: *Revista de Derecho Comunitario Europeo* 49. ISSN: 1138-4026. Available at: `http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=1336&IDA=37257`, visited on 27th March 2019, p. 944.

it faced different legal challenges: Ireland brought proceedings before the CJEU considering that the legal basis for the adoption of the Directive was inappropriate; according to Fabbrini, the Irish challenge was not concerned with the interference of data retention with fundamental rights, but rather with the unwillingness to raise the standards of its own system of data retention.[17] The CJEU rejected this claim,[18] stating that the legal basis —adopting the directive «as an internal market measure»[19]— was indeed the correct one.[20] Also, in several Member States of the European Union the national implementation of the Directive was challenged before the courts: some examples are Bulgaria, Cyprus, Romania, Germany and the Czech Republic. The Constitutional Court of Romania, for example, declared that the national data retention legislation fell short of protecting the *right to respect for private and family life,*[21] whereas the German *Bundesverfassungsgericht* (Federal Constitutional Court) referred to its own constitution and the secrecy of correspondence in its judgement. In general, these judgements partly anticipate the decision of the CJEU.[22]

Finally, an Irish and an Austrian case made their way to the CJEU, each one through a reference for a preliminary ruling, essentially asking about the validity of the Data Retention Directive in view of the Charter of Fundamental Rights of the European Union. The CJEU delivered its decision on 8th April 2014 in what is known as the *Digital Rights Ireland* case.[23] It declares the Data Retention Directive invalid.

[17]Fabbrini, Federico (2015a). "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States". In: *Harvard Human Rights Journal* 28. Available at: `https://harvardhrj.com/wp-content/uploads/sites/14/2009/09/human-rights-in-the-digital-age.pdf`, visited on 10th May 2019, pp. 75-76.

[18]Judgement of the Court (Grand Chamber) of 10 February 2009, *Ireland v European Parliament and Council of the EU*, C-301/06. ECLI:EU:C:2009:68.

[19]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 6.

[20]Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States", pp. 75-76.

[21]European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms). Available at: `https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765`, visited on 1st February 2019, article 8.

[22]For more details about the national judgements: Vedaschi and Lubello, "Data Retention and its Implications for the Fundamental Right to Privacy", pp. 22-26.

[23]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12. ECLI:EU:C:2014:238.

1.2 CJEU Jurisprudence

1.2.1 Digital Rights Ireland

The questions referred to the CJEU originated in the Irish High Court and the Austrian *Verfassungsgerichtshof* (Constitutional Court).[24] In Ireland *Digital Rights Ireland Ltd* claimed that the national legislation and the Data Retention Directive were not legal.[25] In Austria the *Kärntner Landesregierung* (the Government of the State of Carinthia) and 11130 other applicants challenged the legislative changes stemming from the transposition of the Directive as interfering with their right to data protection.[26] The CJEU joined both cases[27] and deduced that «[...]the referring courts are essentially asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter.»[28]

At the beginning of its reasoning the Court already makes an decisive move when it states that traffic data may allow for very specific deductions:

> *«Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, 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.»*[29]

Fabbrini argues that through this decision «[...]the ECJ showed awareness of the pervasive effect of a metadata collection program[...]»,[30] citing an National Security Agency (NSA) responsible who praises the utility of traffic data.

The obligation for retention introduced by the Data Retention Directive amends

[24]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 8.

[25]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 17.

[26]Ibid., para. 19.

[27]Ibid., para. 22.

[28]Ibid., para. 23.

[29]Ibid., para. 27.

[30]Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States", p. 86.

the data protection regime foreseen in the Data Protection Directive[31] from 1995 —as of May 2018 repealed by the General Data Protection Regulation (GDPR)[32]— and the Privacy and Electronic Communications Directive[33] from 2002, «[...]directives which provided for the confidentiality of communications and of traffic data[...].»[34]

Moreover, the Court considers, according to its case law: «To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way[...].»[35]

The CJEU then determined, in light of the foregoing consideration, that the Directive constitutes an interference with the right to respect for private and family life and the right to protection of personal data, as enshrined by article 7 and 8 of the Charter[36,37] because «[...]data relating to a person's private life and to his communications[...]»[38] is retained and access may be granted to authorities.[39,40] It may also affect the right to freedom of expression, having a *chilling effect*, even though data retention does not affect content data.[41,42]

The Court subsequently proceeds to examine the interference of the rights guaranteed by the Charter according to the test of proportionality. In general, the

[31]Directive 95/46/EC of the European Parliament and of the Council. Available at: `https://data.europa.eu/eli/dir/1995/46/oj`, visited on 1st February 2019.

[32]Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: `https://data.europa.eu/eli/reg/2016/679/oj`, visited on 1st February 2019.

[33]Directive 2002/58/EC of the European Parliament and of the Council. Available at: `https://data.europa.eu/eli/dir/2002/58/oj`, visited on 1st February 2019.

[34]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 32.

[35]Ibid., para. 33.

[36]Charter of Fundamental Rights of the European Union. Available at: `https://data.europa.eu/eli/treaty/char_2012/oj`, visited on 1st February 2019.

[37]Vedaschi and Lubello, "Data Retention and its Implications for the Fundamental Right to Privacy", p. 28.

[38]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 34.

[39]Ibid., paras. 34-36.

[40]Guild, Elspeth and Carrera, Sergio (2014). "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive". In: *CEPS Liberty and Security in Europe Papers* 65. Available at: `https://ssrn.com/abstract=2445901`, visited on 26th April 2019, pp. 5-6.

[41]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 28.

[42]Guild and Carrera, "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", p. 6.

interference of the Data Retention Directive is considered to be «wide-ranging», «particularly serious» and may cause the feeling of «constant surveillance»,[43] as well as entailing «[...]an interference with the fundamental rights of practically the entire European population»,[44] «[...] without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.»[45] The decision rightly states that public security is of «utmost importance», but that it does not, therefore, justify any tool or measure to defend it:[46,47] the limitation of the rights concerned is only admissible if «strictly necessary».[48] As data retention affects everyone using electronic communications systems, without any exceptions, there is no direct link to be found «[...]between the data whose retention is provided for and a threat to public security[...]».[49,50]

Also, as the CJEU states, there is no sufficient regulation regarding the access by authorities to the retained data. The decision particularly claims that there is no «objective criterion» for access, that the Directive does not require judicial review for access, nor does it provide any «substantive or procedural conditions» for access by authorities.[51]

The Court finds that there is no sufficient regulation on the interference caused by retention and that the interference is not limited to what is strictly necessary.[52] Therefore, the Directive does not respect the principle of proportionality.[53]

Digital Rights Ireland puts an end to the European Union Data Retention Directive declaring it invalid. Moreover, it implies that the Directive legally never existed, as the effects of the judgement are *ex tunc*.[54] However, Directives are subject to a

[43]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 37.

[44]Ibid., para. 56.

[45]Ibid., para. 57.

[46]Ibid., para. 51.

[47]Guild and Carrera, "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", p. 7.

[48]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 52.

[49]Ibid., para. 59.

[50]See also: Vedaschi and Lubello, "Data Retention and its Implications for the Fundamental Right to Privacy", p. 29.

[51]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, paras. 60-62.

[52]Ibid., para. 65.

[53]Ibid., para. 69.

[54]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 11.

national transposition; the resulting national regulation will not be directly affected by the invalidity of a Directive, as according to CJEU case law each Member State has to decide about the implications of a Directive's invalidity in its legal system on its own. This, precisely, is the reason why data retention schemes have been declared invalid in some Member States. Others modified or revised their data retention schemes and in some cases data retention continued as before.[55]

1.2.2 Tele2

In the aftermath of the *Digital Rights Ireland* decision a Swedish electronic communication provider called Tele2 stopped its data retention. It understood that the national Swedish legislation did not comply with the standards set by the CJEU.[56]

Also, in the United Kingdom the legality of the *Data Retention and Investigatory Powers Act 2014* (DRIPA), that had been enacted after the *Digital Rights Ireland* judgement,[57] was called into question: Mr. Watson and others raised concerns that DRIPA might not be compatible with the Charter, nor with the European Convention on Human Rights (ECHR).[58]

What makes *Tele2* different from the foregoing decision in *Digital Rights Ireland* is the fact that what is called into question is not a European Union Directive, but national legislation of its Member States.[59]

The CJEU mainly focuses on the question whether article 15 of the Privacy and Electronic Communications Directive,[60] taking into account articles 7, 8 and 52(1) of the Charter,[61] «[...]must be interpreted as precluding national legislation [...] for general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications.»[62]

[55]Ibid., pp. 11-12.

[56]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15. ECLI:EU:C:2016:970, para. 44.

[57]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 12.

[58]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 52.

[59]Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 161.

[60]Directive 2002/58/EC of the European Parliament and of the Council.

[61]Charter of Fundamental Rights of the European Union.

[62]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 62.

Electronic communication, including traffic data, should, as a general principle, be confidential as outlined by article 5(1) of the Privacy and Electronic Communications Directive.[63,64] 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.»[65] However, article 15(1) of the same Directive is an important exception to the principle of confidentiality as it permits retention or interception of content or traffic data.[66]

The exception provided for by article 15(1) «must be interpreted strictly» according to CJEU case law. Moreover, the general rule foreseen in article 5 may not be replaced or rendered void by the exception.[67] As the second and the third sentence of article 15(1) provide, national regulation may only be enacted for the objectives set out in the first sentence and must respect the principles of European Union Law, including the Charter.[68,69] Recalling article 52(1) of the Charter, limitations to the rights guaranteed «[...]must be provided for by law and must respect the essence of those rights and freedoms.»[70] Any restrictions on the protection of personal data in combination with the right to respect for private life are only permitted if they are strictly necessary, at least at EU level and according to the case law of the CJEU.[71]

[63]Directive 2002/58/EC of the European Parliament and of the Council, art. 5(1).

[64]Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 164.

[65]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 85.

[66]«Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when 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 or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union», see: Directive 2002/58/EC of the European Parliament and of the Council, art. 15(1).

[67]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 89.

[68]Ibid., paras. 90-91.

[69]Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 164.

[70]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 94.

[71]Ibid., para. 96.

The Swedish legislation provided for a «general and indiscriminate» data retention scheme which retained all traffic data without any exceptions.[72,73] This is indeed a very similar data retention scheme to the one provided in the invalidated Data Rention Directive of 2006.[74] Following the argumentation of the Advocate General the Court affirms that this data is as sensitive as the actual content.[75,76]

As in *Digital Rights Ireland* the CJEU states that the interference is «far-reaching» and «particularly serious» and that the affected population might feel «constant surveillance». Furthermore, there might be a *chilling effect* on the right of freedom of expression.[77] Only the fight against «serious crime» might justify measures of serious interference with fundamental rights;[78] these measures of general interest, however, «[...]cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.»[79] The data retention established by the Swedish legislation is the rule and not the exception because everyone using electronic communication services is affected by this data retention scheme, even without having any relation with ongoing criminal investigations.[80,81]

Therefore, the CJEU concludes: «National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.»[82]

However, the CJEU does not reject the idea of data retention in general: A

[72]Ibid., paras. 97-98.

[73]Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 164.

[74]Directive 2006/24/EC of the European Parliament and of the Council.

[75]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 99.

[76]Even though traffic data is as sensitive as content data, the Court, surprisingly, finds in paragraph 101 that only content data could affect the essence of the rights concerned.

[77]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, paras. 100-101.

[78]Ibid., para. 102.

[79]Ibid., para. 103.

[80]Ibid., paras. 104-106.

[81]Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 165.

[82]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 107.

Member State might enact legislation with «[...]targeted retention of traffic and location data, 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.»[83, 84]

The Court then proceeds to examine a second point, if «[...]the access of the competent national authorities to retained data, where that legislation does not restrict that access solely to the objective of fighting serious crime, where that 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»[85] is compatible with the Charter.

Access to the data that has been retained may only be granted if it is «genuinely and strictly» related to one of the items listed in article 15(1)[86] and this access is only possible, in regard of the field of prosecution of criminal offences, for the «objective of fighting serious crime» due to its serious interference with fundamental rights.[87, 88] It follows, that access —implying a serious interference with fundamental rights— is not permissible for fighting crimes that are not serious. The access to such data shall be reduced to what is «strictly necessary».[89] Also, access must be granted by judicial or independent administrative authorities and data must be stored in the EU, in order to protect the enforceability of jurisdiction.[90, 91]

The CJEU therefore establishes that the Charter precludes «[...]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

[83]Ibid., para. 108.

[84]See also: Fennelly, "Data retention: the life, death and afterlife of a directive", p. 14.

[85]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 114.

[86]«[...]safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system [...]»

[87]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 115.

[88]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 14.

[89]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 115.

[90]Ibid., paras. 120 and 122.

[91]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 15.

administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.»[92]

1.2.3 CJEU Competence

What remains questionable in both decisions *Digital Rights Ireland* and *Tele2* is the scope of application of the Directives, EU law and the competence of the CJEU.

As Fennelly points out in his excellent article,[93] the CJEU in *Digital Rights Ireland* concludes that: «The material objective of that directive is [...] to contribute to the fight against serious crime and [...] to public security.»[94] This is surprising because the Court had confirmed the legal basis of the Data Retention Directive to be an internal market measure, as already stated above (see *supra* 1.1.4).[95]

Moreover, the Court deals with both retention and access in its judgement, even though access is deliberately excluded from the Directive: It is for the Member States to regulate the access conditions to retained data.[96] This exclusion is in line with the principle of conferral, stating that any competence that is not conferred to the EU remains a competence of the Member States. Indeed, national security, which might comprehend access to retained data for the investigation of crimes, is explicitly excluded from EU competences.[97]

On one hand, the courts decision might look like a logical conclusion, because retention and access go hand in hand («no access without retention») and because the legislator should not impose interferences with fundamental rights and leave the formulation of guarantees almost exclusively to the Member States.[98] On the other hand, these considerations are weakening the principle of conferral.[99]

The same is true for the *Tele2* decision. It actually does not only refer to the fact that EU law precludes *national* data retention legislation, it also dictates how

[92]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 124.

[93]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 9.

[94]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 41.

[95]Judgement of the Court (Grand Chamber) of 10 February 2009, *Ireland v European Parliament and Council of the EU*, C-301/06.

[96]Directive 2006/24/EC of the European Parliament and of the Council, art. 4.

[97]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 16.

[98]Ibid., p. 8.

[99]Ibid., pp. 16-19.

national data access should be regulated. It might be argued that its interpretation of article 15(1) does extend the scope of the directive further than what is foreseen in article 1(3) of the same Directive.[100]

1.2.4 Ministerio Fiscal

Ministerio Fiscal is a relatively recent decision from the CJEU delivered in October 2018.[101] It is mainly concerned with access to retained data and not with data retention itself. Its findings might be of importance for future jurisprudence on data retention of the CJEU and in the same way for legislators and national courts.

A Spanish court referred a question for a preliminary ruling to the CJEU with the following facts: A phone had been stolen and the police, in order to clarify the circumstances, filed a request to obtain access to the retained data about the phone. The scope of the request was limited: the subscribers data (name, surname, domicile and telephone number) of the SIM cards that had been activated in the stolen phone in the first twelve days after the theft.[102] The request was addressed to the competent judge, who needs to authorize the access. In first instance, however, the judge refused to grant access, because the crime that was being investigated, is not qualified as a «serious crime».[103] In second instance, the question was referred to the CJEU.[104]

In light of the *Tele2* judgement the question asked by the *Audiencia Provincial de Tarragona* may have led to the Spanish data retention regime being declared contrary to EU law.[105] The Spanish data retention legislation stems, basically, from the now invalid Data Retention Directive.[106]

However, the Court interpreted the scope of the question differently. It basically

[100]Directive 2002/58/EC of the European Parliament and of the Council.

[101]Judgement of the Court (Grand Chamber) of 2 October 2018, *Ministerio Fiscal*, C-207/16. ECLI:EU:C:2018:788.

[102]Ibid., para. 20.

[103]Ibid., para. 21.

[104]Ibid., para. 26.

[105]Rodríguez Lainz, José Luis (2018). "El Régimen Legal español en materia de conservación y cesión de datos para la investigación de delitos. Comentario a la sentencia del TJUE de 2 de febrero de 2018". In: *Diario La Ley* 9291, pp. 6-7.

[106]Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Available at: `https://boe.es/buscar/act.php?id=BOE-A-2007-18243`, visited on 23rd February 2019, preamble I.

reduced the question to aspects of access. This means, essentially, that the Court did not judge the Spanish data retention scheme, but only the access to the retained data. Hence, what was actually being discussed was the question which are the conditions and circumstances for gaining access to retained data.[107]

In *Tele2* the CJEU stated that access to retained data by authorities is only legal in cases which are considered to be «serious crimes».[108] Also, the Data Retention Directive stated the same, making it a guarantee.[109] In *Ministerio Fiscal*, however, the Court finds that this consideration is too strict and modifies its interpretation. Access to retained data may be granted, even in cases where no «serious crimes» are investigated, depending on the proportionality of the access.[110] In this sense, the Court decides that access to the subscribers data (name, surname, domicile and telephone number) of the SIM cards activated in the phone in the first twelve days after the theft is proportional; this data does not reveal substantial and precise information of the affected and constitutes, therefore, no *serious* interference with fundamental rights.[111] In order to justify a serious interference with fundamental rights (permitting precise conclusions about the private life of the affected), the criminal offence being investigated must also be qualified as «serious».[112]

The judgement is not as protective as *Tele2* and even sets the limit for data access lower than the now invalid Data Retention Directive (see *supra* 1.1). In the view of a Spanish jurist, the Court is «cheating while playing solitary».[113] Moreover, the Courts assumes the conversion of a tool that was introduced for the fight against terrorism (see *supra* 1.1), into a tool that might even be used for ordinary offences. Further, the differentiation on what is and what is not proportional regarding data access may be problematic.

[107]Judgement of the Court (Grand Chamber) of 2 October 2018, *Ministerio Fiscal*, C-207/16, para. 49.

[108]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 115.

[109]Directive 2006/24/EC of the European Parliament and of the Council, art. 1(1).

[110]Judgement of the Court (Grand Chamber) of 2 October 2018, *Ministerio Fiscal*, C-207/16, paras. 55 and 57.

[111]Ibid., paras. 59-63.

[112]Ibid., para. 56.

[113]A slightly adapted translation of an idea expressed by Maeztu, David (2018). *El Tribunal de Justicia y la conservación de datos, sentencia "Ministerio Fiscal"*. Available at: `https://www.derechoynormas.com/2018/10/el-tribunal-de-justicia-y-la.html`, visited on 23rd February 2019.

From a different point of view, the Court may have gained, through this decision, the power to decide which access is proportional and which is not. Up until the judgement, Member States could modify their criminal laws and introduce their concept of «serious crime». Now, the Court, decides (if asked, of course) on what is and what is not proportional.

What is furthermore interesting about this verdict, is that the CJEU once again —as in *Digital Rights Ireland* and *Tele2*— assumes its competence regarding the access of data: a field, as pointed out earlier (see *supra* 1.2.3), that may not be EU competence.

1.3 Conclusion

The decisions in *Digital Rights Ireland* and *Tele2* draw the following red lines: a general and indiscriminate data retention scheme is not proportional. Data retention, however, is possible if it is limited in time and aimed at specific subjects. Furthermore, there must exist an objective nexus between the retention and the investigation of a crime.

Data must be stored in the European Union and secured by appropriate security measures, in order to prevent any illicit use. Access may only be granted to authorities after judicial (or independent administrative) review.

According to *Digital Rights Ireland* and *Tele2* access is only possible for serious crimes; but the *Ministerio Fiscal* decision finds that access is also possible for ordinary crimes, if it does not constitute a serious interference with fundamental rights. This last decision leaves the purpose limitation of the Data Retention Directive behind (intended for serious crimes only) and relies on a, fragile, judicial deliberation if an interference is serious or not.

Chapter 2

Beyond the CJEU Jurisprudence: What's next?

2.1 Legal Framework

2.1.1 Overview

Until May 2018 the Privacy and Electronic Communications Directive from 2002 was complementing the Data Protection Directive from 1995,[1] thereby trying to promote data protection and privacy in the era of digital technology.[2] In May 2018 the GDPR, the European Union General Data Protection Regulation, entered into force and repealed the Data Protection Directive from 1995.[3]

The Privacy and Electronic Communications Directive from 2002 is the most specific instrument that refers to data retention (see *supra* 1.2 and article 15 of the Directive).[4] The GDPR provides for a more general framework applicable to data protection. Also, since 2009 the Charter of Fundamental Rights of the European Union guarantees fundamental rights to the citizens of the EU.[5]

Most importantly, however, the CJEU sets very specific and essential limits for data retention in its case law, as described in the previous chapter.

All the foregoing, taken as a whole, should be borne in mind when regulating future forms of data retention in the European Union or in one of its Member States.

[1] Directive 95/46/EC of the European Parliament and of the Council.

[2] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, paras. 82-83.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council, article 94.

[4] This Directive may be repealed soon by a new Regulation, the ePrivacy Regulation of the EU.

[5] However, the Charter does apply only to activities comprised by EU law as stated in the Charter of Fundamental Rights of the European Union, art. 51.

2.1.2 GDPR Principles: Purpose, Minimization, Security

The GDPR principles offer a good starting point for analysing possible configurations of future data retention regulations, as they are at the very centre of the data protection framework of the EU.

It is, however, unclear if this Regulation is actually applicable to data retention. Article 2(2) of the GDPR sets out that:

> *«This Regulation does not apply to the processing of personal data: [...] (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.»*

In light of the foregoing, we might actually conclude that the GDPR is not applicable to data retention. However, Directive 2002/58/EC, includes a similar exclusion in article 1(3)[6] and the CJEU considered this no obstacle for applying this Directive to data retention (see *supra* 1.2). Moreover, some of the following principles did exist prior to the GDPR as well.[7] These principles are also explicitly mentioned in the Directive 2016/680 regulating the «[...]processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [...]».[8,9] Finally, in light of the CJEU case law, they may be a relevant part of the fundamental rights enshrined in article 7, «Respect for private and family life», and 8, «Protection of personal data», of the Charter.[10]

[6] «This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.»

[7] Some principles were already foreseen in 1995, see: Directive 95/46/EC of the European Parliament and of the Council, art. 6.

[8] Directive (EU) 2016/680 of the European Parliament and of the Council. Available at: `http://data.europa.eu/eli/dir/2016/680/oj`, visited on 14th April 2019, art. 1(1).

[9] The list of the GDPR principles is almost identical to the one in art. 4(1) of Directive 2016/680.

[10] For the effects and the influence of the Charter of Fundamental Rights of the EU on a broader protection of these rights see: Fabbrini, Federico (2015b). "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court". In: *iCourts Working Paper Series* 19. Available at: `https://ssrn.com/abstract=2576214`, visited on 13th April 2019, pp. 17-20, 22.

Therefore, they should be taken into account —at least as informing principles— independently of the applicability of the GDPR or not.

The first principle to take into account is *purpose limitation*.[11] Retained data should only be used and treated for a «specified, explicit and legitimate purpose».[12] This purpose would depend on any new legislation and its scope of application: in line with the anterior Data Retention Directive it would concern the investigation of criminal offences.[13]

Secondly, the data retained should be minimized (*data minimisation*) to what is «adequate, relevant and limited [...] in relation to the purpose».[14] Thus, there should be a nexus between the data retained and the purpose, reducing the data to be retained accordingly.

In third place, the retained data should allow the identification of the affected no longer than what is necessary for the purpose of the retention: this principle is called *storage limitation*.[15]

In fourth place, the retained data needs to be stored securely, it should be protected against «loss, destruction or damage» and «unauthorised or unlawful» access, the *integrity and confidentiality* principle.[16]

Lastly, retained data should be «processed lawfully, fairly and in a transparent manner», without obstructing the purpose of the retention at the same time.[17]

Article 6(1)(c) of the GDPR, states that processing is lawful in cases of legal obligation: Obviously, this is the case of data retention imposed by national law, a new Data Retention Directive or any comparable regulation.

[11]Regulation (EU) 2016/679 of the European Parliament and of the Council, article 5(1)(b).
[12]Ibid., article 5(1)(b).
[13]Directive 2006/24/EC of the European Parliament and of the Council, article 1(1).
[14]Regulation (EU) 2016/679 of the European Parliament and of the Council, article 5(1)(c).
[15]Ibid., article 5(1)(e).
[16]Ibid., article 5(1)(f).
[17]Ibid., article 5(1)(a).

2.2 Considerations for the Future of Data Retention

2.2.1 General and Targeted Retention: Objective Nexus

Data retention can basically be carried out in two manners. It can be «general and indiscriminate» [18] as criticised by scholars [19] and the case law of the CJEU or it can be targeted, this is to say that it is actually circumscribed to a certain and determined group or number of persons. [20, 21]

Taking into account the decisions in *Digital Rights Ireland* and *Tele2* it results clearly that the Court does accept data retention, also if it is preventive, but only if such a measure complies with certain limitations. [22, 23] Retention should only apply to persons who are linked to the investigation of a criminal offence. This implies that retention measures should be targeted, usually to persons who are actually suspicious. [24] Targeted retention is less intrusive than «general and indiscriminate» retention,[25] therefore any new data retention regulation should rather be targeted.

Not only should a measure in this sense be targeted, but there ought to be an objective nexus between a retention measure and a criminal investigation. This it to say that retention of traffic data about a determined number of persons should only be permitted, if a suspicion exists that these persons are, directly or indirectly, linked

[18] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 103.

[19] Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States", p. 80.

[20] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 106.

[21] The CJEU case law also cites the use of a geographical criterion as an option, which casts some doubts upon its possible use, see: Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 167.

[22] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, paras. 105-106 and 108.

[23] Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, paras. 57-59.

[24] Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 166.

[25] European Data Protection Supervisor (2011). *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*. Available at: `https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52011XX0923(01)`, visited on 7th April 2019, para. 56.

to the commission of criminal offences.[26, 27] The stored data shall not be used for other unrelated investigations, as this would render the objective nexus requirement void, useless and leaves the door ajar for possible misuse. Eventually, data retention is a tool in order to help with ongoing criminal investigations; it should not be a goal in itself.

Targeted data retention measures might also be used as a preventive investigation tool, according to the case law of the CJEU.[28] If an objective and justifiable reason exists, this is a valid use case; this preventive usage should in any case be limited and reviewed externally on a regular basis.

Some may argue that the actual utility of targeted and general retention is not the same. The first one, targeted retention, is used for the surveillance of a person who is actually suspicious of having participated in a criminal offence, whereas the second on, general retention, would not only be used for the investigation of crimes, but also for the discovery of uncommon communication patterns, which supposedly may identify future criminals.[29, 30] This last argument is neither well founded because the effectiveness of data retention, in this regard, has not been proven,[31, 32] nor well compatible with the protection of fundamental rights and freedoms. It leaves the distinction of what is and what is not *normal*, in terms of communication patterns, in the hands of investigators. Furthermore, it may undermine the presumption of innocence as it permits to treat everyone as a possible suspect, accumulating his or her traffic data, even without any evidence about criminal ongoings.[33]

In this sense, a balanced, proportional data retention system is a targeted one.

[26]Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", pp. 166-168.

[27]Exceptionally, data of persons who are not suspected may be retained if this data may effectively contribute to secure interests such as «vital national security, defence or public security interests», see: Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 119.

[28]Ibid., para. 109.

[29]Fennelly, "Data retention: the life, death and afterlife of a directive", pp. 4-5.

[30]Sarre, Rick (2017). "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia". In: *Asian Journal of Criminology* 12 (3). ISSN: 1871-014X. Available at: `https://doi.org/10.1007/s11417-017-9256-7`, visited on 27th November 2018, pp. 172-173.

[31]Ibid., p. 176.

[32]Guild and Carrera, "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", p. 4.

[33]For further details on the nexus between retention and investigations, see: Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", pp. 166-167.

2.2.2 Accountability, Oversight and Transparency

In order to guarantee legal security for all implied parties, the following aspects shall be taken into account.

According to the GDPR principles (see *supra* 2.1.2), *accountability*[34] shall be expressly highlighted. Tracing usage, access, storage, protection, integrity and security of retained data is necessary in order to guarantee compliance with data retention laws, to facilitate judicial (and/or administrative) control and to ensure the fulfilment of obligations under data protection laws. Without these organisational measures to demonstrate *how* and *by whom* data has been handled, no control can be achieved. This obligation shall be applicable to both telecommunication service providers and to authorities who process the corresponding data, otherwise its utility would only be partial. In other words, the use of retained data should become clearly traceable and this usage shall be disclosed to judicial or administrative institutions if required to do so.

The internal accountability obligation may also stimulate the revision of the legality of retention orders, either by internal legal supervisors of communication service providers or by any equivalent institution in law enforcement authorities, as unlawful processing and disclosure (see *supra* 2.1.2) shall be avoided.[35] Also, it would be desirable for telecommunication service providers to technically separate retained data from any other client data: this would contribute to the CJEU case law requirement of a high standard of security measures.[36]

Another guarantee, which is absolutely indispensable, is judicial *oversight*. Data retention and/or access measures shall always be reviewed by a judicial or an independent authority, in order to check if the legality, formal and material requirements, of the retention and/or access is given.[37] This review shall take place prior to the access to the data by authorities. Ideally a warrant should even be obtained for issuing a data retention order to a communication service provider, which would, even if this warrant is not rapidly granted, permit a greater control *ex ante*.[38] Also,

[34]Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 5(2).

[35]Ibid., art. 6.

[36]For the security standard required see: Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 169.

[37]Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 62.

[38]This would be desirable because any retention measure «constitutes in itself an interference»,

in exceptional cases of validly justified urgency, access to retained data could be obtained without a prior warrant, but should then be subject to a strict posterior review.[39]

Finally, *transparency* is another fundamental guarantee. Once the investigations, in which the data retention measure were applied, have concluded, the affected persons shall be notified as soon as possible about this measures. This notification shall not interfere with the investigations. Through this knowledge of the retention measures, the affected persons may consider legal remedies.[40] More public transparency would be achieved if law enforcement authorities release periodically and publicly statistics on the use of data retention measures.

Through these guarantees, a three-step system is designed. Firstly, an internal control through accountability may avoid misuse in telecommunication service providers or authorities and partially stimulates the internal revision of retention orders. Secondly, judicial oversight is an external control that directly assesses legality. Thirdly, posterior transparency permits the affected persons to take legal actions or file complaints with the relevant data protection authorities. The collaboration between an internal supervisor and the external, judicial and administrative, institutions is necessary to increase the effective control.

In this sense, a well balanced and proportional data retention system guarantees the *accountability* of retained data usage, strictly requires judicial (or independent) *oversight* in all cases and establishes *transparency* by notifying affected persons.

2.2.3 Storage Period and Erasure

Retained telecommunication traffic data shall not be stored for a generally fixed period of time, but rather for an individually established time range in each case. This permits greater respect for individual rights, in light of «what is strictly necessary»,[41] and grants flexibility according to the necessity of each case. In any case, a maximum limit shall exist. According to some opinions a maximum period of one year seems

see: ibid., para. 34.

[39]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 120.

[40]Ibid., para. 122.

[41]Ibid., para. 108.

acceptable.[42]

Once the individually established period has been reached, the retained data shall be permanently and irreversibly erased by the corresponding communication service provider.[43] Also, if the suspicion ceases to exist the retention measure should end.[44] In both cases: a new retention order for the same person under the same or a (directly) related criminal investigation shall not be granted, as it would permit to avoid the set retention period.

2.2.4 Precise and Comprehensive Legislation

Finally, to comply with the standard[45] set by the test of proportionality of the CJEU[46] some formal requirements should be taken into account.

Legislation, whether of Member States or the European Union, on both retention and access, should be «clear and precise» and has to contain provisions on circumstances and conditions that permit the application of data retention and, as the case may be, access, ensuring the existence of safeguards for the protection of personal data of the affected persons.[47, 48]

Beyond these conditions, legislation shall require that any retention order and any access to retained data must follow an objective criteria.[49] Such an objective criteria could be the knowledge of the preparation of a criminal offence or the suspicion that

[42] *Opinion of Mr Advocate General Cruz Villalón delivered on 12 December 2013, Digital Rights Ireland, C-293/12 and C-594/12*. ECLI:EU:C:2013:845. Available at: `https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1556207084604&uri=CELEX:62012CC0293`, visited on 25th April 2019, paras. 143-149.

[43] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 122.

[44] Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 168.

[45] About the standard of the test of proportionality in *Digital Rights Ireland*, see: González Pascual, "El TJUE como garante de los Derechos en la UE a la luz de la sentencia Digital Rights Ireland", pp. 956-958.

[46] For a clear explanation of the test of proportionality in *Digital Rights Ireland*, see: Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States", pp. 78-81.

[47] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, paras. 109 and 117.

[48] Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 54.

[49] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, paras. 110 and 119.

an individual has committed a crime,[50] in the case of ordering a targeted retention measure; in the case of access to retained data, such a criterion could be that access has to be solicited for the same reason as the retention was ordered for. Specifically, access may not necessarily be granted to all the retained data: only to the data necessary for a determined investigation.[51]

Furthermore, the relevant legislation should be as comprehensive as possible: this avoids the distribution of the applicable regulation in different laws and avoids possible contradictions (see also *infra* 3.1.1). This measure provides legal security and certainty.

2.3 Data Preservation or «Quick Freeze»

2.3.1 Introduction

A practical alternative to conventional data retention would be a system that is known as data preservation or «quick freeze». It is based on a simple presumption: that data of specific person or group can be retained or stored if there is a suspicion relating to this person or group.[52]

Data retention, in comparison, is based on another presumption: that it is necessary to retain all traffic data in a general manner. This would permit, apart from investigating committed crimes, to identify atypical activities and to anticipate criminal offences.[53, 54] As already stated, this «general and insdiscriminate»[55] retention does strongly interfere with fundamental rights and is one of the reasons why the

[50] A concept such as «serious crime» or crimes punished with jail sentences of a certain duration could be an additional requirement.

[51] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 96.

[52] European Commission (2011). *Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*. Available at: `https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52011DC0225`, visited on 7th April 2019, p. 5.

[53] Sarre, "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia", pp. 172-173.

[54] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, paras. 55-56.

[55] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 103.

CJEU declared the Data Retention Directive invalid (see *supra* 1.2).

Data preservation is neither a new alternative to data retention, nor a new complementary tool, but was already incorporated in the Budapest Convention on Cybercrime of 2001.[56,57] It was also discussed in the institutions of the European Union before and after adopting the Data Retention Directive: In this sense, the Data Protection Supervisor[58] and the Article 29 Working Party[59] recommended to the EU legislators that data preservation would be an alternative to data retention. However, scholars have hardly discussed data preservation so far.

2.3.2 Principles

As stated, data preservation or «quick freeze» is used for targeted surveillance. Once a person is suspicious to authorities, these authorities may issue an preservation order to the corresponding telecommunication service provider, so that future telecommunication data about the suspicious person is being stored and retained. This preservation order obliges the telecommunication service provider to store the requested data for a certain period of time.[60]

In order to gain access to this data, a judicial warrant would be necessary.[61,62]

[56]Convention on Cybercrime (Budapest Convention). Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, visited on 7th April 2019, art. 16.

[57]Directorate-General for Migration and Home Affairs (European Commission) and Centre for Strategy and Evaluation Services (CSES) (2013). *Evidence of potential impacts of options for revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries*. Available at: https://publications.europa.eu/en/publication-detail/-/publication/5dc1b779-1a1c-4e53-a17f-1fd0fe71e4ad, visited on 7th April 2019, p. 5.

[58]European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, para. 57.

[59]Article 29 Data Protection Working Party (2005). *Opinion 4/2005*. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec13, visited on 7th April 2019, p. 6.

[60]Directorate-General for Migration and Home Affairs (European Commission) and Centre for Strategy and Evaluation Services (CSES), *Evidence of potential impacts of options for revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries*, p. 5.

[61]European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, para. 54.

[62]See also Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*,

Alternatively, judicial review could also be envisioned prior to the preservation order (see *supra* 2.2.2); however, this may be impractical.

It is unclear whether data preservation should only apply to traffic data, as indicated by the European Data Protection Supervisor,[63] or if it could apply to communication content too, as is the case with the Budapest Convention on Cybercrime.[64] It is save to assume, in any case, that the storage or retention of communication content may affect various fundamental rights essentially.[65]

Two different models of data preservation are being discussed: «quick freeze» and «quick freeze plus». In the «quick freeze» model data would only be stored from the moment of the preservation order. In the «quick freeze plus» model the telecommunication service provider would additionally retain (and give access to, if a judicial authorisation is obtained) the data it has stored for any legitimate purposes (i.e. billing or advertisement).[66]

2.3.3 Guarantees: Access Logs and Judicial Review

In order to ensure compliance with fundamental rights, internal and external guarantees should be considered and established (see *supra* 2.2.2).

Internal guarantees affect the telecommunication service providers, who are obliged to retain or store data, and authorities. These guarantees shall, following the underlying principles of the GDPR, establish accountability.[67] This is to say, that it should be possible to trace the usage of the affected data and the compliance with the relevant principles (see *supra* 2.2.2). As a practical idea, already proposed by the Article 29 Working Party, access logs should be established, stating who,

C-203/15 and C-698/15, para. 120.

[63]European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, para. 54.

[64]Directorate-General for Migration and Home Affairs (European Commission) and Centre for Strategy and Evaluation Services (CSES), *Evidence of potential impacts of options for revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries*, p. 8.

[65]See in this regard: Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 101.

[66]European Commission, *Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, p. 6.

[67]Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 5(2).

when and for which purpose had access to the data.[68] These logs shall be made available to judicial and data protection authorities upon request.[69] Internal access should be limited to a certain number of authorized persons[70] and any usage of the data other than for the purpose set out in the legislation should be illegitimate (i.e. access by unrelated third parties).[71,72] Moreover, an internal legal supervisor could be established, in order to check the legality of preservation orders and access requests.

External guarantees affect the access of authorities to the retained or stored data. As stated in the *Digital Rights Ireland* and the *Tele2* case, prior judicial authorisation (or prior review by an independent administrative body) is necessary for access to the retained data.[73,74] This judicial oversight is also remarked by authors like Ryan, stating its importance in relevant decision on data retention.[75] This authorisation may only be granted if specific conditions, such as a plausible suspicion, a threat or other objective criteria, are met.[76]

Both guarantees are complemented by another instrument, which is mandatory according to the Charter of Fundamental Rights of the EU: oversight by the competent data protection authority.[77] This is also an issue addressed by the CJEU, stating expressly that the intervention of said authorities only applies if a complaint is lodged, making it therefore an optional guarantee.[78] Keep in mind that compliance with the applicable legislation can not be demonstrated if there is no internal

[68] Article 29 Data Protection Working Party, *Opinion 4/2005*, p. 8.

[69] Ibid., p. 8.

[70] Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 62.

[71] See the purpose limitation principle in: Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 5(1)(b).

[72] Article 29 Data Protection Working Party, *Opinion 4/2005*, pp. 8-10.

[73] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 120.

[74] Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 62.

[75] Ryan, Michael (2016). "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights". In: *TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016*. Available at: `http://dx.doi.org/10.2139/ssrn.2742057`, visited on 7th April 2019, p. 20.

[76] Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", pp. 168-169.

[77] Charter of Fundamental Rights of the European Union, art. 8(3).

[78] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 123.

accountability regarding the processing of the retained data.

2.3.4 Critical Aspects

Data preservation does in fact share a lot of critical aspects with data retention as declared invalid by the CJEU (see *supra* 1.2).

Firstly, problems relating to access to the retained or stored data are equally valid for both data preservation and data retention: there is no objective difference between the data stored in one way or another, when it comes to access by authorities. Legislation on this subject —access— must be «clear and precise» and has to contain provisions on «substantive and procedural conditions» that permit access to the data.[79] Access may only be granted according to objective criteria and prior independent oversight (i.e. judicial review) must be assured.[80] Furthermore, the affected shall be notified, after the access to the retained data (or after the retention without access) by the competent authorities, but only from the moment when this notification will not affect ongoing investigations anymore.[81, 82]

Secondly, data security measures are applicable in the same way to data retention as to data preservation: data must be stored in the EU, secured with «appropriate technical and organizational measures» and must be irreversibly destroyed once the storage period has ended.[83]

Lastly, what differentiates data retention from data preservation is the *reason* of the retention. Data retention is general and affects virtually everyone without any particular reason, whereas data preservation is targeted retention of communication data because of a particular reason (see *supra* 2.2.1). However, data preservation may affect, depending on the implementation, both content and traffic data: especially the retention of content data could be critical taking into account the CJEU decisions.[84, 85]

[79]Ibid., paras. 117-118.

[80]Ibid., paras. 119-120.

[81]Ibid., para. 121.

[82]Fennelly, "Data retention: the life, death and afterlife of a directive", p. 15.

[83]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 122.

[84]Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 165.

[85]Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 101.

Sure enough, data preservation is not perfect and may be abused (as well as any other governmental power), but it establishes, at least, a link between a specific investigation based on a suspicion, on one hand, and a surveillance measure, on the other. It is therefore compatible with the «objective evidence», between a criminal offence and the affected public, that could justify data retention according to the CJEU.[86, 87]

[86]Ibid., paras. 110-111.

[87]It must be «possible to create a link between the persons whose data are retained and the prevention of or fight against serious crime» according to: Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", pp. 166-167.

Chapter 3

Alternative Systems and Lessons for Data Retention in the EU

In this chapter various data retention systems in different jurisdictions will be analysed in light of the foregoing guarantees and considerations. We will firstly treat two flawed systems and secondly two balanced, rather proportional ones. Both categories permit to draw conclusions for future regulation and analysis of the topic.

3.1 Flawed Data Retention Systems

3.1.1 Access to Telecommunication Data in the United States

The approach to data retention in the United States (US) is very different from the European one discussed above.

Firstly, there is no general, comprehensive regulation concerning data retention of telecommunication data.[1] Secondly, the difference between content and traffic data (see *supra* 1.1) is of utmost importance for constitutional protection.[2] Thirdly, the intervention of third parties implies important restrictions for the expectation of privacy regarding telecommunication data.[3]

Access to data, either content of traffic data, is not regulated in one single act. It is partially covered by the Fourth Amendment of the US Constitution,[4] as long as a

[1] Ryan, "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights", p. 17.

[2] Fura, Elisabet and Klamberg, Mark (2012). "The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA". in: *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights*. Ed. by Casadevall, Josep, Myjer, Egbert and O'Boyle, Michael. Oisterwijk: Wolf Legal Publishers. Available at: `https://ssrn.com/abstract=2169894`, visited on 27th November 2018, p. 477.

[3] Ibid., pp. 476-477.

[4] «The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.» according to: Constitution of the United States. Available

conduct constitutes a «search». Traffic data, however, is not covered by the Fourth Amendment, as expressed by scholars, whereas content data does in fact receive this protection.[5]

Moreover, the case law of the US Supreme Court established what is known as the *third party doctrine*: if a third party has access to data the subject concerned loses its rights of protection granted by the US Constitution. «In other words, by disclosing information to a third party such as a bank or a CSP [communication service provider], the subject gives up all of his Fourth Amendment rights in the information revealed, including data retained in a database or an information network.»[6] Commonly, telecommunication providers in the United States already store traffic data for «marketing purposes», which facilitates the use by law enforcement authorities.[7]

This does not mean that no protection or regulation is offered for traffic data. «Electronic surveillance law in the United States is comprised primarily of two statutory regimes: (1) the Electronic Communications Privacy Act (ECPA), which is designed to regulate domestic surveillance; and (2) the Foreign Intelligence Surveillance Act of 1978 (FISA), which is designed to regulate foreign intelligence gathering.»[8] Generally speaking the ECPA offers a higher level of protection than the FISA. Specifically in reference to traffic data retention, some other legislative measures[9] require the authorities to obtain court orders.[10]

Even though some Acts may grant regulation and protection to traffic and content data, in practice the National Security Agency is creating important databases concerning this data, warrantlessly. There seems to be a divergence between the powers foreseen by the ECPA/FISA and the powers conferred to the President by virtue of the legislation enacted in response to the fall of the twin towers in September

at: `https://www.senate.gov/civics/constitution_item/constitution.htm`, visited on 3rd November 2018.

[5]Fura and Klamberg, "The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA", pp. 476-477.

[6]Ibid., p. 476.

[7]Bignami, Francesca (2007b). "Privacy and Law Enforcement in the European Union: The Data Retention Directive". In: *Chicago Journal of International Law* 8 (1). Available at: `https://ssrn.com/abstract=955261`, visited on 27th November 2018, p. 238.

[8]Fura and Klamberg, "The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA", p. 478.

[9]The Pen Register statute and the Stored Communications Act according to: ibid., p. 479.

[10]Ibid., pp. 478-479.

2001. In some cases of surveillance (measures) it remains unclear which legislation is applicable.[11]

Public and Private Institutions

It is important to stress the difference between data retention by telecommunication service providers, which is *indirect* and retention *directly* executed by law enforcement authorities. The latter, as stated above and in accordance with the Snowden revelations,[12] is common practice in the US; this does not imply that authorities would not rely on *indirect* measures, too.[13] This double dimension, especially visible in the context of the United States, raises the question if a comprehensive regulation should regulate retention and access for both public and private institutions.

In light of the CJEU case law

From the CJEU case law perspective and taking into account the ideas discussed up until now, the United States data retention regulation lacks essential safeguards.

Firstly, no comprehensive and clear legal framework is given for data retention of traffic data. This does interfere fundamentally with the principle of legal security.

Not all retention activities are judicially (or independently) overseen, depriving citizens therefore of a basic safeguard and protection.

There seems to be little transparency or accountability regarding the interference with the private lifes of the population by law enforcement authorities or by telecommunication service providers. Without transparency, control is hardly possible.

Also, retention is not targeted but is affecting the general public, without any (known) objective criteria relating to criminal offences that are being investigated.

Bignami already stated in 2007 that some practices which are common in the US would be «clearly illegal in Europe»,[14] an opinion which seems to be well anticipated

[11] Ibid., pp. 479-481.

[12] Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States", p. 89.

[13] Fura and Klamberg, "The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA", pp. 468-469.

[14] Bignami, Francesca (2007a). "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". In: *Bosten College Law Review* 48 (3). Available at: `https://lawdigitalcommons.bc.edu/bclr/vol48/iss3/3/`, visited on 26th April 2019, p. 635.

in light of the posterior CJEU case law.

3.1.2 Retention in Australia

Australia has a general data retention regulation, enacted in 2015. It provides for a data retention system that affects traffic data of all telecommunication service providers for two years.[15]

This data may be accessed by law enforcement authorities without a judicial warrant nor any other comparable, external and independent, oversight, except for journalists.[16] However, the Commonwealth Ombusdman should «assess agency compliance».[17] It was discussed if the retained data could be used for civil proceedings, but finally this civil usage was discarded.[18, 19]

According to scholars, the data retained in observance of this legislation has been widely used since its entry into force. The most investigated offences were drug-related,[20] even though retention measures are often justified as anti-terrorism measures.[21]

The Australian data retention legislation has not been spared from criticism; it is considered excessive and the lack of safeguards has been pointed out.[22, 23] Also, as a specific Australian characteristic, the absence of a Bill of Rights or a fundamental rights framework has been stressed: other than in most European states, for example, there is no constitutional (or supranational) control possible.[24, 25] This reveals the importance and discretion of the legislator, which is not directly limited

[15]Meares, Michelle (2018). "Mass Surveillance and Data Retention in Australia: Balancing Rights and Freedoms". In: *Journal of Internet Law* 21 (10). ISSN: 1094-2904, p. 3.

[16]Ibid., p. 3.

[17]Sarre, "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia", p. 171.

[18]Ibid., p. 171.

[19]Meares, "Mass Surveillance and Data Retention in Australia: Balancing Rights and Freedoms", p. 4.

[20]Ibid., p. 4.

[21]Sarre, "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia", pp. 172-173.

[22]Ibid., pp. 173-176.

[23]Meares, "Mass Surveillance and Data Retention in Australia: Balancing Rights and Freedoms", p. 3.

[24]Ibid., p. 5.

[25]Sarre, "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia", p. 175.

by fundamental rights. It is, in this case, essentially for the legislator to balance the surveillance power conferred to law enforcement authorities and liberties in a democratic society.

From a European Union perspective, the Australian data retention regulation lacks necessary safeguards. As Meares points out, the Australian regulation would be most probably «considered general and indiscriminate».[26] Furthermore, no judicial (or independent) oversight is guaranteed, except for journalists: access is therefore arbitrarily possible.

This highly intrusive regulation also permits to emphasize the necessity of effective safeguards. Even though the Australian data retention regulation offers protection to journalists (in their condition as an essential part of any critical democratic society) establishing that law enforcement authorities need to obtain a warrant for access to their traffic data, it became known that these authorities also obtained such data *without* a warrant.[27, 28] Eventually, this shows different problems: in the first place, that it should not be exclusively for authorities to determine if they have access or not to sensitive datasets. As the case shows, these powers may be misused. In the second place, that an telecommunication service provider should be, at least, diligent when it comes to collaboration with law enforcement. This is to say that if the law grants special protection to journalists, a partial responsibility of compliance with this legal standard corresponds to the telecommunication service providers, too.[29] In the third place, and most importantly, that safeguards need to be logically interlinked and connected in order to prevent abuse. If law is granting a special treatment to journalists, this legal protection should be effectively ensured by a logical design (see *supra* 2.2.2).[30]

[26]Meares, "Mass Surveillance and Data Retention in Australia: Balancing Rights and Freedoms", p. 5.

[27]Ibid., p. 3.

[28]Sarre, "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia", p. 175.

[29]Service providers should prevent «unauthorized interference and access» according to: Meares, "Mass Surveillance and Data Retention in Australia: Balancing Rights and Freedoms", p. 3.

[30]Sarre writes, in this context, that «the ease with which the access was obtained should remain a matter of concern», see: Sarre, "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia", p. 175.

3.2 Balanced Data Retention Systems

3.2.1 The Austrian Data Preservation System

Austrias data retention system is similar to the data preservation approach explained above (see *supra* 2.3).

After the *Digital Rights Ireland* decision the Austrian *Verfassungsgerichtshof* (Constitutional Court) stroke down the national data retention regime[31,32] and subsequently law enforcement authorities had less legal options for investigating criminal offences through technological means.

Alternatives were discussed and disputed afterwards, but it was not until 2018 that the government proposed and the parliament approved of the so-called *Sicherheitspaket* («Security Package») or, as named by its critics, the *Überwachungspaket* («Surveillance Package»).[33] Included in this legislative *package* a new data preservation regime was defined and called *Anlassdatenspeicherung* (literally «data retention for a reason»).[34]

It enables law enforcement authorities, in this case the public prosecutor's office, to order communication service providers to retain data (traffic data, location data and access data) of a specific subject or subjects.[35] This order may be issued once a an initial suspicion, that a crime has been committed,[36] exists.[37] Moreover, it is necessary that the wilful offence being investigated is at least punished with a six month jail sentence, if the owner of device affected by the retention measure consents, or else with a one year jail sentence,[38] among other possible use cases.

[31]Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States", p. 88.

[32]Verfassungsgerichtshof, 27th June 2014, G47/2012. Available at: `https://www.vfgh.gv.at/downloads/VfGH_G_47-2012_ua_VDS_schriftliche_Entscheidung.pdf`, visited on 25th April 2019.

[33]Adensamer, Angelika and Hanel, Alina (2018). "Das Überwachungspaket im Überblick". In: *juridikum* 3. ISSN: 2309-7477, p. 292.

[34]Ibid., p. 296.

[35]Ibid., p. 296.

[36]Strafprozeßordnung 1975 (StPO). Available at: `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326`, visited on 25th April 2019, § 1(1).

[37]Ibid., § 135(2b).

[38]Being the latter option the most probable case, see: Adensamer and Hanel, "Das Überwachungspaket im Überblick", p. 296.

The relevant data has to be stored for a period as long as necessary to fulfil its purpose, not exceeding twelve months in any case.[39] In order to gain access to the retained data, the public prosecutors office needs a warrant form a judicial institution who controls the legality of the retention order issued,[40] although this is not stated with absolute clarity in the relevant articles.[41,42] It is noteworthy that the affected of the surveillance measures are going to be notified once this information will not jeopardize ongoing and related investigations anymore.[43]

Criticism

Scholars criticize the excessive length of the retention (or preservation) of data, stating that it is likely that data of communication activities of up to a year would have similarities with the system of the Data Retention Directive. Adensamer and Hanel expressly remark that the data which is temporally unlinked (i.e. data collected long before or long after) to the reason of the preservation, foreseen in the current Austrian legislation, may be colliding with fundamental rights as it resembles more a general data retention than a targeted one.[44] It must be said, however, that the Austrian legislation sets twelve months as a maximum, not as a minimum or a standard.[45] This is in line with the opinion of the Advocate General Cruz Villalón who stated that data retention for more than a year would hardly be proportional.[46,47]

Moreover, it is criticised that a judicial warrant is not necessary until the actual access to the retained data is solicited. The legislators claim that this is according

[39] Strafprozeßordnung 1975 (StPO), § 137(3).

[40] Adensamer and Hanel, "Das Überwachungspaket im Überblick", p. 296.

[41] Strafprozeßordnung 1975 (StPO), §§ 134-140.

[42] Rom writes that the new regulation only regulates the preservation or retention of data. To access this data it is necessary to comply with the same standards as foreseen for other datasets, meaning that a judicial authorization is necessary. See: Rom, Brigitte (2018). "Neuerungen im Strafverfahren - das Strafprozessrechtsänderungsgesetz 2018". In: *Österreichische Juristen-Zeitung* 17. ISSN: 0029-9251, p. 764.

[43] Strafprozeßordnung 1975 (StPO), § 138(5).

[44] Adensamer and Hanel, "Das Überwachungspaket im Überblick", p. 296.

[45] Rom, "Neuerungen im Strafverfahren - das Strafprozessrechtsänderungsgesetz 2018", p. 764.

[46] *Opinion of Mr Advocate General Cruz Villalón delivered on 12 December 2013, Digital Rights Ireland, C-293/12 and C-594/12*, para. 150.

[47] Most data is accessed within the first three months according to Guild and Carrera, "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", p. 14.

to CJEU jurisprudence.[48] However, it is unclear if this is the case because the CJEU states that retention (without access) also interferes with fundamental rights:[49] on one hand data retention itself does interfere with the rights of the *Charter of Fundamental Rights of the European Union*; on the other hand control exists, but posterior to the retention. In any case, judicial oversight is mandatory and must take place prior to access to data by authorities.[50]

Even though the GDPR is of direct application in the whole European Union and grants a minimum of standards to comply with, the Austrian data preservation legislation does not establish any additional safeguards. This might be critical because both *Digital Rights Ireland* and *Tele2* insist on the specific requirements that data storage must meet in this context.[51, 52]

Furthermore, a very valid point of criticism is the lack of details regarding the nexus between the initial suspicion and the following data retention or preservation.[53] This nexus between an offence and an investigation measure must exist and is essential for proportionality (see *supra* 2.2.1).[54] The Austrian regulation does not cover this requirement adequately as it does not establish limitations on the use of the accumulated data by the retention measures: even though in other cases of surveillance the Austrian legislation enshrines the exclusion of evidence, in the case of the *Anlassdatenspeicherung* even unrelated evidence obtained by accidental discovery might be used afterwards. This implies that retained data is not necessarily used for the investigation of the initial suspicion.[55]

[48] Adensamer and Hanel, "Das Überwachungspaket im Überblick", p. 296.

[49] Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, para. 34.

[50] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, para. 120.

[51] Ibid., para. 122.

[52] Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, paras. 66-68.

[53] Adensamer and Hanel, "Das Überwachungspaket im Überblick", p. 296.

[54] Møller Pedersen, Udsen and Sandfeld Jakobsen, "Data retention in Europe—the Tele 2 case and beyond", p. 166.

[55] Adensamer and Hanel, "Das Überwachungspaket im Überblick", p. 296.

3.2.2 Data Retention in Canada

In Canada there is no general data retention legislation in force.[56] However, case law gives us a general understanding on how the issue is handled and interpreted.

The Canadian Charter of Rights and Freedoms, as a part of the Canadian Constitution, guarantees «[...]the right to be secure against unreasonably search and seizure».[57] According to Ryan this has been interpreted by the courts as a «reasonable expectation of privacy»; a search is only admissible if it is foreseen by law[58] and once «(1) a prior warrant, (2) issued by a judicial or other impartial arbiter, (3) on a sworn showing of reasonable and probable cause»[59] is obtained.

Similar to the questions arising from the US Constitution, the definition of what constitutes a «search» and what does not is essential to determine the applicable legislation.

The importance of case law in Canada

This question has been addressed in the case law of the Supreme Court of Canada. After the judgement in *R. v. Spencer*[60] it was clear that even the request for subscriber information, voluntarily complied with by a telecommunication service provider, was qualified as a search. Even though the contract with the telecommunication service provider included a clause stating its collaboration with law enforcement, the court ruled that «disclosure was permissible only if required or permitted by law, and that compliance with the particular police request was neither required nor permitted by Canadian privacy laws. The search was therefore illegal.»[61,62]

[56]Ryan, "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights", p. 17.

[57]Constitution Act, 1982. Available at: `https://laws-lois.justice.gc.ca/eng/Const/page-15.html`, visited on 26th April 2019, section 8.

[58]Ibid., section 1.

[59]Ryan, "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights", p. 17.

[60]R. v. Spencer, 2014 SCC 43. Available at: `https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do?r=AAAAAQAHc3BlbmNlcgE`, visited on 29th April 2019.

[61]Ryan, "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights", p. 18.

[62]For the importance of *R. v. Spencer* and more context see: Penney, Steven (2014). "The Digitization of Section 8 of the Charter: Reform or Revolution?" In: *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 67. Available at: `https://digitalcommons.osgoode.yorku.ca/sclr/vol67/iss1/16/`, visited on 29th April 2019, pp. 521-533.

Later, in *R. v. Roger Communications*[63] it was held that «tower dumps», identifying all phone connections and the correspondent subscriber data of a cell phone tower, are not adequate to single out a «few individuals», which are being investigated for a criminal offence.[64] Intrusion should be minimized and therefore bulk retention is only possible if certain standards are met. The application of such a measure must take the principle of minimal intrusion into account and the applicants must justify the retention of data of certain cell towers (time, location and other possible data) in light of an investigation and explain why a certain data type (i.e. credit card information, names) is relevant; they must in addition provide for any information that may allow to reduce the retention measure to less individuals; also, a request for a report about the stored data shall be made and only in justified cases should the relevant «underlying data» made available to the authorities, who furthermore have to justify that this data can be interpreted and used.[65]

Conclusions from a European Perspective

Canadian case law offers, in accordance with the *Canadian Charter of Rights and Freedoms*, a balanced protection of rights and access to data by law enforcement authorities. The scope of application of what constitutes a «search» is relatively broad and does therefore offer protection even if data requested would be subscriber information (compare with *Ministerio Fiscal supra* 1.2 and constitutional protection in the US *supra* 3.1.1); this constitutional framework does grant an initial and fundamental safeguard, as it explicitly requires an independent warrant. Also the intrusion in the sphere of privacy should always be reduced to an minimum, which is comparable to the requirement of proportionality or necessity[66] in CJEU case law.

It remains unclear if principals, such as transparency and accountability, are somehow applicable; time will tell if legislative measures, in this sense, will be taken or judicial decisions arise. Even though, the Canadian legal framework does not necessarily reflect all possible guarantees for data retention discussed in the

[63]R. v. Rogers Communications, 2016 ONSC 70. Available at: `https://www.canlii.org/en/on/onsc/doc/2016/2016onsc70/2016onsc70.html`, visited on 29th April 2019.

[64]Ryan, "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights", p. 19.

[65]R. v. Rogers Communications, 2016 ONSC 70, para. 65.

[66]Ryan, "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights", pp. 20-21.

European Union (see *supra* 2.2), data retention is treated as a sensitive topic in Canadian case law.

Chapter 4

Conclusion

4.1 Answers to the Research Questions

How is data retention and access to retained data shaped and conditioned by the jurisprudence of the Court of Justice of the European Union?

The Court of Justice of the European Union strictly reviewed the Data Retention Directive in *Digital Rights Ireland*. It found that the Directive is in breach of the Charter of Fundamental Rights of the European Union, especially article 7 and 8: the rights to respect for private and family life and protection of personal data. Hence, the Directive was declared invalid. Two years later in *Tele2* the Court concluded that *national* legislation with similar traits is not compatible with European Union Law neither.

Both decision make a distinction between data retention and access to this retained data. Even so, both constitute an interference with the rights concerned. On one hand, the retention of data without any differentiation, «general and indiscriminate», is not proportional. It exposes the population to «constant surveillance» because there is no objective link between a suspicious criminal activity and the retention of telecommunication data. On the other hand, access and storage did not fulfil necessary safeguards: a prior judicial (or independent) authorisation is necessary for access, data must be stored with particularly high security measures, in the European Union, and the access conditions should be clearly identified by law.

The CJEU does not rule out data retention in general, but, taking into account both cases, it sets important limitations in order to protect fundamental rights at stake.

In *Ministerio Fiscal* the CJEU finds that access to retained data might be possible even for ordinary criminal offences, if the data access by law enforcement is not considered to be a serious interference with fundamental rights. This leaves the door open for extending the initial purpose of data retention, the investigation of serious crimes, to all criminal offences.

Beyond the jurisprudence of the Court of Justice of the European Union and the applicable legal framework: which options and models for data retention and access are plausible?

The current legislation in force which is directly focussed on data retention in the European Union is only one article of the 2002 Privacy and Electronic Communications Directive. This regulation is completed by the GDPR and the principles defined therein. It is argued that these principles should at least inform new legislation and the relevant legal framework on data retention.

In order to design a data retention scheme in line with the CJEU case law, some initial considerations are necessary. Firstly, data retention should be targeted and not general. This targeted retention has to be justified by an objective reason, such as a suspicion.

Secondly, law enforcement authorities and telecommunication service providers should be able to demonstrate accountability regarding the processing of the retained data. This is necessary so as to assist a judicial (or independent administrative) institution with its decision in regard to the authorisation of a targeted data retention measure or, as the case may be, access to the data retained. Also, the individuals affected of data retention shall be notified by the authorities; if necessary they can seek legal remedies regarding their surveillance. This provides for a three-step system in which law enforcement and communication service providers cooperate with judicial and/or administrative institutions in order to make informed decisions.

Thirdly, data should be retained according to a time period set individually in each case. Legislation should provide for maximum, in any case. Further, communication service providers should be obliged to permanently delete the stored data.

Finally, legislation should be understandable, precise and as comprehensive as possible, in order to ensure legal security. Also, an objective criteria should be required for any retention measure to be ordered and for soliciting access to data.

Data preservation is a practical solution that would satisfy some of the points stated beforehand. Communication service providers would retain data only if they are ordered to do so by law enforcement on an individual basis. It is, therefore, a form of targeted retention upon suspicion, which together with additional guarantees, such as access logs, may well adapt to the CJEU case law requirements. As critical aspects, questions regarding the access to the stored data and its security

remain important.

Have any of the suggested options for question two or any alternative system proved anywhere to fulfil the principle of proportionality and to respect fundamental rights?

As a result of the jurisdictions and the corresponding legislations discussed, two data retention systems could be described as flawed. Whereas, two are more balanced, rather proportional and respectful of fundamental rights.

The United States and the Australian data retention system would not comply with the standards set out earlier. In the case of Australia the answer is straightforward, because the data retention system in place is of a general nature and facilitates law enforcement access to the retained data without any judicial oversight. Furthermore, the case of Australia gives us good reasons to design logically connected guarantees which complement each other, because even journalists, especially protected by the Australian legislation, had their data retained and accessed without the necessary warrants. Regarding the situation in the United States it must be said that the regulation does not provide a high level of legal security. This is so because different *statutes* may be applicable to traffic data retention, differentiating, i.e., international and internal scenarios; moreover, as a consequence of anti-terrorism legislation extensive surveillance programs (of content and traffic data) have been establish, even though their legality is unclear. This scattered legislation does not provide for sufficient legal security; additionally, some surveillance measures carried out in the United States would most probably be illegal under European Union laws.

The Canadian and the Austrian approach to data retention seem to be more respectful of fundamental rights. In the case of Canada, it has to be said that no comprehensive legal regulation exists, but this void is partially filled with the resulting case law from the constitutional protection of privacy. Obtaining subscriber information of the client of a telecommunication service provider requires a judicial warrant under the Canadian Constitution; an intrusion in the private sphere of an individual should then be reduced to a minimum and practical guidance is given on how to reduce the impact of such an intrusion in specific cases. Data retention and privacy are treated as sensitive topics, although questions regarding additional guarantees remain to be answered. The Austrian approach is directly linked to

the CJEU case law and the applicable legislation provides for a data preservation system: data must be retained by a telecommunication service provider once an corresponding order has been issued by law enforcement. This order may be granted for the investigation of determined wilfully committed criminal offences and data can be stored for up to twelve months. A judicial warrant is necessary for access to the data by law enforcement. The most critical point is the posterior usage of the retained data as this usage is not necessary limited to the initial suspicion. Therefore, this data may be (re)-used in another context, unlinked to the initial reason of the retention.

4.2 Questions for the Future

Important questions remain to be answered in the future regarding data retention. They might as well be considered in a broader context, especially taking into account the influence of new technological solutions for the investigations of criminal offences.

Telecommunication data retention is only one of many forms of data retention: Other schemes operate in the European Union, for example the passenger name record (PNR) data directive. It is probable that the findings in relation with telecommunication data might be valuable for the study of these retention schemes. In any case, future investigation on other data retention schemes is necessary in order to assess them regarding their proportionality.

Another important task would be to study the purpose limitation of data retention. If it was initially conceived for the fight against serious criminal offences, this initial purpose may have become less relevant after the *Ministerio Fiscal* decision. Therefore, the modification of the purpose of retention measures should be followed up on. Possible *mission creeps* of technological investigation tools have, most probably, a big repercussion for fundamental rights.

Moreover, from a comprehensive perspective, it should be further explored if and how access to sensitive telecommunication data by law enforcement affects data retained for private purposes, such as billing or advertisement. In other words, if any data retention regulation may also be applicable to data withheld in accordance with a contractual agreement between private parties or if this data is available to

law enforcement in other ways. In light of the foregoing the international access to data stored by private companies in other states and/or jurisdictions may be an interesting issue.

Finally, the future ePrivacy regulation of the European Union, still not approved of at the time of writing, may change the applicable legal framework. It is, in this sense, important to evaluate the modifications that this regulation may, eventually, bring about. Considering this possible impact, the influence and applicability of the GDPR should also be reconsidered.

Acknowledgements

I would like to thank Antoni Roig Batalla for his professional advice and encouragement during the elaboration of this thesis. He provided me with many helpful suggestions and ideas that contributed to the final result and he dedicated much of his time to clarify my doubts.

Raphaela Stadtmann and Sofija Mecinaj advised and assisted me in order to find relevant Austrian legal articles.

References

Legal Documents

[1] Charter of Fundamental Rights of the European Union. Available at: https://data.europa.eu/eli/treaty/char_2012/oj, visited on 1st February 2019.

[2] Constitution Act, 1982. Available at: https://laws-lois.justice.gc.ca/eng/Const/page-15.html, visited on 26th April 2019.

[3] Constitution of the United States. Available at: https://www.senate.gov/civics/constitution_item/constitution.htm, visited on 3rd November 2018.

[4] Convention on Cybercrime (Budapest Convention). Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, visited on 7th April 2019.

[5] Directive 2002/58/EC of the European Parliament and of the Council. Available at: https://data.europa.eu/eli/dir/2002/58/oj, visited on 1st February 2019.

[6] Directive 2006/24/EC of the European Parliament and of the Council. Available at: https://data.europa.eu/eli/dir/2006/24/oj, visited on 1st February 2019.

[7] Directive 95/46/EC of the European Parliament and of the Council. Available at: https://data.europa.eu/eli/dir/1995/46/oj, visited on 1st February 2019.

[8] Directive (EU) 2016/680 of the European Parliament and of the Council. Available at: http://data.europa.eu/eli/dir/2016/680/oj, visited on 14th April 2019.

[9] European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms). Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765, visited on 1st February 2019.

[10] Judgement of the Court (Grand Chamber) of 10 February 2009, *Ireland v European Parliament and Council of the EU*, C-301/06. ECLI:EU:C:2009:68.

[11] Judgement of the Court (Grand Chamber) of 2 October 2018, *Ministerio Fiscal*, C-207/16. ECLI:EU:C:2018:788.

[12] Judgement of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15. ECLI:EU:C:2016:970.

[13] Judgement of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12. ECLI:EU:C:2014:238.

[14] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Available at: https://boe.es/buscar/act.php?id=BOE-A-2007-18243, visited on 23rd February 2019.

[15] R. v. Rogers Communications, 2016 ONSC 70. Available at: https://www.canlii.org/en/on/onsc/doc/2016/2016onsc70/2016onsc70.html, visited on 29th April 2019.

[16] R. v. Spencer, 2014 SCC 43. Available at: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do?r=AAAAAQAHc3BlbmNlcgE, visited on 29th April 2019.

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://data.europa.eu/eli/reg/2016/679/oj, visited on 1st February 2019.

[18] Strafprozeßordnung 1975 (StPO). Available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326, visited on 25th April 2019.

[19] Verfassungsgerichtshof, 27th June 2014, G47/2012. Available at: https://www.vfgh.gv.at/downloads/VfGH_G_47-2012_ua_VDS_schriftliche_Entscheidung.pdf, visited on 25th April 2019.

Bibliography

[1] Adensamer, Angelika and Hanel, Alina (2018). "Das Überwachungspaket im Überblick". In: *juridikum* 3, pp. 292–302. ISSN: 2309-7477.

[2] Article 29 Data Protection Working Party (2005). *Opinion 4/2005*. Available at: https://ec.europa.eu/justice/article-29/documentation/

opinion-recommendation/index_en.htm#maincontentSec13, visited on 7th April 2019.

[3] Bignami, Francesca (2007a). "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". In: *Bosten College Law Review* 48 (3), pp. 609–698. Available at: https://lawdigitalcommons.bc.edu/bclr/vol48/iss3/3/, visited on 26th April 2019.

[4] Bignami, Francesca (2007b). "Privacy and Law Enforcement in the European Union: The Data Retention Directive". In: *Chicago Journal of International Law* 8 (1), pp. 233–255. Available at: https://ssrn.com/abstract=955261, visited on 27th November 2018.

[5] Directorate-General for Migration and Home Affairs (European Commission) and Centre for Strategy and Evaluation Services (CSES) (2013). *Evidence of potential impacts of options for revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries*. Available at: https://publications.europa.eu/en/publication-detail/-/publication/5dc1b779-1a1c-4e53-a17f-1fd0fe71e4ad, visited on 7th April 2019.

[6] European Commission (2011). *Report from the Commission to the Council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52011DC0225, visited on 7th April 2019.

[7] European Data Protection Supervisor (2011). *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*. Available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52011XX0923(01), visited on 7th April 2019.

[8] Fabbrini, Federico (2015a). "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States". In: *Harvard Human Rights Journal* 28, pp. 65–95. Available at: https://harvardhrj.com/wp-content/uploads/sites/14/2009/09/human-rights-in-the-digital-age.pdf, visited on 10th May 2019.

[9] Fabbrini, Federico (2015b). "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court". In: *iCourts Working Paper Series* 19, pp. 1–23. Available at: https://ssrn.com/abstract=2576214, visited on 13th April 2019.

[10] Fennelly, David (2018). "Data retention: the life, death and afterlife of a directive". In: *ERA Forum*. ISSN: 1863-9038. Available at: https://doi.org/10.1007/s12027-018-0516-5, visited on 27th November 2018.

[11] Fura, Elisabet and Klamberg, Mark (2012). "The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA". In: *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights*. Ed. by Casadevall, Josep, Myjer, Egbert and O'Boyle, Michael. Oisterwijk: Wolf Legal Publishers, pp. 463–481. Available at: https://ssrn.com/abstract=2169894, visited on 27th November 2018.

[12] González Pascual, Maribel (2014). "El TJUE como garante de los Derechos en la UE a la luz de la sentencia Digital Rights Ireland". In: *Revista de Derecho Comunitario Europeo* 49, pp. 943–971. ISSN: 1138-4026. Available at: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=1336&IDA=37257, visited on 27th March 2019.

[13] Guild, Elspeth and Carrera, Sergio (2014). "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive". In: *CEPS Liberty and Security in Europe Papers* 65, pp. 1–15. Available at: https://ssrn.com/abstract=2445901, visited on 26th April 2019.

[14] Maeztu, David (2018). *El Tribunal de Justicia y la conservación de datos, sentencia "Ministerio Fiscal"*. Available at: https://www.derechoynormas.com/2018/10/el-tribunal-de-justicia-y-la.html, visited on 23rd February 2019.

[15] Meares, Michelle (2018). "Mass Surveillance and Data Retention in Australia: Balancing Rights and Freedoms". In: *Journal of Internet Law* 21 (10), pp. 3–6. ISSN: 1094-2904.

[16] Møller Pedersen, Anja, Udsen, Henrik and Sandfeld Jakobsen, Søren (2018). "Data retention in Europe—the Tele 2 case and beyond". In: *International*

Data Privacy Law 8 (2), pp. 160–174. Available at: http://dx.doi.org/10.1093/idpl/ipx026, visited on 27th November 2018.

[17] *Opinion of Mr Advocate General Cruz Villalón delivered on 12 December 2013, Digital Rights Ireland, C-293/12 and C-594/12*. ECLI:EU:C:2013:845. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1556207084604&uri=CELEX:62012CC0293, visited on 25th April 2019.

[18] Penney, Steven (2014). "The Digitization of Section 8 of the Charter: Reform or Revolution?" In: *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 67, pp. 505–534. Available at: https://digitalcommons.osgoode.yorku.ca/sclr/vol67/iss1/16/, visited on 29th April 2019.

[19] Rodríguez Lainz, José Luis (2018). "El Régimen Legal español en materia de conservación y cesión de datos para la investigación de delitos. Comentario a la sentencia del TJUE de 2 de febrero de 2018". In: *Diario La Ley* 9291.

[20] Rom, Brigitte (2018). "Neuerungen im Strafverfahren - das Strafprozessrechtsänderungsgesetz 2018". In: *Österreichische Juristen-Zeitung* 17, pp. 762–769. ISSN: 0029-9251.

[21] Ryan, Michael (2016). "Persona non data: How the Courts in the EU, UK and Canada are addressing the issue of communications data surveillance vs. privacy rights". In: *TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016*. Available at: http://dx.doi.org/10.2139/ssrn.2742057, visited on 7th April 2019.

[22] Sarre, Rick (2017). "Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia". In: *Asian Journal of Criminology* 12 (3), pp. 167–179. ISSN: 1871-014X. Available at: https://doi.org/10.1007/s11417-017-9256-7, visited on 27th November 2018.

[23] Vedaschi, Arianna and Lubello, Valerio (2015). "Data Retention and its Implications for the Fundamental Right to Privacy". In: *Tilburg Law Review* 20 (1), pp. 14–34. Available at: http://booksandjournals.brillonline.com/content/journals/10.1163/22112596-02001005, visited on 27th November 2018.