Data Retention in Portugal: Big Brother is (No Longer) Watching

FRANCISCO PEREIRA COUTINHO*

Abstract: The law implementing the most privacy-invasive instrument ever adopted by the European Union was enforced in the Portuguese legal order until the Portuguese Constitutional Court ruled otherwise on 19 April 2022. The general and indiscriminate retention of data by providers of electronic communications services, and subsequent access thereto by public authorities, was allowed to continue for eight years after the landmark *Digital Rights Ireland* ruling of the Court of Justice that annulled the contentious Data Retention Directive. This article traces this massive breach of the fundamental rights of almost the entire Portuguese population back to a systemic failure of all relevant national stakeholders in the executive, legislative and judicial branches.

Keywords: data retention; privacy; data protection; terrorism; Portuguese Constitutional Court.

Introduction

The usually placid waters of the Portuguese legal order were shaken in mid-April 2022 by a judicial ruling with the potential to trigger a tsunami of criminal conviction reversals that is already provoking a backlash in the investigation and repression of serious criminal offences committed online (Caixinha, 2022). Several provisions of the so-called "Data Retention Law" (Law 32/2008), originally adopted to transpose the contentious "Data Retention Directive" (Directive 2006/24/EC), were declared unconstitutional by the Portuguese Constitutional Court (PCC), as they breach the rights to privacy, data protection and to an effective legal remedy, as interpreted in accordance with the Charter of Fundamental Rights of the European Union ("Charter")[1].

* Associate Professor at NOVA School of Law (Faculdade de Direito da Universidade Nova de Lisboa). Member of CEDIS – I & D Research Center for Law and Society. The analysis of the PCC's case law on data retention develops an article published in *Diritti Comparati* (Francisco Pereira Coutinho, 2022). All websites accessed on 1 August 2022. Direct quotes from doctrinal, legal and judicial sources in Portuguese were translated by the author. Judicial rulings referred to with no indication of source should be presumed to have originated from the Court of Justice (of the European Union). I would like to thank Graça Canto Moniz, Mateus Correia de Carvalho, Marta Marinho and Teresa Violante for their comments and bibliographical suggestions. The usual disclaimers apply.

[1] Decision 268/2022, 828/19, 19 April 2022.

Electronic copy available at: https://ssrn.com/abstract=4216870

The ruling caused shockwaves across the political spectrum and triggered a constitutional crisis (of sorts) (Mota Delgado, 2022) (Violante, 2022), with both the President of the Republic (Carmo, 2022a) and the Prime Minister (Carmo, 2022b) hinting on media outlets at the need for a mooted constitutional amendment in a field pre-empted by EU law. The Attorney-General went as far as to request the annulment of the ruling (Gustavo, 2022), an unprecedented claim promptly dismissed by the PCC on procedural and material grounds[2].

Eight years into the data retention saga, initiated with the landmark *Digital Rights Ireland* ruling of the Court of Justice that annulled the Data Retention Directive[3], this article seeks to ascertain why it took so long to remove this national law, which stemmed from what was once accurately described as the "the most privacy-invasive instrument ever adopted by the EU in terms of scale and the number of people it affects" (European Data Protection Supervisor, 2010), from the statute book. I will begin by discussing the impact that a general and indiscriminate (blanket) retention of metadata has on fundamental rights (section one), which will be followed by an analysis of the relevance of metadata for law enforcement and intelligence authorities (section two). My attention will then shift to an analysis of the lifespan of the Data Retention Directive, from its conception to its demise, and further attempts at resurrection in light of the case law of the Court of Justice (section three). I will finish by addressing how the implementation of the Data Retention Directive unfolded in the Portuguese legal order, focusing on the behaviour of key stakeholders in the legislative, executive, and judicial branches (section four).

1. A CCTV camera for inside one's head

Metadata are "data about data". In the context of electronic communications services in the EU, they refer to data generated by natural persons ("data subjects") through the use of landline phones, fax, mobile phones and the internet, namely traffic data – i.e. "data processed for the purpose of the conveyance of a communication on

[2] Decision 382/2022, 828/19, 13 May 2022.
[3] C-293/12 and C-594/12, 8 April 2014, ECLI:EU:C:2014:238.

Electronic copy available at: https://ssrn.com/abstract=4216870

an electronic communications network or for the billing thereof" – and location data – i.e. "data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service" [Article 2(b)(c) of the "E-privacy Directive" (Directive 2002/58/EC)][4]. They include, *inter alia*, calling telephone numbers, numbers called, as well as web (URL), IP and email addresses.

Metadata are personal data whenever they can be used to trace and identify persons involved in electronic communications[5]. If that is the case, they can only be collected for specified, explicit and legitimate purposes (purpose limitation principle) (Article 5 (1)(b) GDPR) and must be kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation principle) (Article 5 (1)(e) GDPR). Except when technically necessary for the conveyance of a communication, their storage and access by providers of publicly available electronic communications services or of public communications networks ("service providers") is in principle prohibited without the consent of the data subjects concerned (confidentiality of communications principle) (Article 5 of the E-privacy Directive). Retention of traffic data is allowed solely for billing (i.e. for the benefit of the data subject/consumer) or for marketing purposes (when the data subject has given consent) (Article 6 of the E-privacy Directive), while location data "may only be processed when they are made anonymous, or with the consent of the users or subscribers (of electronic communication systems) to the extent and for the duration necessary for the provision of a value-added service" (Article 9 of the E-privacy Directive). In other words, unless consent is given by the data subject,

[4] The following definition of "electronic communication metadata" is included in Article 3(4)(c) of the proposal for an "E-privacy Regulation" (COM/2017/010 final): "(D)ata processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication".

[5] Discovering whether metadata are personal data is often tricky. In *Breyer,* C-582/14, 19 October 2016, ECLI:EU:C:2016:779, §49, a dynamic IP address was considered personal data when registered by an online media service provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person. According to Article 4(1) of the General Data Protection Regulation ("GDPR") (Regulation (EU) 2016/679) "personal data means any information relating to an identified or identifiable natural person". An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier.

Electronic copy available at: https://ssrn.com/abstract=4216870

metadata must be erased or anonymised by service providers after they are no longer needed for interconnection or billing purposes[6].

Legal safeguards limiting data retention are necessary because metadata, taken as a whole, can tell you a lot about a person's private life. Who has that person been in touch with, and how often? Where is she and where has she been? What are her interests and habits? Metadata retention is like having a CCTV (Close-Circuit Television) camera installed inside one´s head (Bowden, 2010:4). As smartphones became ubiquitous – 84% of the Portuguese population had one in 2020[7] –, the compilation of a detailed profile of almost the entire population is no longer in the realm of sci-fi[8].

It is thus simply wrong to disregard the privacy-encroaching potential of metadata *vis-à-vis* content data and classify the interference with fundamental rights stemming from data retention as "very low" (Bacelar Gouveia, 2022). A general and indiscriminate retention of metadata by service providers – and its further access by law enforcement and intelligence agencies – entails a particularly serious interference with the right to privacy and the other rights (e.g. respect for communications) laid down in Article 7 of the Charter, and also with the right to data protection enshrined in Article 8 of the Charter[9]. Furthermore, the mere knowledge that data are being retained and may

[6] *Tele*2 *Sverige*, C-203/15 and C-698/15, 21 December 2016, ECLI:EU:C:2016:970, §86. According to the Article 29 Data Protection Working Party (2003: §§2.6.-2.8. and 4.2), the principle of proportionality requires that, in the cases where the bill has been paid by the data subject/consumer and is not being challenged, the storage period of metadata should have a maximum duration of three to six months, and can only include traffic data that are adequate, relevant and not excessive for billing purposes. This implies that if there is no billing for certain types of communications, the corresponding metadata cannot be retained. In the Portuguese legal order, the six-month limitation period for electronic communication billings enshrined in Article 10 (1) of Law 23/96, concerning public services, sets the outside temporal limit during which data may be stored by service providers when a bill is not being challenged or payment is not pursued.

[7] See https://www.marktest.com/wap/a/n/id~2700.aspx.

[8] See *Digital Rights Ireland*, C-293/12 and C-594/12, cit., para. 27 ("(Metadata) (…) 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"), and *Quadrature du Net*, C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791, § 117 ("(Metadata) may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health").

[9] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §§ 32-37, and *Tele*2 *Sverige*, C-203/15 and C-698/15, cit., §100.

Electronic copy available at: https://ssrn.com/abstract=4216870

subsequently be used to establish patterns of individuals' behaviour without the data subjects being informed has a "chilling effect" on the exercise of other fundamental rights[10]. Not only is people's willingness to gather together in support of common beliefs on political, religious, cultural and other matters curtailed, but free speech is also deterred, which is particularly problematic for whistle-blowers and for persons whose communications are subject to obligations of professional secrecy[11]. The effects of even a "vague"[12] or "diffuse"[13] feeling of constant surveillance may arguably be considered as an interference with the constitutional rights to freedom of expression (Article 11 of the Charter) and to freedom of association (Article 12 of the Charter).

2. Big Brother is watching

The potential relevance of the swarm of metadata generated by the dissemination of electronic communications in the unravelling of serious crime, and particularly for detecting and dismantling terrorist and organised crime networks, has not gone unnoticed[14]. Law enforcement and intelligence authorities soon realised that, besides trawling metadata to identify potential criminals, they could very easily "delve into the past" of any citizen by examining metadata tracing the history of communications made by persons well before they were suspected of being connected with a felony. Since access required storage, two models of data retention programmes were lawfully pursued[15]. The most problematic, considering the prohibition of

[10] The "chilling effect" doctrine on the exercise of fundamental rights was recognised by the European Court of Human Rights in *Altuğ Taner Akçam v. Turkey*, 27520/07, 25 October 2011, §81 (freedom of expression) and by the United States Supreme Court in *NAACP v. Alabama*, 357 U.S. 499 (1958), at 462 (freedom of association).

[11] *Quadrature du Net*, C-511/18, C-512/18 and C-520/18, cit., § 118.

[12] Opinion of Advocate General Cruz Villalón delivered on 12 December 2013, *Digital Rights Ireland*, 8 April 2014, C-293/12 and C-594/12, ECLI:EU:C:2013:845, §§ 52 and 72.

[13] German Federal Constitutional Court, *Data Retention,* 2 March 2010, 1 BvR 256/08, 263/08, and 586/08, *BVerfGE* 125, at 260, §212.

[14] See Council of the European Union (2002a, §5): "(B)ecause of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications is now a particularly important and useful tool in the investigation and prosecution of crime, in particular organised crime".

[15] I will not deal with the unlawful programmes for mass surveillance of personal data developed by Western intelligence agencies revealed after the Snowden scandal. For a thorough assessment of those surveillance practices in some Member States, see Bigo et al. (2013).

Electronic copy available at: https://ssrn.com/abstract=4216870

unfettered large-scale exploratory or general surveillance[16], was the "telephone record programme" developed in the United States of America by the National Security Agency under Section 215 of the "Patriot Act" (2001). The programme was based on the unrestricted collection from telecommunication operators ("telcos") of metadata covering five years of telephone calls made by whole of the American population, and the subsequent trawling of that metadata for terrorist suspects (Privacy and Civil Liberties Oversight Board, 2014: 8-10)[17]. The other model avoided the costs of building large State-run data storage facilities by simply providing public authorities with access on a case-by-case basis to metadata collected and retained by service providers, while at the same time obliging the latter to screen their networks in search of links that might constitute a terrorist threat[18].

In the EU, Article 14(1) of the "Telecommunication Privacy Directive" (Directive 97/66/EC) already allowed for restrictions to the principle of confidentiality resulting from proportional measures aimed at safeguarding national security and/or the enforcement of criminal law. However, the explicit green light for the adoption of national data retention programmes preventing the deletion of data no longer needed for billing purposes, and also obliging service providers to transmit that data, giving the public authorities access to it and/or screening metadata on behalf of the authorities, was given by the so-called "data retention amendment" introduced in Article 15 (1) of the E-privacy Directive.

The E-privacy "data retention amendment", which states that Member States "may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period", was adopted in the aftermath of the terrorist attacks in the United States of America on 11 September 2001. Its origin relates directly to a Council meeting of 20 September 2001 that mandated the Commission "to submit proposals for ensuring that law enforcement authorities are able to investigate criminal acts involving the use

[16] European Court of Human Rights, *Klass and Others v. Germany*, 5029/71, 6 September 1978, §51.

[17] This data retention programme was restricted by the US Congress in 2015 ("Freedom Act") and, particularly, in 2020 ("Safeguarding American's Private Records Act").

[18] See Article L. 851-3 (I) of the French Internal Security Code: "(F)or the sole purpose of preventing terrorism, (telcos and ISPs) may be required to implement on their networks automated data processing practices designed (…) to detect links that might constitute a terrorist threat".

Electronic copy available at: https://ssrn.com/abstract=4216870

of electronic communications systems and to take legal measures against their perpetrators" (Council of the European Union, 2001: §4), and to the implementation of the international obligation stemming from the Security Council's Resolution 1373 adopted a week later, which requires States to "take the necessary steps to prevent the commission of terrorist attacks" (Security Council, 2001: §2(b)).

Terrorism became the trump card to restrict fundamental rights by obliging service providers to store metadata for periods longer than needed for technical or commercial purposes, so that public authorities could be granted access to them[19]. Mandatory blanket retention of metadata was adopted mainly, but by no means exclusively, as a counterterrorism measure in Belgium (retention for one year), the Czech Republic (one year), Denmark (one year), Luxembourg (one year), France (one year), Ireland (three years), Italy (up to four years) and Spain (one year)[20].

Securitization gained decisive traction after mass terrorism arrived in Europe with the Atocha train station bombing attacks that killed 193 people on 11 March 2004 in Madrid (Ray, 2022a). "Deeply shocked", the European Council declared that acts of terrorism were attacks against the values on which the Union is founded, and further instructed the Council to establish common rules on the retention of metadata by service providers (European Council, 2004: 4). One month later, France, Ireland, Sweden and the United Kingdom submitted a proposal for a framework decision that foresaw the blanket storing of metadata between 12 and 36 months "to meet the needs of the security, intelligence and law enforcement agencies in the fight against modern

[19] *Ireland v Parliament and Council*, C-301/06, 10 February 2009, ECLI:EU:C:2009:68, § 67: "The evidence submitted to the Court confirms that, following the terrorist attacks [of 11 September 2001 in New York (United States), 11 March 2004 in Madrid (Spain) and 7 July 2005 in London (United Kingdom)], several Member States, realising that data relating to electronic communications constitute an effective means for the detection and prevention of crimes, including terrorism, adopted measures pursuant to Article 15(1) of Directive 2002/58 with a view to imposing obligations on service providers concerning the retention of such data".

[20] See, respectively, Article 14 of the Law on Cybercrime, of 28 November 2000 (Belgium), Act 127/2005 (Electronic Communications Act) (Czech Republic), Act 378 of 6 June 2002 (Anti-Terrorism Act), which extended the scope of Section 786 of the Administration of Justice Act (Denmark), Privacy and Electronic Communications Act, of 30 May 2005 (Luxembourg), Article 29 of the Law on Everyday Security, of 15 November 2001 (France), Secret direction of the Irish Government of April 2002 adopted under Section 110(1) of the Postal and Telecommunications Services Act, 1983 (Ireland), Section 132 of the Data Protection Code (Decree-Law of 30 June 2003, 196) (Italy), and Article 12(1) of the Information Society and Electronic Services Law (Law 34/2002) (Spain).

Electronic copy available at: https://ssrn.com/abstract=4216870

criminals including terrorists" (Council of the European Union, 2004a: 6). The proposal was particularly relevant for the British and Irish Governments, which were struggling to gain Parliamentary approval for legislation requiring service providers to retain data (McIntyre, 2008: 329-330) (Jones and Hayes, 2013:10).

In addition to avoiding national parliaments, a "third-pillar" framework decision under Title VI of the EU Treaty also allowed national governments to bypass the will of the European Parliament, although this body did have to be consulted. Not surprisingly, given the emphatic stance it took on 6 September 2001 that "a general data retention principle must be forbidden" (European Parliament, 2001: §I), the European Parliament rejected the legislative initiative (European Parliament, 2005a), endorsing the report of the Committee on Civil Liberties, Justice and Home Affairs, which questioned the proportionality of blanket data retention and the legal basis chosen by the Council to pursue it (European Parliament, 2005b). The argument that regulating obligations imposed on service providers necessarily fall within European Community competence and, therefore, had to be approved by the Council in tandem with the European Parliament, based on a Commission proposal for a directive, was also supported by the Council's own legal service (Legal Service of the Council of the European Union, 2005), and eventually led to the data retention framework proposal being abandoned[21].

EU-wide blanket data retention would possibly have reached a political dead-end had it not been for the terrorist attacks that killed 56 people in London on 7 July 2005 (Ray, 2022b). The United Kingdom held the Presidency of the Council at the time and used the attacks as a justification for the urgent adoption of the directive on data retention proposed by the Commission on 21 September 2005 (Jones and Hayes, 2013: 9). The Council's call was quickly answered by the European Parliament, which adopted the proposal on 14 December 2005 in a single reading (European Parliament, 2005c). Responsiveness to the public's growing security concerns probably explain the European Parliament's transformation into a "responsible legislator" (Servant, 2013: 982) at the expense of "selling out" its traditional civil liberties principles regarding data protection (Peers, 2005: 7-8). The fastest legislative procedure in the history of the EU ended on 15

[21] See the minutes of the 12 October 2005 meeting of the Council of the European Union (2005), where a majority of delegations expressed their openness to the idea of adopting a directive on data retention.

Electronic copy available at: https://ssrn.com/abstract=4216870

March 2006 (Hornung and Schnabel, 2009: 120), following the Council's qualified majority approval, with Ireland and the Slovakia voting against (Council of the European Union, 2006a: 4).

3. Lifetime of the most privacy-invasive legislative instrument ever adopted by the EU

3.1. A securitarian DNA that reflects a controversial conception and birth

The European legislator justified the compression of fundamental rights arising from data retention with the overarching threat to public and national security posed by terrorism:

> "Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 (right to privacy) of the (European Convention of Human Rights) is therefore a necessary measure" (Recital 9 of the Data Retention Directive).

The idea that data retention is a *necessary* and *effective* counterterrorism law enforcement instrument is at best wishful thinking. An official report from 2014 on the pervasive NSA telephone metadata retention programme found not "a single instance involving a threat to the United States in which the (…) program made a concrete difference in the outcome of a counterterrorism investigation", or "an instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack" (Privacy and Civil Liberties Oversight Board, 2014: 146). In *Tele 2 Sverige*, the most persuasive evidence in this regard provided to the Court of Justice was the statement from the French Government that access to the communications data of the persons involved in the terrorist attacks of 2015 in France

Electronic copy available at: https://ssrn.com/abstract=4216870

was “extremely useful” in discovering the authors of those attacks and their accomplices[22].

The Data Retention Directive was clearly the offspring of a securitarian zeitgeist. After stating the overall importance of metadata “for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States” (Recital 11)[23], the Directive determined that metadata should be available to law enforcement authorities dealing with “serious crime” (Article 1 (1)). Purpose creep naturally ensued, with several Member States failing to elaborate on the concept or allowing data to be accessed and used to prevent and combat crime generally or for national security purposes (European Commission, 2011: 6 and 8), thereby ignoring the Council’s urge for Member States to have due regard to the crimes listed in Article 2(2) of the Framework Decision on the European Arrest Warrant and crime involving telecommunication (Council of the European Union, 2006b: 2).

Service providers were to be obliged to collect and store metadata necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify the users’ communication equipment, and to establish the location of mobile communication equipment (Article 5 of the Data Retention Directive). The retention could not cover content data of electronic communications, including information consulted using an electronic communications network (Article 1 (2) *in fine* of the Data Retention Directive). Member States were given leeway to decide on whether to reimburse storage costs and to set the length of the retention period within a temporal window of six months to two years (Article 6 of the Data Retention Directive). Access to data or the use thereof by the police

[22] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 July 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:572, §183.

[23] This statement convinced neither the Article 29 Data Protection Working Party (2005: 5-6), which considered that the necessity for “unprecedented, continued, pervasive monitoring of all kinds of communication and movement of the totality of citizens in their daily life” was not based on “crystal-clear evidence”, nor the European Data Protection Supervisor (2011: §75), which advised the Commission to “invest in collecting further practical evidence from the Member States in order to demonstrate the necessity of data retention as a measure under EU law” before presenting a revised version of the Directive. This debate is still not settled, with a comparative statistical study of the European Parliament requested by a Pirate Party MEP finding in January 2020 no direct impact of data retention on crime clearance rates across Member States (European Parliament Research Service, 2020: 3).

Electronic copy available at: https://ssrn.com/abstract=4216870

or judicial authorities was also left to be defined by national law (Recital 25 and Article 4 of the Data Retention Directive), which had also to ensure service providers' respect for data security[24].

Preventive blanket data retention had long been pursued by law enforcement and intelligence agencies as an alternative to the less intrusive targeted surveillance of data preservation ("quick freeze") – i.e. the conservation of specific data relating to specified individuals in certain cases. "Quick freeze" was considered insufficient to trace the source of illegal content, such as racist and xenophobic material and child pornography or the source of attacks against information systems, or to identify those involved in using electronic communications networks for the purpose of organised crime and terrorism (Council of the European Union, 2004b: Recitals 5 and 6). While data preservation allows access to metadata generated by communications made *after* someone has been identified as a suspect of a crime, with data retention law enforcement authorities can go "back in time" (European Commission, 2015: 12) by examining metadata generated by someone *before* that person has been identified as being potentially connected, even indirectly or remotely, with a crime[25]. According to the Cybercrime Office of the Portuguese Public Prosecution Service (2015: 4), this is the reason why:

> "(D)ata retention must be indiscriminate, on the one hand, and include every citizen, on the other. When data are collected and retained it is not possible to know if they may be needed in the future as evidence of a crime. Only after a crime has been committed will data previously obtained through general and indiscriminate retention have value as evidence. When there is already a suspect under investigation, other instruments can be used to gather information relating to that person that may be necessary (e.g. the interception of communications). It

[24] Article 7 of the Data Retention Directive, which refers to the following data security principles with respect to data retained: a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network; b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure; c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention. Compliance with data security by service providers had to be supervised by "one or more public authorities" in accordance with Article 9 of the Data Retention Directive.

[25] Opinion of Advocate General Saugmandsgaard Øe, *Tele2 Sverige*, C-203/15 and C-698/15, cit., §§179-180.

Electronic copy available at: https://ssrn.com/abstract=4216870

is precisely when evidence of the facts has not been obtained in advance or a suspect has not been identified that it is useful to access retained data– the latter may actually be the only means of discovering who committed a particular crime. However, at that moment, such data must have already been retained and stored (all data regarding every citizen). This explains why data retention (…) is only useful if the data regard every citizen, indiscriminately".

3.2. The troubles of infancy

The transposition of the Data Retention Directive proved troublesome, unsurprisingly. The deadline of 15 September 2007 was generally ignored. The European Commission sent letters of formal notice under the 258 TFEU infringement procedure, informing of default and requesting action, to Austria, Bulgaria, Cyprus, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, and Sweden[26]. Reasoned opinions followed on 18 September 2008 targeting Austria, Greece, Ireland, Lithuania, the Netherlands, Poland, Romania, and Sweden[27]. Judicial actions were brought in May and June 2009 against Austria, Greece, Ireland, the Netherlands and Sweden, in August 2010 against Luxembourg, and in July 2012 against Germany[28]. The Court of Justice declared an infringement by Austria, Greece, Ireland, and Sweden[29]. Only Sweden ended up being fined € 3 million, in May 2013[30].

[26] The letters were sent on 27 November 2007 in infringements procedures 2007/1036, 2007/1045, 2007/1051, 2007/1078, 2007/1092, 2007/1071, 2007/1083, 2007/1108, 2007/1116, 2007/1126, 2007/1133, 2007/1139, 2007/1149, 2007/1153, 2007/1159, 2007/1168, 2007/1178, 2007/1187, 2007/1193 and 2007/1181. Formal notices were afterwards sent to Belgium on 16 September 2012 (infringement procedure 2012/2152), to the Czech Republic on 25 November 2011 (infringement procedure 2011/1143), and to Germany on 16 June 2011 (infringement procedure 2011/2091).

[27] Reasoned opinions were afterwards also sent to Belgium (30 May 2013), the Czech Republic (22 March 2012), Germany (27 November 2011 and 22 March 2012), Luxembourg (20 November 2009), and again to Romania (27 October 2011 and 22 March 2012).

[28] In cases C-189/09 (*Commission v Austria*), C-211/09 (*Commission v Greece*), C-202/09 (*Commission v Ireland*), C-192/09 (*Commission v Netherlands*), C-185/09 (*Commission v Sweden*), C-394/10 (*Commission v Luxembourg*), and C-329/12(*Commission v Germany*).

[29] In cases *Commission v Austria*, C-189/09, 29 July 2010, ECLI:EU:C:2010:455, §22, *Commission v Greece*, C-211/09, 26 November 2009, ECLI:EU:C:2009:737, §10, *Commission v Ireland*, C-192/09, 26 November 2009, ECLI:EU:C:2009:736, §14, and *Commission v Sweden*, C-185/09, 4 February 2010, ECLI:EU:C:2010:59, §12.

[30] *Commission v Sweden*, C-270/11, 30 May 2013, ECLI:EU:C:2013:339, §60. On 16 April 2014, the Commissioner Cecilia Mallström pledged in the European Parliament to return the fine to Sweden after

Electronic copy available at: https://ssrn.com/abstract=4216870

Delays in transposition stemmed from staunch political resistance to data retention[31]. Constitutional judicial challenges to national law implementing the directive followed suit in Austria (Anderl and Alona Klammer, 2021: 44-48), Belgium (Van de Heyning, 2021: 61), Bulgaria (Kashumov, 2021: 76-77), Cyprus (Kombos and Laulhé Shaelou, 2019: 1412-1414), the Czech Republic (Polčák, 2021: 104-107), Germany (Albers, 2021: 120-121), Ireland (Fennelly, 2021: 140-141), Poland (Podkowik and Zubik, 2021: 160-162) Romania (Şandru, 2021: 191-198), Slovakia (Gera and Husovec, 2021: 206-209), and Slovenia (Toplak, 2021: 221-222). A couple of judicial decisions stand out.

On 8 October 2009, the Constitutional Court of Romania struck down Law 298/2008 – a.k.a. "Big Brother Law" (Şandru, 2021: 192) – considering that the obligation it imposed on service providers to proceed to an open-ended collection of metadata for law enforcement purposes was a disproportionate infringement of the right to privacy (Article 26 of the Constitution), the right to secrecy of correspondence (Article 28 of the Constitution), and freedom of expression (Article 30(1) of the Constitution) (Zubik, Podkowik and Rybski, 2021). This was tantamount to indirectly declaring the Data Retention Directive itself unconstitutional (Şandru, 2021: 192). The Romanian court unfortunately failed to appropriately qualify the issue at hand as a problem of European constitutional law – i.e. on the compatibility with the Charter of national law implementing EU law (Article 51(1) of the Charter) – that required a request for a preliminary ruling on validity to be submitted to the Court of Justice under Article 267(3) TFEU. Some of the arguments the Constitutional Court of Romania used on the inadmissibility of blanket data retention would, however, resonate years later in Luxembourg. It argued that any obligation to retain data is an exception to the principle of confidentiality of communications. Blanket retention of metadata is inadmissible precisely because it transforms the exception into an absolute rule. Its indiscriminate nature is, moreover, "likely to overturn the presumption of innocence and to transform *a priori* all users of electronic communications services or public communications

the *Digital Rights Ireland* ruling of the Court of Justice invalidating the Data Retention Directive (European Parliament, 2014).

[31] That was the case in Austria (*Commission v Austria*, C-189/09, cit., §4), Germany (Grimm, Wendel and Reinbacher, 2019: 459 and 477), and Sweden (*Commission v Sweden*, C-270/11, cit., §33).

Electronic copy available at: https://ssrn.com/abstract=4216870

networks into persons suspected of committing terrorist offences or serious crimes" (Zubik, Podkowik and Rybski, 2021: 354-355).

A few months later, several provisions of the German data retention legislation received the same fate as the Romanian legislation, in a mass complaint case triggered by around 34,000 citizens at the Federal Constitutional Court. However, unlike their Romanian counterparts, the German judges ruled that the blanket data storage obligation stemming from the Directive was not unconstitutional. It was considered an exceptional but otherwise proportional restriction of fundamental rights. This conclusion was based on the arguments that the preventive retention of data: i) was imposed on multiple private service providers and not on public authorities, which could only retrieve and use the data under strict conditions; ii) did not include the content of telephone conversations and emails or websites visited online; iii) was limited to six months[32]; and iv) was a response to pressing social needs created by the development of new technologies – e.g. the repression of serious criminal offences perpetrated online that would escape detection if metadata were deleted[33]. A preliminary reference to the Court of Justice was not necessary because the Federal Constitutional Court only purported to review national law implementing the directive in respect of matters left to the discretion of the national legislator, namely the level of data security, storage requirements, and the procedures governing access and use of data by public authorities[34]. Given the severe level of encroachment on fundamental rights of the possible use of metadata, which according to the court allows for the creation of meaningful personality and mobility profiles of virtually every citizen[35], the principle of

[32] This was considered a very long storage period "at the upper limit of what (could) be justified from the point of view of proportionality" (*Data Retention*, 2 March 2010, cit., §215 bb)).

[33] *Data Retention*, 2 March 2010, cit., §§213 b), 214 aa), 215 bb), 216 cc) and 218. This conclusion, argues Marion Albers (2021: 126-127), is hardly reconcilable with the prohibition of preventive storage of personal data for indefinite or not yet definable purposes – itself a corollary of the principle of limitation of purpose which requires data to be necessary for the respective purposes – adopted in the *Census* judgment of 15 December 1983 (1 BvR 209/83 et al., *BVerfGE* 65, at 46-47), as it admits the constitutionality of a bulk retention of data that will necessarily determine that a vast majority of the data retained will prove unnecessary.

[34] Articles 4, 7 and 8 of the Data Retention Directive. In *Ireland v Parliament and Council*, C-301/06, cit., §83, the Court of Justice clarified that the aim of the Directive was not to harmonise the issue of access to data by the competent national law enforcement authorities or that relating to the use and exchange of those data between those authorities.

[35] *Data Retention*, 2 March 2010, cit., §211.

Electronic copy available at: https://ssrn.com/abstract=4216870

proportionality in the narrow sense required preventive blanket data retention to follow high standards of data security and to subject data access and use by public authorities to strict procedural and substantive requirements[36] – e.g. the retrieval and transmission of data had to be limited to situations where it was necessary "to ward off dangers to the life, limb or freedom of a person, to the existence or the security of the Federation or of a *Land* or to ward off a danger to public safety"[37], and required, in principle, prior judicial review[38] and prior notification of the data subjects concerned[39]. As neither those standards nor the said requirements were generally met in the German legislation on data retention, the Court declared a breach of the inviolability of the secrecy of telecommunication foreseen in Article 10 of the Basic Law[40].

3.3. Demise

Ireland immediately sought the annulment of the Directive at the Court of Justice, arguing that data retention had to be dealt with under a "third pillar" legal basis where Member States hold veto power[41]. The Luxembourg court rejected the claim considering that the Directive essentially regulated operations of service providers in the internal market independent of the implementation of any police and judicial cooperation in criminal matters, as it harmonised neither the issue of access to data by public authorities nor that relating to the use and exchange of data between authorities[42].

Ireland's annulment request related solely to the choice of legal basis and not to any possible infringement of fundamental rights[43]. The Court of Justice was again able to avoid reviewing a possible interference of data retention with the exercise of

[36] Idem, §§220 and 225-231.

[37] Idem, §231.

[38] Idem §§247 aa) and 249.

[39] Idem, §243 bb).

[40] Idem, §§292.

[41] Ireland contented that the only legal basis on which the measures contained in Directive 2006/24 could be validly founded was Title VI of the EU Treaty ("TEU"), namely Articles 30 TEU, 31(1)(c) TEU and 34(2)(b) TEU (*Ireland v Parliament and Council*, C-301/06, cit., §28).

[42] *Ireland v Parliament and Council*, C-301/06, cit., §§83-85.

[43] Idem, §57.

Electronic copy available at: https://ssrn.com/abstract=4216870

fundamental rights when Austria claimed that its delay in transposing the Directive stemmed from doubts as to whether it respected the right to privacy enshrined in Articles 8 of the ECHR and the Charter[44]. The Court promptly dismissed the argument, considering it should have been raised in an action for annulment and not, as was the case, as a means of defence in an infringement action[45]. The assurance in Recital 22 of the Directive of "full compliance with citizens' fundamental rights" was later invoked in another infringement action to measure the degree of seriousness of the breach of EU law imputed on Member States for not transposing the directive[46].

Yet it was only a matter of time until the national courts questioned the Court of Justice directly on the compatibility of the Directive with the exercise of fundamental rights protected by the Charter, under the Article 267 TFEU procedure. Preliminary references in this regard were submitted by the Irish High Court and the Austrian Constitutional Court during 2012. On 8 April 2014, the Court of Justice declared the Data Retention Directive invalid due to breach of Articles 7 and 8 of the Charter[47].

Digital Rights Ireland is a landmark ruling that effectively bans securitarian legal instruments based on a preventive general and indiscriminate retention of metadata. The Court of Justice had no qualms in classifying the retention of data mandated by the Directive as a "wide-ranging and particularly serious" interference with the rights to privacy and data protection of virtually the entire European population[48]. The fact that data were retained and could subsequently be used without data subjects being informed was considered likely to generate in their minds the feeling that their private lives were under constant surveillance[49]. The judicial review of the discretion of the legislator in this domain had to be strict, considering the extent and seriousness of the interference[50]. The Court salomonically conceded that the data retention obligations stemming from the Directive were a "valuable tool" in attaining the objective, in the

[44] *Commission v Austria*, C-189/09, cit., §10-11.
[45] Idem, §15.
[46] *Commission v Sweden*, C-270/11, cit., §48-49.
[47] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §69.
[48] Idem, §§37, 56 and 65.
[49] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §37.
[50] Idem, §§47-48.

Electronic copy available at: https://ssrn.com/abstract=4216870

general interest, of contributing to the fight against serious crime in order to ensure public security, and breached neither the essence of the right to privacy, as the content of communications as such was not stored, nor the essence of the right to data protection, as service providers had to respect certain principles of data protection and data security[51].

However, the storage of data in bulk required by the Directive failed the test of proportionality as it was not limited to what was strictly necessary. The breach of the principle of proportionality derived directly from the general and indiscriminate nature of the retention, which covered all persons and all means of electronic communication, as well as all metadata "without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime"[52]. This meant it affected even persons for whom there was no "evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime", as well as persons whose communications were subject to the obligation of professional secrecy[53]. A proportional measure required retained data to have at least some indirect link to a threat to public security. That would be the case of targeted retention surveillance measures focused on collecting data pertaining either "to a particular period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime", or "to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences"[54]. Such a data retention measure should also, contrary to that laid down by the Directive, distinguish between the categories of retained data and their "possible usefulness for the purposes of the objective pursued or according to the persons concerned"[55], and adopt a particularly high level of protection and security to ensure effective protection of the retained data against the risk of abuse and against any unlawful access and use of that data[56]. Service providers should, *inter alia*, be

[51] Idem, §§ 39-50.
[52] Idem, §57.
[53] Idem, §58.
[54] Idem, §59.
[55] Idem, §63.
[56] Idem, §66-68.

Electronic copy available at: https://ssrn.com/abstract=4216870

obliged to retain data in the EU and to irreversibly destroy data at the end of the data retention period[57].

Surprisingly, given that issues of access to data were outside the scope of the Directive[58], the Court also lambasted the European legislator for not setting any substantive and procedural conditions on access to the retained data and their subsequent use. Unrestricted access by public authorities would be tantamount to unlawful exploratory or general surveillance (Article 29 Working Party , 1999: 8). Therefore, access to the retained data required a prior review carried out by a court or by an independent administrative body. Furthermore, access to data or the use thereof had to be strictly restricted to a limited number of persons involved in preventing and detecting precisely defined serious offences or in conducting criminal prosecutions relating thereto[59].

3.4. Attempts at resurrection

Digital Rights Ireland relieved Member States from implementing the Directive at a time when most of them had already duly introduced data retention into their domestic legal orders[60]. The ruling of the Court of Justice retroactively eliminated the effects of the Directive from the legal system of the EU (Türk, 2009: 228-229)[61], but had no effect on the *formal* validity of the corresponding implementing national law, as the latter stemmed from *domestic* sources of law[62]. For that reason, between June 2014 and

[57] Idem, §67-68.

[58] *Ireland v Parliament and Council*, C-301/06, cit., §83, and Recital 25 and Article 4 of the Data Retention Directive.

[59] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §§61-62.

[60] The exceptions being Germany and the Czech Republic after the *Data Retention* judgments of the Federal Constitutional Court of Germany of 2 March 2010, cit., and of the Constitutional Court of the Czech Republic of 22 March 2011, Pl. ÚS 24/10 (Albers, 2021: 131) (Polčák, 2021: 114-115).

[61] *FMC,* C-212/94, 8 February 1996, ECLI:EU:C:1996:40, §55 ("(A) judgment of the Court in proceedings for a preliminary ruling declaring a (EU) act to be invalid takes effect, like a judgment annulling an act, from the date on which the act entered into force, with all the consequences which that entails"), and, by analogy, Court of First Instance, *Corus UK* Ltd, T-171/99, 10 October 2001, ECLI:EU:T:2001:249, §50 ("(A) judgment of annulment (…) takes effect *ex tunc* and thus has the effect of retroactively eliminating the annulled measure from the legal system").

[62] Portuguese Constitutional Court, 420/2017, 13 July 2017, §10: "(T)he declaration of invalidity of a directive has no automatic consequence on the validity of a transposing Portuguese legal act. This act (…)

Electronic copy available at: https://ssrn.com/abstract=4216870

June 2015 legislation transposing the Directive was judicially rendered inoperative in the Netherlands[63], and revoked by constitutional courts in Austria, Belgium, Bulgaria, Poland, Romania, Slovenia, and Slovakia[64]. In most Member States, however, legislation providing for a general and indiscriminate retention of metadata remained untouched. Since Member States were expressly authorised to adopt data retention as an exception to the principle of confidentiality (Article 15(1) of the E-privacy Directive), could such legislation still be enforced?

As national law on data retention falls within the scope of Article 15(1) of the E-privacy Directive[65], and thus implements EU law within the meaning of Article 51(1) of the Charter[66], a negative answer looked straightforward in light of the principle of primacy: since the Directive was held to be incompatible with Articles 7 and 8 of the Charter, then it followed that implementing national legislation with the very same provisions also breached the Charter, and consequently had to be rendered inapplicable in the domestic legal realm[67].

A positive answer was, however, voiced based on the idea that the *Digital Rights Ireland* ruling could not be interpreted as establishing a ban on the adoption of a blanket data retention legal scheme. National law adopted to implement the Data Retention Directive was not structurally incompatible with the Charter and was lawful if accompanied by appropriate procedural and substantive safeguards[68]. The argument

stems from an autonomous source of validity and legitimacy". See also Bobek (2017: 164): "National law can only be invalidated by the national institutions and EU law by the EU institutions".

[63] By a decision of 11 March 2015 of a District Court of The Hague considering the Data Retention Act 2009 to be manifestly incompatible with EU law (Besselink and Claes, 2019: 203).

[64] Constitutional Court of Austria, 27 June 2014, G 47/2012; Constitutional Court of Slovenia, 3 July 2014, U-I-65/13; Romanian Constitutional Court, 8 July 2014, 440; Constitutional Tribunal of the Republic of Poland, 30 July 2014, K 23/11; Constitutional Court of Bulgaria, 12 March 2015, 8/2014; Constitutional Court of Slovakia, 29 April 2015, PL. ÚS 10/2014; Constitutional Court of Belgium, 11 June 2015, 84/2015.

[65] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §§65-81.

[66] *Fransson*, C-617/10, 26 February 2013, ECLI:EU:C:2013:105, §§20-21.

[67] *Simmenthal*, 106/77, 9 March 1978, EU:C:1978:49, §17.

[68] See: in Cyprus, several rulings of the Supreme Court discussed by Markou (2021: 90-94); in Denmark, a memorandum of the Danish Ministry for Justice dated 2 June 2014, quoted by Krunke and Baumbach (2019: 297-298); in Estonia, a decision from the Supreme Court of 23 February 2015, quoted by Madis Ernits et al. (2019: 927); in Finland, an opinion from the Constitutional Law Committee of Parliament dated April 2014, quoted by Ojanen and Salminen (2019: 318); in Sweden, the special report from the Swedish Ministry for Justice "Datalagring, EU-rätten och svensk rätt, Ds 2014:23", 13 June 2014, quoted in *Tele*2 *Sverige*, C-203/15 and C-698/15, cit., §46; in the United Kingdom, the ruling of the English High Court in *Davis & Ors v. SSHD*, 17 July 2015, CO/3665/2014, CO/3667/2014, CO/3794/2014, §89.

Electronic copy available at: https://ssrn.com/abstract=4216870

was far-fetched, but it was even used by Advocate General Øe in response to preliminary references submitted by British and Swedish courts in the *Tele2 Sverige* case[69].

The remaining doubts on the lawfulness of blanket data retention were resolved by the Court of Justice on 21 December 2016. Article 15(1) of the E-privacy Directive requires data retention to be an exception to the principle of confidentiality which can only be pursued with the objective of fighting serious crime[70]. National law implementing the Data Retention Directive transforms the exception into a rule as it provides for a "general and indiscriminate" retention of metadata[71]. It therefore exceeds the limits of what is strictly necessary and is not justified as required by Article 15(1) of the E-Privacy Directive, read in the light of Articles 7, 8, 11 and 52(1) of the Charter[72]. These provisions do not, however, preclude Member States from adopting legislation permitting, as a preventive measure, the *targeted* retention of metadata provided that such retention is limited to what is strictly necessary in terms of the categories of data to be retained, the means of communication affected, the persons concerned, and the retention period adopted[73]. Such retention of data is admissible only when there is "objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences", namely when national authorities consider that "there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences"[74]. Given the seriousness of the interference with fundamental rights it entails, national legislation authorising preventive targeted data retention relating to specific circles of people or geographical locations must establish stringent safeguards concerning access to the retained data and the protection and security of that data. Beyond the

[69] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §205.

[70] Idem, cit., §§102-104.

[71] Idem, §97 and 104.

[72] Idem, §107.

[73] Idem, §108.

[74] Idem, §111. In *La Quadrature du Net,* C-511/18, C-512/18 and C-520/18, cit., §150, the Court added that those areas may include places "vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas", while in *Commissioner of An Garda Síochána*, C-140/20, cit., §80, it admitted that Member States could pursue targeted data retention derived from the use of average crime rate statistics in a geographical area, without public authorities necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime.

Electronic copy available at: https://ssrn.com/abstract=4216870

requirements laid down in *Digital Rights Ireland*, the Court declared that access should be restricted to cases that deal with serious crime and, as a general rule, should only be granted "to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime"[75]. Moreover, the principle of transparency requires national authorities that have been granted access to "notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities" so that such persons can exercise their right to a legal remedy[76].

The *Tele2* ban on blanket data retention was tweaked in *La Quadrature du Net*, where the Court of Justice admitted the lawfulness of national legislation providing for precautionary, general, and indiscriminate retention of data for a limited period of time in order to safeguard national security in the face of a serious threat that is shown to be genuine and present or foreseeable[77]. The court of Luxembourg also accepted that the following categories of traffic data could be retained in bulk: i) IP addresses, with the objective of safeguarding national security, combating serious crime and preventing serious threats to public security[78]; ii) data relating to the civil identity of subscribers and registered users of electronic communications ("users' civil identity data") with the objective of safeguarding national security, combating crime and safeguarding public security[79]. Any national measure had to ensure that the retention of data complies with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risk of abuse and unlawful access[80].

[75] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §§115 and 119. The Court also acknowledged that access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating terrorist activities (idem, §119).

[76] Idem, §121.

[77] *La Quadrature du Net,* C-511/18, C-512/18 and C-520/18, cit., §137. Such a retention, however, could not be "systematic in nature" (idem, §138).

[78] Idem, cit., §168. The Court accepted the argument that where an offence is committed online, inter alia, in cases involving particularly serious child pornography offences, IP addresses retained in bulk might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified (Idem, §154).

[79] Idem, cit., §168. See also *Ministerio Fiscal*, C-207/16, 2 October 2018, ECLI:EU:C:2018:788, paras. 59-61.

[80] *La Quadrature du Net,* C-511/18, C-512/18 and C-520/18, cit., §168.

Electronic copy available at: https://ssrn.com/abstract=4216870

4. Data Retention in Portugal: chronicle of a fate (long) foretold

4.1. Primacy

The EU Treaties created their own legal system which "became an integral part of the legal systems of the Member States and which their courts are bound to apply"[81]. The judicial catchphrase is arguably the most important in the history of legal integration in Europe. It basically means that, contrary to public international law, EU law is directly applicable (enforceable) in each Member State. The "justiciability" stemming from the direct effect of EU provisions opens up the possibility of normative conflicts with national law. But how should national judicial and administrative bodies deal with vertical conflicts in a federal polity such as the EU? According to the principle of primacy, prevalence must always be given to the application of EU law:

> "(B)odies called upon, within the exercise of their respective powers, to apply EU law are obliged to adopt all the measures necessary to ensure that EU law is fully effective, disapplying if need be any national provisions or national case-law that are contrary to EU law. This means that those bodies, in order to ensure that EU law is fully effective, must neither request nor await the prior setting aside of such a provision or such case-law by legislative or other constitutional means"[82].

The legal status of the Portuguese Data Retention Law was not in doubt after the *Digital Rights Ireland* ruling of the Court of Justice. It could not be applied as it breached the Charter by imposing a general and indiscriminate retention of data (Guerra and Calvão, 2015: 79-80) (Silva Ramalho and Duarte Coimbra, 2015: 1038-1039) (Silveira and Freitas, 2017: 52-53) (Pereira Coutinho and Piçarra, 2019: 616). In light of the ongoing and widespread enforcement of the Data Retention Law in the Portuguese legal order, the principle of sincere cooperation required an intervention by the legislative, executive or judicial branch. The resilience of this law is a testimony to a delusional legislator, an absent data protection supervisor, and an erratic Constitutional Court.

[81] *Costa v ENEL*, 6/64, 15 July 1964, ECLI:EU:C:1964:66, at 593.

[82] *Minister for Justice and Equality*, C-378/17, 4 December 2018, ECLI:EU:C:2018:979, §50.

Electronic copy available at: https://ssrn.com/abstract=4216870

4.2. A delusional legislator

The Portuguese Government initially took an ambivalent stance on data retention. While advocating the adoption of EU-wide legislation on the matter (Council of the European Union, 2002b: 20-22), domestically it dithered even in following through with international obligations regarding the (much) less privacy-intrusive alternative of "quick-freeze" data preservation[83]. Unsurprisingly, it voted for the Data Retention Directive (Council of the European Union, 2006: 4), and diligently approved a draft bill on its implementation less than a fortnight before the transposition deadline[84]. But the endorsement of preventive blanket data retention was half-hearted. In *Digital Rights Ireland*, written observations were submitted to the Court of Justice questioning whether the measure was adequate in terms of attaining the objective of fighting serious crime, since there were several methods of electronic communication which fell outside the scope of the Directive, or which allowed anonymous communication[85].

The draft bill on data retention sailed through Parliament. The only opposition came from the far-left parties, which were not shy in portraying the measure as an unprecedented attack on civil liberties stemming from a "European securitarian paranoia on the loose" (Filipe, 2008: 22-23). The Government counterargued that "special safeguards" "fully" protected the right to privacy (Silveira, 2008: 19-20).

So strong were the safeguards that the Portuguese Data Retention Law was even considered "a special case of legality" and an "example" for other national laws (Portela and Cruz-Cunha, 2010: 3 and 10). Unfortunately, the Portuguese Government firmly believed this legal myth to be true. After informing the Council that no legislative action was needed following the *Tele2* ruling (Council of the European Union, 2017: 10), the Government ignored recommendations to the contrary submitted by the data protection authority (2017b) and by the Ombudsman (2019) urging the limitation of the

[83] See Article 12 of the Cybercrime Law (Law 109/2009), which implements Article 16 of the Convention on Cybercrime of the Council of Europe, ETS 105 (entry into force 1 July 2004). The Portuguese Government signed the Convention on 23 November 2001, but only approved a Draft Bill on its object on 14 May 2009.

[84] Draft Bill 161/X/3, approved by the Council of Ministers on 6 September 2007.

[85] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §50.

Electronic copy available at: https://ssrn.com/abstract=4216870

scope of the data retention legal framework, and instead promoted its expansion by allowing access to data retained in bulk in cases of fraud and counterfeiting of non-cash means of payment[86].

The delusion was not justified. After *Tele2*, no doubts remained as to the unlawfulness of the obligation imposed on service providers to retain *all* metadata of *all* data subjects for *all* means of electronic communication with the intent to make this data accessible for the purpose of the investigation, detection and prosecution of serious crime[87]. National law, such as the Portuguese, providing for a general and indiscriminate retention of data exceeded, by default, the limits of what was strictly necessary, thereby breaching Articles 7, 8, 11 and 52(1) of the Charter[88]. The nature of the safeguards introduced by the national legislator was irrelevant to assess the validity of such a serious interference with fundamental rights[89].

In any event, the "special safeguards" introduced by the Portuguese legislator, such as making access to retained data subject to prior judicial review (Article 3(2) and 9 of Law 32/2008), would always fall very short of what was necessary to effectively protect the data subjects in question against any unlawful access to and use of their data. Firstly, as service providers were not required to retain data within the EU, there was no guarantee that the protection and security requirements for the retained data would be controlled by an independent data protection authority[90]. Secondly, data subjects' rights, under Articles 7 and 8 of the Charter, to request access to their personal data and, where appropriate, to have the latter rectified or erased, and, under Article

[86] Article 4 of Law 19/2021, which amends Article 2(g) of Law 32/2008.

[87] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §112.

[88] Idem, §107.

[89] The Court of Justice addressed this issue directly in *Commissioner of An Garda Síochána*, C-140/20, cit., §47: "(N)ational legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference, which results from the general retention of those data provided for under that national legislation, with the rights guaranteed by Articles 5 and 6 of that directive and by the fundamental rights to which those articles give specific effect".

[90] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §68, and *Tele2 Sverige*, C-203/15 and C-698/15, cit., §§122-3. This was not a "minor issue" (Silva Ramalho and Duarte Coimbra, 2015: at 1038) given that retained data could even have been transferred to a third country (the United States of America) where the legislation authorises public authorities to have unrestricted access to those data while not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data (*Schrems I*, C-362/14, 6 October 2015, ECLI:EU:C:2015:650, §§93-95).

Electronic copy available at: https://ssrn.com/abstract=4216870

47(§1) of the Charter, to avail themselves of an effective remedy before a tribunal, were restricted because public authorities that had been granted access to the retained data were not obliged to notify the persons affected[91]. Thirdly, service providers were not obliged to implement technical measures providing for the *irreversible* destruction of the data at the end of the data retention period[92]. Fourthly, no objective criterion was established limiting the *number of persons* authorised to access and subsequently use the retained data [93]. Fifthly, data security concerning the transmission of retained data to law enforcement authorities was impaired by the non-binding nature of the electronic application created for that specific purpose by Ordinance 469/2009[94].

Finally, proportionality was compromised by the fact that the Data Retention Law established a single period of retention without any distinction being made between the categories of data to be retained based on their possible usefulness for the purposes of fighting serious crime or according to the persons concerned[95].

The principle of sincere cooperation enshrined in Article 4(3)(§2) TUE obliged the Portuguese legislator to take appropriate measures to ensure fulfilment of the obligations arising out of the Treaties, which meant revising the legal framework on data retention in line with the Charter, as interpreted in the case law of the Court of Justice. Its sole intervention extending public authorities' access to data retained under the Data Retention Law only amplified the seriousness of the infringement of EU law.

4.3. An absent supervisor

The *Comissão Nacional de Proteção de Dados* is an independent supervisory authority established by the Portuguese State to review the level of data protection guaranteed by EU law in the Portuguese legal order (Article 3 of Law 58/2019). That control is expressly required by Article 8(3) of the Charter and constitutes an essential

[91] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §121.

[92] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §67, and *Tele2 Sverige*, C-203/15 and C-698/15, cit., §122.

[93] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §62.

[94] *Privacy International*, C-623/17, 6 October 2020, ECLI:EU:C:2020:790, §68. This IT application was still not being used in 2017 (Comissão Nacional de Proteção de Dados, 2017b: 9).

[95] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §63.

Electronic copy available at: https://ssrn.com/abstract=4216870

element of the right to data protection[96]. National data protection authorities are different to other domestic administrative bodies because they derive directly from EU primary law and, consequently, their tasks and powers are determined by EU secondary law (Articles 55 to 59 GDPR). They form a "European composite administration" through their participation in the European Data Protection Board, as well as in the complex administrative procedures of cooperation and consistency (Articles 60-62, 63-67, and 68 (3) GDPR). Data protection authorities are thus hybrid bodies: they are national public entities established under national law that perform tasks of a European agency (Hijmans, 2016: 309-311) (Pereira Coutinho, 2020: 16-17). For that reason, they must act with "complete independence", remaining free from external influence, whether direct or indirect, and neither seeking nor taking instructions from anybody (Article 52(1) and (2) GDPR).

Called upon to comment on draft versions of the Data Retention Law, the Portuguese data protection authority proposed several amendments, which were duly incorporated by the Government. The most relevant was arguably the proposal to reduce the retention period from two years to one year to follow the standard set in many Member States, some of which had recently suffered terrorist attacks (Comissão Nacional de Proteção de Dados, 2007a: 3) (Silveira, 2008: 20-21). Harmonisation was not, however, a criterion that could be considered objective to establish a period of retention limited to what was strictly necessary[97]. Given that Portugal fortunately never experienced severe security threats, the retention period should have been "as short as possible" (Article 25 Data Protection Working Party, 2005: 6), which meant six months.

Another important contribution concerned the need for the law to specify the purpose of retaining data. The data protection authority accurately stated that the definition of purpose is crucial (Comissão Nacional de Proteção de Dados, 2007b: 3-4). The problem is that it never turned these words into action by using its corrective powers, under Article 58(2) GDPR, to check and sanction the unlawful access by law

[96] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §123.

[97] *Digital Rights Ireland*, C-293/12 and C-594/12, cit., §62.

Electronic copy available at: https://ssrn.com/abstract=4216870

enforcement authorities (public prosecutors and criminal police) to data retained by service providers for billing purposes.

A practice was adopted to deliberately circumvent the limitation of access to retained data to cases related to serious crime listed in Article 2(1)(g) of the Data Retention Law. The list was considered "very restrictive" as it did not include many of the offences set out in Article 187(1) of the Code of Criminal Procedure and in Article 11 of the Cybercrime Law, such as slander, smuggling or generally any cybercrime (Pinho, 2018: 169-170). As metadata were deemed "essential evidence" (Pinho, 2018: 169), access to data retained by service providers for billing purposes was sought following two legal pathways: i) traffic and location data were accessed after judicial authorisation under Article 189(2) of the Code of Criminal Procedure in cases related to criminal offences listed in Article 187(1) of the Code of Criminal Procedure; ii) IP addresses and users' civil identity data were accessed *without* prior judicial review in cases related to *any* crime in accordance with Articles 11 and 14 of the Cybercrime Law (Cybercrime Office, 2016: 7)[98].

The practice breaches the principle of specificity which requires data retention and subsequent access to be solely related to billing. Further exceptions to the principle of confidentiality can only be admitted under Article 15(1) of the E-Privacy Directive, read in the light of Articles 7, 8, 11 and 52(1) of the Charter, as interpreted by the case law of the Court of Justice. Blanket retention of metadata is admissible in very specific circumstances (serious threat to national security) or for specific metadata (IP addresses and users' civil identity data), and only for criminal law and/or national security purposes that have to be clearly and precisely laid down in law, which has also to establish strict safeguards concerning access and data protection and security. Neither those purposes nor those safeguards are set out in Law 41/2004, which implements the E-Privacy Directive[99]. That did not stop the Public Prosecution Service from declaring, after the

[98] In *Prokuratuur*, C-746/18, 2 March 2021, ECLI:EU:C:2021:152, §57, the Court of Justice declared that the Estonian public prosecution service could not be considered an "independent administrative body" for the purpose of carrying out the prior review to which access by the competent national authorities to retained data must be subject.

[99] Pinho (2018: 171): "(T)he fact that the storage of data for billing purposes (…) is not procured for the investigation, detection, and prosecution of criminal offences means that this processing does not include the safeguards applicable to that specific purpose".

Electronic copy available at: https://ssrn.com/abstract=4216870

annulment of the Data Retention Law by the Constitutional Court, that it will persist in its blatant breach of EU law by requesting IP addresses from service providers under Article 14(1) and (4) of the Cybercrime Law (Cybercrime Office, 2022: 2-3) – an odd announcement given that IP addresses are *traffic data* which are not necessary for billing purposes, and thus cannot be retained by service providers in accordance with Article 6 of Law 41/2004[100].

The national data protection authority also remained silent after the seminal *Digital Rights* constitutional ruling of the Court of Justice of 8 Abril 2014. It took more than fourteen months for it to elliptically declare that the "legitimacy" of data retention under Law 32/2008 was yet to be determined in the Portuguese legal order (Comissão Nacional de Proteção de Dados, 2015: 10). Right after the *Tele2* ruling, it went further by stating that the lack of proportionality of blanket data retention "endangers the 'validity' of the law implementing the Directive and, therefore, compromises its constitutionality", thereby predicting the inevitability of a Constitutional Court's decision (Comissão Nacional de Proteção de Dados, 2017a: 20-21). A few weeks later, the authority requested Parliament to amend the Data Retention Law (Comissão Nacional de Proteção de Dados, 2017b). In the absence of any foreseeable action from the legislative branch, it invoked the principle of primacy to declare it would no longer enforce its sanctioning powers under the Data Retention Law (Comissão Nacional de Proteção de Dados, 2017c: 3). This basically meant that service providers no longer had any incentive to fulfil their obligations to ensure a "particularly high level of protection and security" of the retained data, as no independent supervisory authority was ensuring compliance with data protection (Ombudsman, 2019: 15). This problem was solved on 7 June 2022 when the data protection authority used its powers under Article 58(2)(d) of the GDPR, and ordered service providers to delete, in 72 hours, data retained in accordance with Law 32/2008 (Comissão Nacional de Proteção de Dados, 2022a). The following week, with a staggering 2933-day delay[101], service providers duly announced they had deleted the data (Ambrósio de Sousa, 2022).

[100] Pinho (2018: 171) and *La Quadrature du Net,* C-511/18, C-512/18 and C-520/18, cit., §154.

[101] Service providers were obliged to destroy the database created under the Data Retention Law for the simple reason that the processing of those data was not necessary for compliance with an *applicable* legal obligation to which they were subject (Article 6(1)(c) GDPR). In the absence of any other *lawful basis* for

Electronic copy available at: https://ssrn.com/abstract=4216870

The national data protection authority's justification for its decision to order the deletion of retained data was the need to comply with the Constitutional Court ruling of 19 April 2022. It stated that the declaration of unconstitutionality annulled the Data Retention Law and, consequently, rendered application of its provisions impossible in the Portuguese legal order (Comissão Nacional de Proteção de Dados, 2022a). The problem is that, as the data protection authority *expressly* recognised in July 2017 (Comissão Nacional de Proteção de Dados, 2017c), the Data Retention Law breached the Charter and was *already* inapplicable in the Portuguese legal order, which begs the question why the deletion of data was not ordered right after the *Digital Rights Ireland* and *Tele2 Sverige* rulings. The national data protection authority thus failed miserably by standing idly by and passively observing a serious breach of the fundamental rights of almost the entire Portuguese population for more than eight years.

4.4. An erratic Constitutional Court

The "*Simmenthal* mandate" obliges national courts to apply EU law in its entirety to cases within their jurisdiction and to protect rights which individuals derive from it, setting aside, if necessary, any conflicting provision of national law (Claes, 2006: 108). Portuguese courts were thus obliged to apply the Charter and refuse any request to access data retained by service providers under the Data Retention Law made after the *Digital Rights* ruling of the Court of Justice.

On 16 October 2016, this mandate was sidestepped in a child pornography case by a judge in a lower criminal court in Lisbon, who invoked the Portuguese Constitution to deny access to civil identity data of the subscriber or user of electronic communication systems to whom an IP address was allocated at the time of a communication. Instead of dismissing the appeal submitted by the Public Prosecution Service, arguing this was a question regarding the application of EU law to be decided

processing, the storage of data in breach of the principle of lawfulness was liable to be sanctioned. See, however, Silva Ramalho and Duarte Coimbra (2015: 1040), who reject such liability, claiming that service providers were not obliged to disapply national law breaching EU law and could thus continue to enforce a law which the authors themselves consider to be in a state of "latency" (Silva Ramalho and Duarte Coimbra, 2015: 1042).

Electronic copy available at: https://ssrn.com/abstract=4216870

by ordinary courts with the assistance of the Court of Justice[102], the PCC surprisingly decided to uphold the lawfulness of blanket retention and further use of users' civil identity data in Decision 410/2017.

Neglecting the fact that any legal provisions imposing data retention on service providers necessarily fall within the scope of Article 15 (1) of the E-Privacy Directive and must meet the requirements of the Charter as interpreted by the Court of Justice, the PCC declared it was not bound by the latter's case law and would follow an autonomous hermeneutic path based on national, European, and international fundamental rights parameters[103]. This path had the Court identifying users' civil identity data and IP addresses as basic data when they are, according to the Court of Justice, traffic data[104], and, in a blatant breach of its obligation to submit a preliminary reference in accordance with Article 267 (3) TFEU, it implicitly considered that such metadata could be retained in bulk, a matter the Luxembourg court only dealt with in L*a Quadrature du Net*[105]. Most importantly, the decision allowed the PCC to bypass the *Tele2 Sverige* ruling, which it quotes but ostensibly ignores, by not reviewing the nature of the general and indiscriminate retention of data enforced by the Data Retention Law or the latter's safeguards protecting the data subjects in question against the risk of abuse and unlawful access. The Court satisfied itself with a reference to pre-*Tele2 Sverige* soft law guidelines from the Public Prosecution Service's Cybercrime Office that claim that the strictness of the safeguards included in the Data Retention Law sheltered it from any problems of constitutionality (Cybercrime Office, 2015: 3). The PCC then undertook a

[102] See, among others, Decision 466/2003, 125/02, 14 October 2003, Decision 46/04, 885/03, 19 January 2004, Decision 598/04, 685/03, 12 October 2004, and Decision 569/2016, 238/16, 19 October 2016, which refused to qualify the compatibility between national law and EU primary law as a question of constitutionality subject to review by the PCC, referring to José Manuel Cardoso da Costa (1998: 1371): "(T)he incompatibility between provisions of domestic law and (EU law) should not be assimilated to a category or a dogmatic concept whose utilization or application (…) would mean withdrawing from ordinary courts the final decision of that question within their jurisdiction".

[103] Decision 410/2017, §10.

[104] See, regarding users' civil identity data, *Ministerio Fiscal*, C-207/16, cit., §42 ("(I)t is apparent from recital 15 of Directive 2002/58 that traffic data may include, inter alia, the name and address of the person sending a communication or using a connection to carry out a communication. Data relating to (…) identity (…) can also prove necessary in order to bill for the electronic communications services provided and therefore form part of traffic data as defined in subparagraph (b) of the second paragraph of Article 2 of the directive"), and concerning IP Addresses, *Quadrature du Net*, C-511/18, C-512/18 and C-520/18, cit., §152.

[105] Decision 410/2017, §11.

Electronic copy available at: https://ssrn.com/abstract=4216870

"specific" constitutional review, where it concluded that the provision granting law enforcement authorities access to users' civil identity data is a proportional restriction to the right to privacy[106].

The ruling empowered the unfettered judicial application of provisions manifestly in breach of EU constitutional law. On 28 November 2018, the Lisbon Civil Court of Appeal, after quoting the decision of the PCC at length to conclude on the applicability of the Data Retention Law, quashed a first instance court ruling that rejected granting access to civil identity data retained for billing purposes under Article 14(1) and (4) of the Cybercrime law, arguing that such a possibility was forfeited after the *Digital Rights Ireland* ruling[107]. It was against this bleak legal background that the Ombudsman, following an application in December 2017 from a privacy advocacy group (D3, 2017), requested the PCC to conduct an abstract constitutional review of the Data Retention Law in an exceptionally well-reasoned legal opinion delivered on 16 September 2019 (Ombudsman, 2021).

When reviewing the Data Retention Law, the PCC essentially had two options. It could have dismissed the case, arguing that it could not address the constitutionality of provisions which were inapplicable in the Portuguese legal order, as they manifestly breached the Charter. Such a constitutional review could theoretically be observed as hypothetical, similarly to the review of legal provisions revoked before entering into force. The PCC wisely pursued a different path. Even if the Data Retention Law provisions were inapplicable in the domestic realm, they *organically* stemmed from a national source of law the formal validity of which could never be affected by a ruling of the Court of Justice. EU law, the PCC states, quoting the Spanish Constitutional Court's Declaration 1/2004 on the Constitutional Treaty, has *primacy* but not *supremacy* over national law (i.e. it trumps but does not revoke national law)[108]. That meant that the contested provisions on data retention could only be revoked by the Portuguese Parliament or by the PCC in an abstract review procedure. Given that the Data Retention Law was being profusely applied in the Portuguese legal order (including by the PCC), the question

[106] Idem, §§12-14. See also Violante (2021: 183-184).

[107] Tribunal da Relação de Lisboa, 28 November 2018, 8617/17.8T9LSB-A.L1-3, at 3.3. and 3.4.

[108] Decision 268/2022, cit., §8.1.

Electronic copy available at: https://ssrn.com/abstract=4216870

could not be said to be (*factually*) hypothetical. Under the duty of sincere cooperation, the PCC was then obliged to do everything within its means to secure the uniform application of EU law in the Portuguese legal order. It followed this obligation by interpreting the relevant fundamental rights provisions of the Portuguese Constitution in accordance with the Charter, as interpreted by the Court of Justice – I fail to understand the criticism of six justices in a concurring vote on the use of the principle of consistent interpretation instead of the direct application of the Charter in a case that revolved exclusively around the technical revocation of inapplicable provisions of national law breaching EU constitutional law and, *a fortiori*, the Portuguese Constitution. The hermeneutic path taken by the PCC mimics that of other Constitutional Courts also dealing with data retention[109], and is perfectly aligned with the obligation to apply EU law provisions in the *conditions prescribed* by EU law (Article 8 (4) of the Portuguese Constitution), which is based on the pluralistic constitutional assumption of the existence of a systemic compatibility between fundamental rights protection in the Portuguese and European constitutional orders[110]. Such a path obviously precluded the possibility of a decision limiting the ruling's effects under Article 282 of the Constitution, including those concerning *res judicata*, as the PCC expressly acknowledged by invoking, in response to the Attorney General's ruling annulment request[111], the *Commissioner of An Garda Síochána* ruling of the Court of Justice[112]. In a nutshell, the PCC limited itself to certifying the obituary of provisions which (legally) were already dead in the water.

The 19 April 2022 ruling is arguably the most compelling ever adopted by the PCC concerning the relation between EU and national constitutional law. It is an 11 to 1 decision which, without ever admitting it, in effect reverses its previous case law solving the conundrum posed by the unlawful resilience of the Portuguese data retention legal

[109] That was the case of the Belgium Constitutional Court (Popelier and Van de Heyning, 2019: 1249), the Slovak Constitutional Court (Vikarská and Bobek, 2019: 868), and the Slovenian Constitutional Court (Bardutzki, 2019: 714).

[110] As Teresa Violante (2022: 5) accurately remarked, the principle of consistent interpretation allowed the PCC to "link the national standard of protection with the European parameter, leading to a fully congruent standard of fundamental rights protection through the application of the national constitutional provisions".

[111] Decision 382/2022, cit., §4.

[112] C-140/20, 5 April 2022, §128.

Electronic copy available at: https://ssrn.com/abstract=4216870

framework. The Court recognises the regulation of data retention as falling within the scope of the Charter, and thus subject to a constitutional review within the parameters set by the (ever abundant) Court of Justice's case law on data retention[113]. The Data Retention Law was found to have two major structural flaws – both missed by the July 2017 ruling of the PCC. Firstly, by not requiring metadata to be retained in the EU it jeopardises the effectiveness of data protection authorities' powers under the GDPR[114]. Secondly, by not creating an obligation for data subjects to be notified that their data are being shared with public authorities, it effectively impairs access to legal remedies for unlawful access to personal data[115]. Although these flaws would be enough to strike down the metadata law *in totum*, the PCC also reviewed the proportionality of data retention, only admitting, in line with the Luxembourg court, the bulk retention of users' civil identity data, and, in cases concerning serious criminal offences, such as child pornography, the blanket retention of IP addresses[116].

Astonishingly, the ruling is not centred on the crux of the constitutional problem posed by the enforcement of a general and indiscriminate retention of data of almost the entire Portuguese population. The PCC opted to focus its review primarily on an assessment of the safeguards concerning access, data protection and data security set out in the Data Retention Law, arguing that *in theory* the strictness of these safeguards could allow for a broader scope of the restriction on fundamental rights entailed by data storage[117]. This assumption was at the heart of its ruling in 2017, but is at odds with the case law of the Court of Justice, which made it crystal clear that a blanket retention of data such as that envisaged in Portugal is, *by itself*, a "very far-reaching" and "particularly serious" unlawful interference with fundamental rights, it being irrelevant whether the retained data has been used subsequently, since access to such data is a separate interference with fundamental rights and thus requires a separate justification[118]. The assumption was also immaterial to the case at hand; even if the Data

[113] Decision 268/2022, cit., §8.2.
[114] Idem, §16.
[115] Idem, §19.
[116] Idem, §17.1-17.4.
[117] Decision 268/2022, cit., §14.
[118] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §100, and *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, cit., §§115-119 and 140-141.

Electronic copy available at: https://ssrn.com/abstract=4216870

Retention Law, as the PCC wrongly assumed in Decision 410/17, included minimum safeguards effectively protecting data subjects against the risk of abuse and unlawful access, it would still have to be declared unconstitutional as it provided for continuous and systematic retention of data.

Throughout its judgment, the PCC is always at pains to articulate its reasoning with its previous case law on data retention. This explains why it decided to embark on a thorough review of the admissibility of specific bulk retention of users' civil identity data and static and dynamic IP addresses – the latter of which it now conceptually acknowledges may well qualify as traffic data – in order to conclude that the retention of these metadata for one year would not be, *in itself*, unconstitutional, *if* the legislator had laid down the obligation for data to be stored in the EU[119]. The proportionality balancing carried out in Decision 410/17 is, according to the PCC, perfectly aligned with that of the Court of Justice[120]. *Alas*, this is a bold statement not reconcilable with the fact that, concerning IP addresses, the retention period exceeded what was strictly necessary in light of the objective pursued[121], and not enough conditions and safeguards were established concerning the use of that specific data regarding communications made and activities carried out online, particularly via tracking[122].

I am also not convinced by the fundamental rights review undertaken by the PCC concerning the blanket retention of traffic and location data. This measure was found to breach the right to privacy and the right to data protection after failing the proportionality test[123]. According to the Court of Justice, while these rights are not absolute and must be considered in relation to their function in society[124], the sensitive nature of the information that traffic and location data may provide, determines that

[119] Decision 268/2022, cit., §17.4.

[120] Idem, §17.3.

[121] By way of comparison, Article 113(b) of the German Law on Telecommunications establishes a 10-week maximum period of retention.

[122] According to the Court of Justice, *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, cit., §§153 and 156, IP addresses "may be used, among other things, to track an Internet user's complete clickstream and, therefore, his or her entire online activity", and thus enable a detailed profile of the internet user to be produced.

[123] Decision 268/2022, cit., §18.

[124] *Schrems II*, C-311/18, 16 July 2020, EU:C:2020:559, §172.

Electronic copy available at: https://ssrn.com/abstract=4216870

the confidentiality of that data is *essential* for the right to respect for private life[125]. Should it not then follow that systematic retention of metadata breaches the essence of the right to privacy? In *Tele2 Sverige*, the Court stated that it did not. Although it classified the interference with fundamental rights stemming from national legislation implementing the Data Retention Directive as "very far-reaching" and "particularly serious", it dismissed any breach of the essence of the right to privacy, arguing that the content of the communications was not stored[126]. However, the Luxembourg court contradictorily recognised that the retained data was a means of establishing a profile of the individuals concerned, which was information "no less sensitive, having regard to the right to privacy, than the actual content of communications"[127]. The idea that the bulk storage of metadata is necessarily less intrusive than the acquisition of content was also rejected by the European Court of Human Rights in *Big Brother Watch*[128]. If, as former National Security Agency general counsel Stewart Baker reportedly stated, "metadata absolutely tells you everything about somebody's life", meaning that if law enforcement and intelligence authorities have enough metadata they "don't really need content" (Cole, 2014), then there is no reason to distinguish between the bulk retention of metadata *vis-à-vis* content data when considering its adverse effects on the essence of the right to privacy. It is my contention that the Court of Justice and the PCC failed by not declaring that a general and indiscriminate retention of data of the whole population envisaged in the Data Retention Directive and in the Data Retention Law must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter; the Luxembourg court should have followed the reasoning taken in *Schrems* regarding legislation permitting public authorities to have access on a generalised basis to the content of electronic communications[129].

[125] *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, cit., §142.

[126] *Tele2 Sverige*, C-203/15 and C-698/15, cit., §§100-101.

[127] Idem, §99.

[128] *Big Brother Watch and Others v. United Kingdom*, 25 May 2021, 58170/13, 62322/14 and 24960/15, §363.

[129] *Schrems I*, C-362/14, cit., §94.

Electronic copy available at: https://ssrn.com/abstract=4216870

Conclusion

In Decisions 403/2015 and 464/2019, the PCC blocked successive legislative attempts to grant intelligence agencies access to metadata retained in bulk by service providers. But is it reasonable to believe that metadata have not been accessed *unlawfully* by intelligence agencies over the past two decades? There is no doubt that was the case of law enforcement authorities concerning data retained under Laws 41/2004 and 32/2008. A passive European Commission, which has been ignoring pledges to launch infringement procedures against Member States whose laws implementing the Data Retention Directive have not been repealed (European Parliament, 2020: §32), combined with a systemic failure of all relevant national stakeholders in the executive, legislative and judicial branches allowed general and indiscriminate retention of data to continue in the Portuguese legal order until April 2022.

The ink on the PCC's ruling was barely dry when the Government proposed an amendment to Law 41/2004 granting access to law enforcement authorities to metadata retained for billing purposes, while obliging service providers to retain data not necessary for that specific purpose (e.g. IP addresses)[130]. This is a clumsy attempt to square the circle by covertly transforming the purpose of a database created for consumer law purposes (Comissão Nacional de Proteção de Dados, 2022b: §47). If approved, it will most certainly not survive a constitutional review that will control this novel securitarian drift by upholding the fundamental right of data subjects to expect their communication and data relating thereto to remain anonymous.

References

Albers, Marion, 2021. "Data Retention in Germany", in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 117-136

Ambrósio de Sousa, Filipa, 2022. "Nos, Vodafone e Altice garantem cumprimento da lei de metadados", *Eco*, 12 June 2022

[130] Draft Bill 11/XV/1, approved by the Council of Ministers on 26 May 2022.

Electronic copy available at: https://ssrn.com/abstract=4216870

Anderl, Axel and Alona Klammer, 2021. “Data Retention in Austria”, in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 39-52

Article 29 Working Party, 1999. *Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications*, adopted on 3 May 1999

Article 29 Data Protection Working Party, 2003. *Opinion 1/2003 on the Storage of Data for Billing Purposes*, 29 January 2003

Article 29 Data Protection Working Party, 2005. *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)*, 21 October 2005, at 5-6

Bacelar Gouveia, Jorge, 2022. “Erros de todos, boa fortuna de alguns, ódio ardente institucional”, *Diário de Notícias*, 5 May 2022

Bardutzki, Samo, 2019. “The Future Mandate of the Constitution of Slovenia: A Potent Tradition Under Strain”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 687-744

Besselink, Leonard and Monica Claes, 2019. “The Netherlands: The Pragmatics of a Flexible, Europeanised Constitution”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 179-220

Bigo, Didier et al., 2013. *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, European Parliament (Directorate-General for Internal Policies)

Bobek, Michal, 2017. “The Effects of EU Law in the National Legal Systems”, in C. Barnard and S. Peers (eds.), *European Union Law*, Second Edition, Oxford University Press, 143-176

Bowden, Caspar, 2002. “Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation”, *Duke Law & Technology Review*, 1, 1-7

Caixinha, Carla, 2022. “Preso por pornografia de menores libertado ao abrigo dos metadados”, *RR*, 10 June 2022

Cardoso da Costa, José Manuel, 1998. “O Tribunal Constitucional português e o Tribunal de Justiça das Comunidades Europeias”, in *Ab uno ad omnes*, Coimbra Editora, 1363-1380

Carmo, Cátia, 2022a. “Marcelo admite alterações à Constituição por causa da lei dos metadados: «O problema é que não há revisões pontuais», *TSF*, 11 May 2022

Carmo, Cátia, 2022a. “Costa admite revisão constitucional, mas que pode ser «cirúrgica» por causa dos metadados”, *TSF*, 11 May 2022

Claes, Monica, 2006. *The National Courts' Mandate in the European Constitution*, Hart

Electronic copy available at: https://ssrn.com/abstract=4216870

Cole, David, 2014. “We Kill People based on Metadata”, *New York Review of Books*, 10 May 2014

Comissão Nacional de Proteção de Dados, 2007a. Opinion 47/07, of 29 August

Comissão Nacional de Proteção de Dados, 2007b. Opinion 38/07, of 16 July

Comissão Nacional de Proteção de Dados, 2015. Opinion 51/2015, of 16 June

Comissão Nacional de Proteção de Dados, 2017a. Opinion 24/2017, of 18 April

Comissão Nacional de Proteção de Dados, 2017b. Deliberation 641/2017, of 9 May

Comissão Nacional de Proteção de Dados, 2017c. Deliberation 1008/2017, of 18 July

Comissão Nacional de Proteção de Dados, 2022a. “CNPD ordena eliminação dos dados das comunicações conservados ao abrigo de norma declara constitutional”, 9 June 2022

Comissão Nacional de Proteção de Dados, 2022b. Opinion 50/2022, of 21 June

Council of the European Union, 2001. *Extraordinary Council meeting – Justice, Home Affairs and Civil Protection*, C/01/327, 12019/01 (Presse 327), 20 September 2001

Council of the European Union, 2002a. *2477th Council meeting*, 15691/02 (Presse 404), 19 December 2002

Council of the European Union, 2002b, *Answer to questionnaire on traffic data retention*, 14107/02, 20 November 2002, Brussels, published in *Statewatch*, 12, 6, November-December 2002

Council of the European Union, 2004a. *Explanatory Memorandum – Framework Decision on the Retention of Communications Data*, 8958/04 ADD 1, 28 April 2004

Council of the European Union, 2004b. *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, 8958/04, 28 April 2004

Council of the European Union, 2005. *Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom*, (2004/0813(CNS))

Council of the European Union, 2006a. *2709ème session du Conseil de l'Union européenne (Justice et Affaires Interieures), tenue à Bruxelles, le 21 février 2006*, 6598/06 ADD 1, 27 February 2006

Council of the European Union, 2006b. *Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC [first reading]– Statements*, Doc. 5777/06 ADD 1, 10 February 2006

Council of the European Union, 2017. *Retention of electronic communication data*, 6726/1/17 REV 1, 7 March 2017

Cybercrime Office (Public Prosecution Service), 2015. “Retenção de dados de tráfego e Lei nº 32/2008, de 17 de Julho”, *Nota Prática nº 7*, 30 December 2015

Electronic copy available at: https://ssrn.com/abstract=4216870

Cybercrime Office (Public Prosecution Service),2016. “Pedido de dados a operadores de comunicações”, *Nota Prática nº 8*, 18 February 2016

Cybercrime Office (Public Prosecution Service), 2022. “Nota Informativa: Retenção de Dados de Tráfego – Acórdão do Tribunal Constitucional”, 17 May 2022

D3, 2017. “Press release: D3 pede à Provedora de Justiça que leve metadados ao Constitucional”, 27 November 2017

Ernits, Madis et al., 2019. “The Constitution of Estonia: The Unexpected Challenges of Unlimited Primacy of EU Law”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 887-950

European Commission, 2011. *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM/2011/0225 final

European Data Protection Supervisor, 2010. “«Moment of truth» for the Data Retention Directive: EDPS demands clear evidence of necessity”, *Communique de Presse*, EDPS/10/17, 3 December 2010

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)*, 2011/C 279/01, 31 May 2011, §75

European Commission, 2015. *Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*, SEC(2005) 1131, 21 September 2015

European Council, 2004. *Declaration on Combating Terrorism*, Brussels, 25 March 2004

European Parliament, 2001. *Recommendation of the European Parliament on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer related Crime (2001/2070(COS))*, adopted on 6 September 2001, A5-0284/2001

European Parliament, 2005a. *European Parliament legislative resolution on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, adopted on 27 September 2005* (8958/2004 – C6-0198/2004 – 2004/0813(CNS))

European Parliament, 2005b. *Report of the Committee on Civil Liberties, Justice and Home Affairs on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, adopted on 31 May 2005 (8958/2004 – C6-0198/2004 – 2004/0813(CNS))

Electronic copy available at: https://ssrn.com/abstract=4216870

European Parliament, 2005c. *European Parliament legislative resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))*, adopted on 14 December 2005

European Parliament, 2014. *European Court of Justice judgment of 8 April concerning data retention (C 293/12 and C 594/12)*, *Debates*, 16 April 2014

European Parliament, 2020. R*esolution of 26 November 2020 on the situation of Fundamental Rights in the European Union - Annual Report for the years 2018 - 2019* (2019/2199(INI))

European Parliament Research Service, 2020. "General data retention / Effects on Crime", 27 January 2020

Fennelly, David, 2021. "Data Retention in Ireland", in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 137-154

Filipe, António MP (Communist Party), 2008. *Diário da Assembleia da República*, I, 31, 5 January 2008, 19-26

Gera, Matej and Martin Husovec, 2021. "Data Retention in Slovakia", in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 203-218

Grimm, Dieter, Mattias Wendel and Tobias Reinbacher, 2019. "European Constitutionalism and the German Basic Law", in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 407-492

Guerra, Clara and Filipa Calvão, 2015. "Anotação", *Forum de Proteção de* Dados, 1, July 2015, 77-80

Gustavo, Rui, 2022. "Procuradoria pede anulação do acórdão do Constitucional sobre os metadados. E apresentou dois motivos para o fazer", *Expresso*, 9 May 2022

Hijmans, Hielke, 2016. *The European Union as a constitutional guardian of internet privacy and data protection*, University of Amsterdam

Hornung, Gerrit and Christoph Schnabel, 2009. "Data Protection in Germany II: Recent decisions on online searching of computers, automatic number plate recognition and data retention", *Computer Law & Security Review Volume*, 25, 2, 115-122

Jones, Chris and Ben Hayes, 2013. *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness

Kashumov, Alexander, 2021. "Data Retention in Bulgaria", in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 75-84

Kombos, Constantinos and Stéphanie Laulhé Shaelou, 2019. "The Cypriot Constitution Under the Impact of EU Law: An Asymmetrical Formation", in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 1373-1432

Electronic copy available at: https://ssrn.com/abstract=4216870

Krunke, Helle and Trine Baumbach, 2019. “The Role of the Danish Constitution in European and Transnational Governance”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 269-315

Legal Service of the Council of the European Union, 2005. “Projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme - Base juridique”, 7688/05, 5 April 2005

Markou, Christiana, 2021. “Data Retention in Cyprus in the Light of EU Data Retention Law”, in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 85-100

McIntyre, T. J., 2008. “Data Retention in Ireland: Privacy, Policy and Proportionality”, *Computer Law & Security Review*, 24, 4, 326–334

Mota Delgado, Miguel, 2022. “The EU law of a Portuguese institutional crisis: the Data Retention ruling of the Portuguese Constitutional Court”, *EU Law Live*, 23 May 2022

Ojanen, Tuomas and Janne Salminen, 2019. “Finland: European Integration and International Human Rights Treaties as Sources of Domestic Constitutional Change and Dynamism”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 359-404

Ombudsman, 2019. Recommendation 1/B/2019, of 22 January

Ombudsman, 2021. “Lei n.º 26/2020. Provedora de Justiça requer a fiscalização do Tribunal Constitucional”, 16 September 2021

Peers, Steve, 2005. “The European Parliament and data retention: Chronicle of a ‘sell-out’ foretold?”, *Statewatch Analysis*, 1 December 2005

Pereira Coutinho, Francisco, 2020. “A Independência da Comissão Nacional de Proteção de Dados”, *Anuário da Proteção de Dados*, 9-47

Pereira Coutinho, 2022. “Better Late Than Never: Blanket Data Retention Struck Down at Last by the Portuguese Constitutional Court*”, Diritti Comparati,* 24 June 2022

Pereira Coutinho, Francisco and Nuno Piçarra, 2019. “Portugal: The Impact of European Integration and the Economic Crisis on the Identity of the Constitution”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 2019, 591-640

Pinho, Carlos, 2018. “Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?”, *Revista do Ministério Público*, 154, 167-192

Podkowik, Jan and Marek Zubik, 2021. “Data Retention in Poland”, in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 155-174

Polčák, Radim, 2021. “Data Retention in the Czech Republic”, in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 101-116

Electronic copy available at: https://ssrn.com/abstract=4216870

Popelier, Patricia and Catherine Van de Heyning, 2019. “The Belgian Constitution: The Efficacy Approach to European and Global Governance”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 1225-1270

Portela, Irene and Maria Manuela Cruz-Cunha, 2010. “What about the Balance between Law Enforcement and Data Protection?”, in I. Portela and M. M. Cruz-Cunha (eds.), *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*, IGI Global, 1-18

Privacy and Civil Liberties Oversight Board, 2014. “Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court”, 23 January 2014

Ray, Michael, 2022a. “Madrid train bombings of 2004”, *Encyclopedia Britannica,* 4 Mar. 2022

Ray, Michael, 2022b. “London bombings of 2005”, *Encyclopedia Britannica,* 30 Jun. 2022

Şandru, Simona, 2021. “Data Retention in Romania”, in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 189-202

Security Council, 2001. S/RES/1373 (28 September 2001)

Servant, Ariadna Ripoll, 2013. “Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision”, *Journal of European Public Policy*, 20, 7, 972-987

Silva Ramalho, David and José Duarte Coimbra, 2015. “A declaração de invalidade da Diretiva 2006/24/CE: presente e future da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves”, *O Direito*, 147, IV, 997-1045

Silveira Alessandra and Pedro Miguel Freitas, 2017. “The recent jurisprudence of the CJEU on personal data retention: implications for criminal investigation in Portugal”, *UNIO – EU Law Journal*, 3, 2, 45-56

Silveira, João Tiago (Secretary of State for Justice), 2008. *Diário da Assembleia da República*, I, 31, 5 January 2008, at 19-26

Toplak, Jurij, 2021. “Data Retention in Slovenia”, in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 219-225

Türk, Alexander, 2009. *Judicial Review in EU Law*, Elgar

Van de Heyning, Catherine, 2021. “Data Retention in Belgium”,in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 53-74

Vikarská, Zuzana and Michal Bobek, 2019. “Slovakia: Between Euro-Optimism and Euro-Concerns”, in A. Albi and S. Bardutzki (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, 835-886

Electronic copy available at: https://ssrn.com/abstract=4216870

Violante, Teresa, 2021. “Data Retention in Portugal”, in M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Law*, Springer, 175-188

Violante, Teresa, 2022. “How the Data Retention Legislation Led to a National Constitutional Crisis in Portugal”, *Verfassungsblog*, 9 June 2022

Zubik, M., J. Podkowik and R. Rybski (eds.), 2021. “The Constitutional Court of Romania: Judgment of 8 October 2009, Ref. No. 1258/2009”, *European Constitutional Courts towards Data Retention Law*, Springer, 350-356

Electronic copy available at: https://ssrn.com/abstract=4216870