This is an Accepted Manuscript of an article published by Cambridge University Press in the European Constitutional Law Review (2019) 15:1, 14-157, available online: https://doi.org/10.1017/S1574019619000038

The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios

Edoardo Celeste*

Data retention saga – Interpretative strategy of the Court of Justice – Expansive potential of the principles set by the Court of Justice – 'Reverse' *effet utile* and conflict of competence – EU acts under threat – Domino effect on national security measures – Future scenarios – Twilight of the model of bulk data retention – Modulation of the ban on bulk data retention according to the vulnerability of data processing or depending on the prior unknowability of the threats – Divergence from the European Court of Human Rights – Legitimisation of bulk data retention.

"*Equo ne credite, Teucri!*
Quidquid id est, timeo Danaos et dona ferentes"

— Virgil, *Aeneid*, II, 48-49

INTRODUCTION

'Beware of Greeks bearing gifts' warned Laocoön, priest of Apollo, trying to persuade his compatriots to be suspicious of what they believed to be a divine gift. Nevertheless, the Trojans pulled the wooden horse into the walls of their city, unaware of the consequences that would ensue.

The well-known story of the Trojan horse shares many elements with what has been deservedly defined as a modern 'saga'[1] and can ultimately be compared with a Virgilian plot: the Court of Justice's case-law on data retention. In *Digital Rights Ireland,* the Court of Luxembourg invalidated the contested Data Retention Directive, ruling that an indiscriminate system of bulk data retention is not compatible with EU law.[2] However, the model of bulk data retention provided by the Directive is not unique to this act. Bulk data retention represents a widespread paradigm, common to many law enforcement techniques. Hence, the core idea at the origin of the present investigation: the principles set by the Court of Justice in *Digital Rights Ireland* could be regarded as a sort of Trojan horse. This set of requirements, introduced in an apparently circumscribed case concerning a European directive, would have the potential to undermine a whole category of legal acts both at national and EU level, definitively condemning, in this way, the model of bulk data retention.

---

* PhD candidate at the Sutherland School of Law, University College Dublin; Irish Research Council Government of Ireland Postgraduate Scholar. I am grateful to those who attended the panel 'Regulating surveillance' at the Amsterdam Privacy Conference 2018 for their thought-provoking questions on an earlier version of this paper. I would also like to thank my supervisor, Dr TJ McIntyre, and three anonymous reviewers for their helpful comments and suggestions.

[1] M. Cole and F. Boehm, 'EU Data Retention – Finally Abolished?, Eight Years in Light of Article 8', 97 *Critical Quarterly for Legislation and Law* (2014) p. 58 at p. 78.

[2] ECJ 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*.

This paper illustrates the extent of this expansive potential by examining the interpretative strategy adopted by the Court of Justice in its case-law. In this way, the article aims to ultimately explore what the potential consequences for the model of bulk data retention could be in the future. While, at first sight, the case-law of the Court will seem to point out towards an imminent twilight of bulk data retention, a deeper analysis will reveal that, in fact, this expansive trend is fragmented, and that the apparently unescapable destiny of bulk data retention is more uncertain.

The first section of this paper will analyse the *Digital Rights Ireland* case, in which the Luxembourg Court first outlawed the model of bulk data retention, and will explain how the principles then established by the Court can have an expansive potential *à la* Trojan horse. The second section will consider the first wave of this expansive trend along with the first adjustments introduced by the Court. In *Tele2 Sverige*,[3] the Luxembourg judges *de facto* applied the *Digital Rights Ireland* principles to national statutes implementing the invalidated Data Retention Directive. The recent judgment in *Ministerio Fiscal*,[4] in which the Court had to retouch one of the requirements set in its previous case-law, instead shows us that this expansion is not straightforward, and that doubts at national level still persist. We will then focus on the further expansive potential of the Court of Justice's ban on bulk data retention. The third section will contend that, by generating a sort of domino effect, it risks undermining a considerable number of other EU and national acts. To support this claim, the Court's opinion on the EU-Canada PNR Agreement[5] and the pending reference of the UK Investigatory Powers Tribunal in the *Privacy International* case[6] will be analysed. Finally, the last section will illustrate three potential future scenarios of this expansive trend. Our final question will be: will the Court of Justice's wooden horse eventually mark the end of bulk data retention? Interestingly, the answer will not be what one could expect. In light of the recent developments in the case-law of the European Court of Human Rights, it will be argued that holding an outright ban on bulk data retention no longer seems to be a realistic option. It will be suggested that the interaction between the two courts will probably lead to a re-modulation or to a progressive re-legitimisation of the bulk data retention model.

BANNING BULK DATA RETENTION

In the political climate of the war on terror, data processed by providers of telecommunications services became a valuable source of information for law enforcement authorities.[7] In the aftermath of the terrorist attacks in Madrid (2004) and London (2005), EU Directive 2006/24/CE, the so-called Data Retention Directive, eventually harmonised national legislation by establishing the categories of data that telecommunications providers ought to store, and the maximal retention period within which law enforcement authorities could access them before their deletion.

The Data Retention Directive was already under the scrutiny of the Court of Justice before the well-known case *Digital Rights Ireland*. Immediately after its adoption in 2006, Ireland, subsequently joined by Slovakia, asked the Court to review the validity of the legal basis chosen to pass the Directive.[8] Originally, a group of member states, including Ireland, had proposed to adopt a framework decision on data retention on the basis of what, before the Lisbon Treaty, was the third

[3] ECJ 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige*.

[4] ECJ 2 October 2018, Case C-207/16, *Ministerio Fiscal*.

[5] ECJ 26 July 2017, Opinion 1/15, *EU-Canada PNR Agreement*.

[6] ECJ (pending), C-623/17, *Privacy International*.

[7] *See* E. Herlin-Karnell, 'Case C-301/06, Ireland v. Parliament and Council, Judgment of the Court (Grand Chamber) of 10 February 2009', 46 *CML Rev* (2009) p. 1667; TJ McIntyre, 'Data Retention in Ireland: Privacy, Policy and Proportionality', 24 *CLSR* (2008) p. 326.

[8] ECJ 10 February 2009, Case C-301/06 *Ireland* v *Parliament and Council*.

pillar on police and judicial co-operation in criminal matters.[9] This legal basis would have excluded the European Parliament from the procedure of deliberation and would have offered that legal act only limited possibilities to be challenged before the Court of Justice.[10] Indulging the Parliament's request, the Commission eventually converted the decision into a directive and, consequently, the legal basis became the harmonisation of the internal market under the first pillar (Article 95 TEC). The Court rejected Ireland's claim. According to the Luxembourg judges, the Data Retention Directive only harmonised the rules relating to the processing of data by telecommunications service providers, and did not affect the activities of law enforcement authorities, which remained exclusively regulated by national law. Therefore, this act aimed to remove potential obstacles within the internal market, and the appropriate legal basis was the first, and not the third, pillar.[11]

Moreover, before *Digital Rights Ireland*, several member states' courts dealt with national statutes implementing the Data Retention Directive.[12] Although, in these cases, national legislation was always found – at least partially – unconstitutional, often because of the implications for the right to privacy, the validity of the Directive was never contested.[13]

The Digital Rights Ireland*'s principles*

Only in 2014, the Court of Justice examined the Data Retention Directive for the second time.[14] The Irish High Court and the Austrian Constitutional Court had stayed their proceedings to ask the Luxembourg judges to deliberate on the compatibility of the Data Retention Directive with EU fundamental rights. The Court of Justice, in a decision that immediately appeared destined to become a leading case, eventually invalidated the Data Retention Directive.[15]

The Court found that the Directive respected the essence of the right to private and family life and the protection of personal data enshrined in the Charter of Fundamental Rights. Despite the fact that an indiscriminate retention and potential use of traffic data could generate a feeling of 'constant surveillance',[16] the Directive did not affect the content of private communications. Furthermore, the Luxembourg judges held that the data retention regime undoubtedly pursued an objective of general interest, such as public security, but eventually concluded that it did not satisfy the so-called proportionality test. In particular, the Court identified a number of 'core failings' that prevented the Directive from attaining the necessary level of clarity and precision, which is required to justify a particularly serious interference to fundamental rights.[17]

More specifically, the Court held that the Directive:

---

[9] F. Boehm and M. Cole, 'Data Retention after the Judgment of the Court of Justice of the European Union', *Report to the Greens/EFA Group*, 30 June 2014, www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf, visited 25 June 2018.

[10] B. Nascimbene, 'European Judicial Cooperation in Criminal Matters: What Protection for Individuals under the Lisbon Treaty?' 10 *ERA Forum* (2009) p. 397.

[11] *See* S. Poli, 'European Court of Justice. The Legal Basis of Internal Market Measures with a Security Dimension. Comment on Case C-301/06 of 10/02/2009, Ireland v. Parliament/Council, Nyr', 6 *EuConst* (2010) p. 137; Herlin-Karnell, *supra* n. 7.

[12] *See* Cole and Boehm, *supra* n. 1.

[13] Ibid.

[14] *Digital Rights Ireland*, *supra* n. 2.

[15] *See* X. Tracol, 'Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) Thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws Which Enacted It', 30 *CLSR* (2014) p. 736.

[16] *Digital Rights Ireland*, *supra* n. 2, para. 37.

[17] J. Kühling and S. Heitzer, 'Returning through the National Back Door? The Future of Data Retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere', 40 *European Law Review* (2015) p. 263 at p. 264.

- allowed member states to introduce indiscriminate data retention regimes, and did not limit the *retention* to data that is at least remotely linked to a serious crime;[18]
- did not establish objective criteria to restrict the *access* and *use* of data by national authorities, and in particular did not foresee any prior review by a court or an independent administrative body;[19]
- did not provide for substantive and procedural safeguards relating to the *access* and subsequent *use* of data by national authorities;[20]
- imposed fixed ranges of retention periods, and did not allow national legislation to define them flexibly, according to the specific purposes of the retention;[21]
- did not lay down rules concerning the security of the data *retained* by electronic communication providers, and in particular did not provide for the irreversible destruction of data and for their storing within the EU.[22]

Trojan horse effect: reverse effet utile *and conflict of competence*

Digital Rights Ireland was immediately celebrated as a seminal case. It is impossible to neglect the euphoria surrounding the publication of the decision.[23] The Data Retention Directive was invalidated, and this was read as a triumph of fundamental rights on state prerogatives. Nevertheless, for the purposes of this paper, it is also important to highlight the other side of the coin. The principles set by the Court of Justice reveal our earlier Trojan horse comparison: having clear expansive potential towards a vast category of legal acts involving bulk data retention.

In particular, this was immediately perceived in relation to national implementing legislation. In *Digital Rights Ireland*, the Luxembourg judges identified a series of 'core failings' of the Directive. In this way, they indirectly laid down, what at first sight might seem, a series of requirements for the European legislator to shape a new directive fully in compliance with fundamental rights. Yet, since the Data Retention Directive had been transposed by member states in their national legislation, one is inclined to think that this set of principles also applies to these statutes. As is known, the Court of Justice can invalidate European acts, but not national law. However, in the present case, the European act at stake was a directive, which had been almost literally transposed into national law. The first conundrum was therefore whether the requirements set by the Court of Justice also applied to national law transposing the Directive, even after the annulment of the latter. In essence, if a sort of 'reverse' *effet utile* could work.[24]

Beyond this issue, there was a problem of conflict of competences. In *Ireland* v *Parliament and Council*, the Court originally distinguished between the retention of data operated by private actors, harmonised by the Directive, and the subsequent access and use of such data by national authorities, exclusively regulated by national law.[25] Interestingly, one can notice that in *Digital Rights Ireland* the Court *de facto* blurred this distinction. The judges correctly considered retention and access as two separate interferences with regard to the right to private and family life.[26] However, when listing

[18] *Digital Rights Ireland*, *supra* n. 2, paras. 58-59.

[19] *Ibid*., para. 60.

[20] *Ibid*., paras. 61-62.

[21] *Ibid*., paras. 63-64.

[22] *Ibid*., paras. 66-68.

[23] *See, e.g.*, M.-P. Granger and K. Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection', 39 *European Law Review* (2014) p. 835.

[24] Kühling and Heitzer, *supra* n. 17 at p. 274.

[25] *Ireland* v *Parliament and Council*, *supra* n. 8, para. 83.

[26] *Ibid*., paras. 34-35.

the main failings of the Directive, they eventually provided a hotchpotch of issues both related to retention and access, without considering the fact that the latter was in principle a matter of competence of the national legislator excluded from the scope of application of the Directive.[27] By deciding what the Directive was missing, the Luxembourg judges *de facto* set a series of requirements for public security authorities, intruding into an area of law in principle belonging to the competence of the national legislator.[28]

In particular, there was one specific prescription laid down by the Court of Justice that, above all, national actors were reluctant to subscribe to: the prohibition of a regime of bulk data retention.[29] In *Digital Rights Ireland,* the Court severely criticised the data retention regime instituted by the Directive whereby all traffic data had to be indiscriminately retained by electronic communications service providers, regardless of their potential connection with a criminal activity.[30] Interpreting this criticism as if the Court had wanted to definitively ban all kinds of bulk data retention, would have meant the end of a law enforcement paradigm that was widely used for a variety of purposes, from crime prevention to the fight against terrorism. Admittedly, from the wording of the judgment, it is not fully clear what the position of the Court was. There was indeed the option to think that bulk data retention was prohibited unless it was paired with a strict access regime providing the necessary guarantees.[31]

As a consequence of this politico-legal conundrum, member states reacted in multifarious ways. Some states tried to incorporate the *Digital Rights Ireland* requirements into their national law; some national courts quashed the respective legislation transposing the Directive in its entirety; other states unperturbedly maintained their law.[32] In this climate of legal uncertainty, urged by internal pressures from both public security authorities and privacy activists, the Administrative Court of Appeal of Stockholm and the Court of Appeal of England and Wales turned again to the Court of Justice to seek elucidation in the *Tele2 Sverige* case.[33]

FIRST EXPANSION, FIRST ADJUSTMENTS

As we have seen, national courts and legislators already perceived *Digital Rights Ireland* as imposing requirements on national data retention legislation, although this case technically concerned only a European directive. However, in the aftermath of this judgment, in many states there was significant reluctance to accept that the Court of Justice had definitively sacrificed the system of bulk data retention on the altar of fundamental rights, and that the Court had laid down specific requirements to be incorporated into national law. This doubtful attitude was supposed to end with *Tele2 Sverige.* In this case, the Court was indeed called to show the 'print of the nails' to its sceptical national colleagues, confirming a first expansion of the *Digital Rights Ireland* principles. Yet, the recent decision of the Court of Justice in *Ministerio Fiscal*, in which the Luxembourg judges had to clarify – not to say, rectify – some of the criteria established in *Tele2 Sverige*, is emblematic of the fact that this expansive trend is not completely straightforward, and that doubts and incertitude still persist.

---

[27] *See* Directive 2006/24/EC, Recital (25).

[28] See *Secretary of State for the Home Department* v *Davis MP & Ors* [2015] EWCA Civ 1185, paras. 101-103.

[29] *See ibid*., paras. 48 and 65.

[30] *Digital Rights Ireland*, *supra* n. 2, paras. 56-59.

[31] This was the position of the court of first instance in the *Davis* case. See *Secretary of State* v *Davis*, *supra* n. 41, paras. 48 and 65.

[32] For a comprehensive account, *see* Kühling and Heitzer, *supra* n. 17.

[33] *Tele2 Sverige*, *supra* n. 3.

Bulk data retention and national law: Tele2 Sverige

In 2015, the Court of Justice had the occasion to confirm the main principles set in *Digital Rights Ireland* in the *Schrems* case, where the Luxembourg judges assessed the validity of Commission's Decision 2000/520.[34] This act established that the safeguards provided by the United States under the so-called Safe Harbour regime offered an adequate level of protection for the purpose of legally transferring personal data from the European Union to American companies. In the aftermath of the Snowden revelations, Mr Schrems, the plaintiff in the main case, lamented the possibility of his personal data having being accessed and retained by United States' national security agencies in contrast to his right to data protection guaranteed by EU law. The Court eventually invalidated the Decision, arguing that legislation, such as that in force in the United States, which allows an indiscriminate access and storage of personal data transferred from the European Union, does not guarantee an adequate level of protection.[35]

In 2016, the Court of Justice came back more directly on the data retention issue in the *Tele2 Sverige* case. This time, the scenario the Court had to examine was quite different from *Digital Rights Ireland*. Firstly, the Court was asked to verify the compatibility with EU law of two national statutes, the Swedish and the British one. It is useful to remind oneself that, in such cases, the Court cannot directly invalidate national law. The Court limits itself to the interpretation of EU law, *de facto* ascertaining the abstract conformity of the national act with EU law, whilst the actual task of annulling national legislation is reserved to national courts.[36]

Secondly, EU law no longer included a set of provisions on data retention because, as we have seen, in *Digital Rights Ireland* the Court invalidated Directive 2006/24/EC. This observation is not inconsequential. The Court of Luxembourg does not exercise its jurisdiction, and the Charter of Fundamental Rights of the EU does not apply where national legislation falls outside the scope of EU law.[37] The national statutes at issue had been adopted to implement a no longer existing directive. If they were found to lie outside the scope of EU law because they did not implement any EU act, the Court could not have applied the Charter of Fundamental Rights and, ultimately, would not have had jurisdiction on the case. Consequently, in *Tele2 Sverige*, the Court had first to ascertain whether the national legislation at stake fell within the scope of EU law.[38]

Article 5 of Directive 2002/58/EC, the so-called ePrivacy Directive, provides for the principle of confidentiality of communications and related traffic data. However, Article 15 of the Directive allows member states to adopt legislative measures restricting this principle when necessary and proportionate to protect national security, defence, public security, and ensure the prosecution of criminal offences. In *Tele2 Sverige,* the Data Retention Directive was no longer available, therefore the Court could not argue that the Swedish and British statutes were implementing that text. Therefore, the Luxembourg judges held instead that such national legislation was exercising the derogation provided by Article 15 of the ePrivacy Directive.[39] Consequently, according to its

---

[34] ECJ 6 October 2015, Case C-362/14, *Schrems*.

[35] *Schrems*, *supra* n. 34, paras. 91-94.

[36] Article 267 TFEU; *see* P. Craig and G. de Búrca, *EU Law: Text, Cases, and Materials* (Oxford University Press 2015).

[37] Article 51(1) CFR literally reads: "The provisions of the Charter are addressed to […] the Member States only when they are *implementing* Union law" (emphasis added). However, the Court of Justice in its case-law has tended to broaden the scope of this provision, generally talking of member states' legislation 'within the scope of EU law'. *See* ECJ 26 February 2013, Case C-617/10, *Åkerberg Fransson*; F. Fontanelli, 'Hic Sunt Nationes: The Elusive Limits of the EU Charter and the German Constitutional Watchdog: Court of Justice of the European Union: Judgment of 26 February 2013, Case C-617/10 Åklagaren v. Hans Åkerberg Fransson', 9 *EuConst* (2013) p. 315. For a general overview, *see also* Craig and G. de Búrca, *supra* n. 36, pp. 410-419.

[38] *Tele2 Sverige*, *supra* n. 3, para. 64 ff.

[39] In January 2017, the European Commission issued a proposal for a new regulation on the protection of personal data in electronic communications aiming to repeal the current ePrivacy Directive. Article 11 of the proposed regulation reflects the terms of Article 15 of the ePrivacy Directive.

established case-law,[40] the Court concluded that a national statute implementing a derogation to EU law, like the British and Swedish legislation, falls within the scope of EU law.

In contrast to *Digital Rights Ireland*, the Court argued that a bulk data retention regime, such as that instituted by the analysed national law, represented a serious interference not only to Article 7 and 8 of the Charter of Fundamental Rights, but also to Article 11, which protects freedom of expression.[41] In *Tele2 Sverige,* the Court carried out a global assessment of the interference caused by a general and indiscriminate data retention regime, such as those at issue, without individually analysing the interference to every single right, as it did in *Digital Rights Ireland* and *Schrems*.[42]

The rest of the reasoning of the Court in *Tele2 Sverige* is similar to that of *Digital Rights Ireland*. The Court held that a data retention regime does not affect the essence of the fundamental rights involved since it does not concern the content of communications;[43] that the legislation at issue pursues an objective – the fight against crime – which is in theory capable of justifying an interference to those rights;[44] and that, nevertheless, a data retention regime which is not 'targeted', but general and indiscriminate, does not represent a necessary and proportionate measure.[45]

Essentially, this decision confirmed what the referring courts were afraid to believe the Court of Justice had meant in *Digital Rights Ireland*. Firstly, that bulk data retention is *per se* incompatible with EU fundamental rights, even if it is accompanied by a strict access regime. Only a system of 'targeted' data retention would conform to a combined reading of the ePrivacy Directive and the Charter of Fundamental Rights. Secondly, that national law providing for the retention and access of traffic data by state authorities is subject to a series of mandatory requirements established by the Court. In *Tele2 Sverige,* the Luxembourg judges converted the core failings of the invalidated Data Retention Directive into positive requirements for national legislation. Furthermore, even if the Court was cautious in the terminology used,[46] it is apparent that the judges laid down a set of mandatory conditions that national legislation on access by competent authorities should fulfil.

The requirements set in *Tele2 Sverige* essentially reflect those listed in *Digital Rights Ireland*, except for one additional condition. In the 2016 case, the Court also required competent national authorities to notify persons whose data has been accessed, unless this notification jeopardises their investigations.[47] Overall, there is nothing new under the sun – one may think. Yet, as we will see in the next section, both at national and EU level, these requirements really appear as a Copernican revolution.

Adjusting the Tele2 Sverige*'s principles:* Ministerio Fiscal

Ministerio Fiscal was a case referred to the Court of Justice by the Provincial Court of Terragona, and decided by the Grand Chamber in October 2018.[48] A Spanish citizen was seriously injured and,

---

[40] *See* ECJ 18 June 1991, Case C-260/89, *ERT*; Craig and G. de Búrca, *supra* n. 36, pp. 413-414.

[41] *Tele2 Sverige, supra* n. 3, para. 92 ff. *Cf* Opinion of AG Villalón, ECJ 12 December 2013, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, point 52.

[42] *Tele2 Sverige*, *supra* n. 3, paras. 92-93; *see* X. Tracol, 'The Judgment of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige and Watson Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level', 33 *CLSR* (2017) p. 541.

[43] *Tele2 Sverige*, *supra* n. 3, para. 101; *cf Digital Rights Ireland*, *supra* n. 2, para. 39.

[44] *Tele2 Sverige*, *supra* n. 3, para. 102; *cf Digital Rights Ireland*, *supra* n. 2, para. 44.

[45] *Tele2 Sverige*, *supra* n. 3, paras. 103 and 108; *cf Digital Rights Ireland*, *supra* n. 2, para. 57.

[46] For example, the Court prefers to talk about the circumstances in which electronic communication service providers should grant competent authorities access to retained data, instead of saying when competent authorities should have the power to access data; *see, e.g., Tele2 Sverige*, *supra* n. 4, paras. 118-119.

[47] *Tele2 Sverige*, *supra* n. 3, para. 121.

[48] *Ministerio Fiscal*, *supra* n. 4.

on the same occasion, robbed of his mobile phone. The police therefore decided to ask different telephone operators to check if a new line was activated on the stolen phone. However, the supervising judicial authority refused the police's request on the ground that traffic data could be accessed only in the presence of a serious crime. The Ministerio Fiscal, which is the Spanish public prosecutor, contested this decision before the Provincial Court of Terragona, who eventually referred the case to the Court of Justice. The proceedings before the Luxembourg judges were stayed until *Tele2 Sverige* was decided. Subsequently, the Spanish court confirmed its interest in the decision, considering that the position of the Court of Justice was still not clear.[49]

The central point of the issue before that Luxembourg Court was the compatibility of Spanish legislation with one of the *Digital Rights Ireland/Tele2 Sverige* prescriptions: requiring the presence of a *serious* crime in order to access traffic data. Spanish law defined a crime as serious if it entailed more than three years of imprisonment. The Provincial Court asked the Court of Justice whether such a criterion satisfied the standards of 'strict review' requested by *Digital Rights Ireland* in order to justify a restriction to the rights to personal and family life and to the protection of personal data.[50]

First of all, the Court of Justice had to demonstrate jurisdiction on the matter, showing that this longstanding issue is still contested. The Spanish government, supported by the United Kingdom, argued that the existing EU legislation explicitly excludes the activities of the state in the field of public security, such as the access by national authorities to data retained by commercial companies for the prevention of crimes, from the scope of EU law.[51] The Advocate General Saugmandsgaard Øe interestingly proposed a new technique to draw a dividing line between EU and national law in the context of law enforcement. He differentiated data directly processed by competent authorities from data first processed for commercial purposes, and subsequently accessed by national authorities.[52] The Court eventually reiterated the reasoning already presented in *Tele2 Sverige*, according to which national legislation implementing an exception to a European directive still falls within the scope of EU law.[53]

Secondly, it is apparent that the main issue in this case was generated by the vagueness of the expression 'serious crimes' adopted by the Court of Justice in *Tele2 Sverige*. This concept, if not accompanied by precise criteria, can lead to interpretative divergence at national level. As observed by the Advocate General, the Court recognised that the ePrivacy Directive does not require a crime to be serious in order to justify a restriction to the principle of confidentiality of communication.[54] Consequently, the Court of Justice had to clarify – not to say, rectify – its *Tele2 Sverige* prescription. The Luxembourg judges argued that, according to the principle of proportionality, only serious interferences to the rights to personal and family life and to the protection of personal data require to satisfy the criterion of the seriousness of the crime involved.[55] However, the Court held that, in the present case, the police only wanted to access names of SIM cards owners, and not to make any link with other traffic data, a situation that would have represented a serious intrusion in their private life. Therefore, the Luxembourg judges concluded that access by national authorities to this limited set of data did not constitute a serious interference to the relevant rights, and consequently did not require to demonstrate the seriousness of the crime involved.[56]

Last, but not least, it is interesting to notice that in this case the Court did not contest the underlying system of bulk data retention in place in Spain. Paragraph 49 of the final judgment and point 38 of

[49] *Ibid*., para. 27.

[50] *Ibid*., para. 26.

[51] Ibid., paras. 29-30. *Cf Ireland* v *Parliament and Council*, *supra* n. 8.

[52] Opinion of AG Saugmandsgaard Øe, ECJ 3 May 2018, Case C-207/16, *Ministerio Fiscal*, point 47.

[53] *Ministerio Fiscal*, *supra* n. 4, para. 34; *see Tele2 Sverige*, *supra* n. 3, paras. 72-74.

[54] *Ministerio Fiscal*, *supra* n. 4, para. 53.

[55] *Ibid*., paras. 55-56.

[56] *Ibid*. paras. 59-60.

the Opinion of the Advocate General stress that the Court is not called to deliberate on the conformity of the Spanish system of data retention with EU fundamental rights. It is possible to anticipate that this circumstance, together with other factors that we will consider in the last section, shows that the expansive potential of the Court's principles *de facto* presents a series of limits. The very architecture of the European judicial system, which does not allow the Court of Justice to go beyond the questions referred by national courts and prevents it from quashing national legislation, slows down and fragments the effective application of the data retention principles within the member states. This situation increases the state of uncertainty at national level, amplifies national divergence, and ultimately appears to be in stark contrast with the proactive approach that the Court adopted so far in the data retention saga.

FURTHER EXPANSIVE POTENTIAL

As we have seen in the first section of this paper, part of the doubts emerging at national level were due to the intrinsic expansive potential of the requirements imposed by the Court of Justice in *Digital Rights Ireland*. National courts and legislators immediately had the impression that those prescriptions, which theoretically referred to the Data Retention Directive, would have exercised a sort of 'reverse' *effet utile* on national legislation, as *Tele2 Sverige de facto* confirmed. Yet, the new principles laid down by the Court do not exhaust their expansive potential by influencing national legislation on traffic data retention in the field of public security. As we will explore in the next two sub-sections, there is evidence to claim that, in the coming years, the data retention saga will further expand in two directions, horizontally and vertically. In the first case, the requirements developed by the Court of Justice could potentially apply to EU acts implying forms of data retention. In the second case, there is the possibility that the Court's prescriptions will eventually affect other branches of member states' law that presuppose a system of bulk data retention, and in particular those regulating national security authorities.

EU acts under threat: EU-Canada PNR Agreement

Data retention is a common aspect to many law enforcement strategies at EU level. The obvious question that arises is therefore: why not extend the *Digital Rights Ireland* requirements to other EU acts implying data retention, even if they do not involve traffic data? As we have seen, the Court of Justice crafted this series of requirements in such a broad manner that they seem to be truly applicable in a general way. By doing so, one realises that the situation, also at EU level, is not rosy.

The examples – unfortunately – could be multiple. The agreement between the EU and US on the transfer of Passenger Name Record (PNR) data, Directive 2016/681 that establishes a system of collection and exchange of PNR data within the EU, the EU-US Terrorist Finance Tracking Programme, and the EURODAC's databases of biometric data of asylum seekers are all systems characterised by a general and indiscriminate collection of data, which are often not accompanied by a clear and precise definition of the categories of data that can be accessed by competent authorities, which lack mechanisms of independent review, and which provide for a fixed period data retention that is not proportionate to the aims effectively pursued.[57]

The risk that the *Digital Rights Ireland* requirements become the trump of the Luxembourg Court to invalidate these acts is no longer pure theoretical speculation. The recent Opinion of the Court on the EU-Canada PNR Agreement has already lifted the lid on the potential horizontal effects of *Digital Rights Ireland* on other EU acts.[58] The Opinion can be read as the EU's starting point in paying attention to the 'plank' in its own eye. In January 2015, the European Parliament asked the Court to

[57] For an accurate and comprehensive analysis of these measures, *see* Boehm and Cole, *supra* n. 9.

[58] Opinion 1/15, *supra* n. 5.

assess the compatibility of the EU-Canada Agreement on the transfer of Passenger Name Record (PNR) data with the right to data protection. Between 2006 and 2009, there was already a similar agreement in place.[59] It allowed Canadian competent authorities to process PNR data of passengers coming from the EU for public security reasons. Similarly, the new agreement would authorise Canadian authorities to obtain a selected amount of data from air carriers and to use them for five years in order to prevent terrorism and transnational crimes.

In July 2017, the Court of Justice held that the new agreement between EU and Canada was incompatible with the rights to private and family life and to the protection of personal data.[60] As in the case of traffic data, the Court found that the retention and use of PNR data does not affect the essence of these rights, but nevertheless represented an interference that should be adequately justified.[61] The main concern of the Court related to the processing of sensitive data.[62] The Luxembourg judges argued that the new agreement did not provide any solid justification for processing such data, also considering the potential risks deriving from a discriminatory use of sensitive information. Moreover, when assessing the use and retention of PNR data by Canadian authorities, the Luxembourg judges constantly referred to the requirements laid down in *Tele2 Sverige.*[63] The Court contested the fixed five years retention period, lamenting that, after the departure of unsuspected passengers, their data should be deleted and that, during their stay in Canada, retained data should be accessed only according to precise criteria and following a prior review of a court or an independent administrative body.

Domino effect on national security: Privacy International

Tele2 Sverige is emblematic of the expansive potential of *Digital Rights Ireland* in a vertical sense. The Court projected the requirements laid down in relation to the Data Retention Directive into the national dimension. In particular, *Tele2 Sverige* focused on national law on the retention and access of traffic data for public security purposes, and in particular for the prevention and repression of criminal offences. However, the Court of Justice established these requirements in such a general way that one could argue that they are indistinctly applicable to any branch of national law implying data retention. Therefore, including legislation regulating national security (i.e. intelligence) authorities. This was, in a nutshell, the claim promoted by the NGO Privacy International before the UK Investigatory Powers Tribunal, which, as it turns out, has recently referred some questions for preliminary ruling to the Court of Justice.[64]

In the aftermath of *Tele2 Sverige,* the British referring judge, Lord Lloyd-Jones of the Court of Appeal of England and Wales, at the very start of his judgment, wrote: 'I regret to say that the task now facing this court is far from easy in view of the fact that the preliminary ruling from the CJEU is lacking in clarity.'[65] This is emblematic of the mix of uncertainty and scepticism which followed *Tele2 Sverige.* The prescriptions of the Court of Justice, which were supposed to clarify those laid down in *Digital Rights Ireland* and translate them in the context of national law, were still perceived as problematic and, to a certain extent, inopportune. For example, the Court of Appeal of England and Wales eventually accepted to incorporate in its final decision only two of the various requirements

[59] *See ibid*., para. 14 ff.

[60] For an accurate and comprehensive analysis of Opinion 1/15, *see* M. Cole and T. Quintel, 'Data Retention under the Proposal for an EU Entry/Exit System (EES). Analysis of the impact on and limitations for the EES by *Opinion 1/15* on the EU/Canada PNR Agreement of the Court of Justice of the European Union', *Legal opinion for The Greens/EFA Group*, October 2017, hdl.handle.net/10993/35446, visited 28 June 2018.

[61] *Opinion 1/15*, *supra* n. 5, para. 150.

[62] *Ibid*., para. 164 ff.

[63] *Ibid*., para. 190 ff.

[64] *Privacy International*, *supra* n. 6.

[65] *Secretary of State for the Home Department* v *Watson & Ors* [2018] EWCA Civ 70, para. 7.

established by the Court of Justice in *Tele2 Sverige*. Namely, that '(1) access to and use of retained communications data should be restricted to the objective of fighting serious crime; and [that] (2) access to retained data should be dependent on a prior review by a court or an independent administrative body.'[66]

This choice was artificially justified by the appellate court in different ways, by arguing, for instance, that the Court of Justice was mainly referring to the Swedish legislation or that the specific point at issue had not been raised by the parties in the national proceedings.[67] However, another – and perhaps more decisive – consideration taken into account by the Court of Appeal in circumscribing the extent of its final decision was the fact that another British jurisdiction, the Investigatory Powers Tribunal, had in the meantime referred for preliminary ruling to the Court of Justice a series of questions on the same topic.[68]

The Investigatory Powers Tribunal is the British body that has jurisdiction over cases of alleged infringement of human rights, and in particular of the right to privacy, by law enforcement and national security authorities.[69] The NGO Privacy International brought a claim before the Investigatory Powers Tribunal challenging the British legislation allowing national security (i.e. intelligence) authorities to obtain and process bulk traffic data.[70] In particular, Privacy International argued that the requirements established by the Court of Justice in *Tele2 Sverige* also applied in the context of national security.

As we have seen, *Tele2 Sverige* examined the national legislation on the retention and access of traffic data for public security purposes, and in particular for the prevention and repression of criminal offences. In the specific case of the United Kingdom, access and use of traffic data by public security and national security authorities are regulated by two distinct pieces of legislation and entail two slightly different procedures.[71] For public security purposes, telecommunications operators retain traffic data and allow, when necessary, relevant authorities to access them; while, in the field of national security, telecommunications operators are required to transfer all traffic data to the competent authorities, which will then be responsible for the retention of such information. In other words, telecommunications providers do not retain traffic data for national security purposes, but directly transfer such data to the competent authorities. However, apart from these differences, the model of bulk retention and access of traffic data is essentially the same. For this reason, Privacy International requested to apply the *Tele2 Sverige* requirements also in the context of national security.

In its provisional conclusion, the Investigatory Powers Tribunal showed some reservations about this interpretation. In particular, the Tribunal claimed that national security falls outside the scope of EU law and that, in a previous case, it had already positively ascertained the compatibility of the British system of bulk data retention for national security purposes with the European Convention on Human Rights.[72] However, considering the Luxembourg judges' ambivalent wording in *Tele2 Sverige* and

---

[66] *Ibid*., para. 9.

[67] *See, e.g*., *ibid*., paras. 21 and 26.

[68] *See, e.g*., *ibid*., paras. 12, 19, 21, 26(3).

[69] *See* www.ipt-uk.com/default.asp, visited 12 July 2018.

[70] *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs & Ors* [18 October 2017] IPT/15/110/CH (UK IPT). The links to all the relevant judgments of the Investigatory Powers Tribunal on this case can be found at www.ipt-uk.com/judgments.asp?id=41, visited 12 July 2018.

[71] *Ibid*., para. 20.

[72] See, respectively, *Privacy International* v *Secretary of State*, *supra* n. 70, paras. 35 and para. 46 as well as *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs & Ors* [17 October 2016] IPT/15/110/CH (UK IPT).

the overall uncertainty surrounding the matter, the Tribunal, in agreement with both parties, saw the necessity to seek clarification from the Court of Justice.[73]

FUTURE SCENARIOS: THE END OF BULK DATA RETENTION?

The previous paragraphs have illustrated the expansive potential of the principles set by the Court of Justice in relation to bulk data protection. A series of requirements originally established to invalidate a European directive seems to be progressively extending to other EU acts, and even to fields of member states' legislation apparently beyond the scope of EU law. Will such an expansive trend ultimately mark the end of bulk data retention in Europe? This last section will discuss three possible forthcoming scenarios. Surprisingly, in light of the recent developments of the Luxembourg and Strasbourg courts, it will show that the end of bulk data retention seems now unlikely to occur.

Scenario A: The end of bulk data retention

In *Tele2 Sverige,* the Court held that Article 15 of the ePrivacy Directive, interpreted in light of Article 7, 8 and 11 of the Charter of Fundamental Rights, precludes national legislation providing for the general and indiscriminate retention of traffic data.[74] In contrast to the position of the court of first instance in the British case that led to *Tele2 Sverige*,[75] the Court of Justice did not admit the possibility of tolerating a system of general retention if it is accompanied by a strong set of guarantees in relation to the subsequent access by national competent authorities. In *Tele2 Sverige*, the Court *de facto* made the principles set with regard to the Data Retention Directive in *Digital Rights Ireland* applicable to national legislation, which, in that case, concerned the retention and the access to traffic data for public security purposes, and in particular for the prevention and repression of criminal offences.

Privacy International is emblematic of a further vertical expansive potential of the Court of Justice's interpretative strategy. This case concerns another branch of national law, that related to national security, i.e. to intelligence services' activities. A key passage of the interpretative strategy adopted by the Court of Justice to apply the *Digital Rights Ireland* principles in *Tele2 Sverige* was to consider national law regulating data retention as falling within the scope of application of EU law. In this way, the Court could affirm its jurisdiction and apply the Charter of Fundamental Rights. In light of the reference by the UK Investigatory Powers Tribunal, it is now essential to understand whether this reasoning could also be applicable in the context of national security.

There seems to be no reason for not extending this conclusion to member states' legislation regulating national security. One could argue that, in so far as competent authorities access data which has been previously processed by commercial operators, whether such data is retained by such operators or not, the ePrivacy Directive still applies. Consequently, the Court could consider the legislation regulating national security authorities' access, retention and use of personal data collected by commercial operators as implementing Article 15 of the ePrivacy Directive, and therefore falling within the scope of EU law.

If the Court of Justice took a similar position in *Privacy International*, and started reconsidering the validity of other EU acts involving bulk data retention, as we have seen in the previous section, one could instinctively think of a progressive twilight of the law enforcement model based on bulk data retention. However, as the next sub-sections will show, in light of the same opinion of the Court on the proposed EU-Canada PNR Agreement, and of the recent developments of the case-law of the

---

[73] *Privacy International*, *supra* n. 6.

[74] *See* text to n. 45 *supra*.

[75] *See* text to n. 31 *supra*.

European Court of Human Rights, a definitive end of the system of bulk data retention seems to be unlikely to happen.

Scenario B: Modulating the ban on bulk data retention

In the recent opinion on the new EU-Canada PNR Agreement, the Court of Justice constantly referred to the requirements laid down in *Tele2 Sverige*. This is why, as we have seen in the previous section, this text at first sight appears as evidence of the expansive potential of the *Digital Rights Ireland* principles in relation to other EU acts involving bulk data retention. Nevertheless, one can notice that the Court, in fact, validated the possibility of Canadian authorities to obtain and process with electronic means the PNR data of *all* passengers coming from the EU, regardless of the existence of a link to public security concerns.[76] The Court justified this choice, arguing that 'the exclusion of certain categories of persons, or of certain areas of origin, would be liable to prevent the achievement of the objective of automated processing of PNR data'.[77] In other words, according to the Luxembourg judges, limiting the amount of PNR data would undermine the effectiveness of controls at the borders. Moreover, the Court did not object to the subsequent bulk retention of such data, provided that it lasts until the moment of departure of passengers.[78] Implicitly, therefore, the Luxembourg judges recognised the utility of the model of bulk data retention.

At first sight, such a position appears to be inconsistent with the previous case-law. As we have seen, in *Tele2 Sverige* the Court categorically excluded the admissibility of any bulk retention of data, even if it is accompanied by strict rules on its subsequent use. Unless one hypothesises that the Court is extensively reconsidering its unconditional prohibition and exploring new avenues of balancing digital privacy and national security, this change could be explained as a first attempt to modulate the ban on bulk data retention.

There could be two potential avenues to achieve this objective. The first way could be by introducing a hierarchy of vulnerability of data processing. According to this criterion, on the one hand, bulk processing of traffic data would be inadmissible because of the amount of data that they are able to disclose. On the other hand, the bulk retention of data, such as PNR data, which are able to reveal only a limited amount of information about the data subject, could be derogatorily admitted because of their limited level of intrusion into private life. A second way, then, could be to assess the necessity and proportionality of bulk data retention. In the context of national security, for instance, potential threats are not previously known and, consequently, a more targeted collection of data would be impossible. Therefore, in so far as a system of bulk data retention is made necessary by the unknowability of the threats, and its proportionality is justified by the nature of such threats, one could imagine that in similar contexts the ban on general retention of data could be relaxed. *A contrario*, one could argue that the general and indiscriminate access to data would not be justifiable in the case of investigation of criminal offences, since crimes have already occurred and, therefore, a limitation of the data to be retained and accessed is possible.[79] A similar method of reasoning could be very useful in deciding *Privacy International.* The provisional position of the referring court, the UK Investigatory Powers Tribunal, follows this line,[80] and suggests a potential way for the Court of Justice to distinguish *Privacy International* from its previous case-law.[81]

---

[76] *Opinion 1/15*, *supra* n. 5, paras. 168 ff. and 186 ff.

[77] *Ibid*., para. 187.

[78] *Ibid*., para. 196 ff.

[79] *Cf* the view taken in ECtHR 12 January 2016, Application No. 37138/14, *Szabó and Vissy* v *Hungary*, paras. 18-20.

[80] *Privacy International* v *Secretary of State*, *supra* n. 72, paras. 8 ff. and 56.

[81] *See ibid*., para. 14.

Scenario C: Re-legitimising bulk data retention

One of the questions referred by the Court of Appeal of England and Wales to the Court of Justice was if the prescriptions established in *Digital Rights Ireland* really intended to go beyond what the jurisprudence of the Strasbourg Court required.[82] The Court of Appeal argued that if the criteria laid down by the Luxembourg judges were considered as mandatory, this would have meant a 'dramatic departure' from the case-law of the Strasbourg Court.[83] Considering member states' laws related to national security as lying outside the jurisdiction of the Luxembourg Court, the main concern of the Court of Appeal was that the application of the *Digital Rights Ireland* requirements could create an unjustified and complicated discrepancy between the standards applied to national legislation requiring telecommunications operators to retain data, on the one hand, and that regulating the access and use of personal data by national authorities, on the other hand.

In *Tele2 Sverige,* the Court of Justice succinctly answered that EU law is not prevented from providing further guarantees, especially with regard to the right to protection of personal data, which is not enshrined in the European Convention on Human Rights.[84] Beyond that, the Court did not fully assess the eventuality suggested by the British court, founding the issue as general or hypothetical.[85] However, concretely, while until recently the substantive difference between the two courts in relation to data retention was rather limited, two new cases decided in 2018 by the European Court of Human Rights seem to outline a picture of interpretative divergence between Luxembourg and Strasbourg, which is similar to that prefigured by the Court of Appeal of England and Wales. Our third and last scenario will analyse this situation.

Until not long ago, the case-law of the Strasbourg Court seemed to have followed the Court of Justice's 'deep pass' with regard to the balancing of digital privacy and national security measures.[86] The mutual interaction between the two courts and their substantive alignment were apparent. On the one hand, the Luxembourg judges, both in *Digital Rights Ireland* and in *Tele2 Sverige*, paid due attention in referring to the relevant jurisprudence of the Strasbourg Court.[87] On the other hand, the European Court of Human Rights in the Grand Chamber case *Zakharov* v *Russia,*[88] which concerned the Russian system of interception of mobile phone communications, and, subsequently, in the case *Szabó* v *Hungary*, which focused on Hungarian antiterrorism secret surveillance measures,[89] applied a series of minimal requirements on national surveillance legislation which essentially corresponded to the prescriptions of the Luxembourg judges.[90]

Although the Strasbourg Court was never explicit on this point, its strong condemnation of national surveillance systems that do not specifically identify the categories of persons which could be potentially targeted led one to think that bulk interceptions or other large-scale collections of data could not be considered admissible under the Convention. This interpretation also appeared to be in line with the previous case-law of the Court involving the massive retention of biological samples.[91]

---

[82] *Tele2 Sverige*, *supra* n. 3, para. 59.

[83] *Secretary of State* v *Davis*, *supra* n. 28, para. 112.

[84] *Tele2 Sverige*, *supra* n. 3, para. 129.

[85] *Ibid*., paras. 130-132.

[86] M. Cole and A. Vandendriessche, 'From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance', 2 *Eur. Data Prot. L. Rev.* (2016) p. 121; *cf* P. Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR', 11 *European Law Journal* (2005) p. 365.

[87] See *Digital Rights Ireland*, *supra* n. 2, paras. 35, 54-55; *Tele2 Sverige*, *supra* n. 3, paras. 119-120.

[88] ECtHR 4 December 2015, Application No. 47143/06, *Zakharov* v *Russia*.

[89] *Szabó* v *Hungary*, *supra* n. 79.

[90] *Zakharov* v *Russia*, *supra* n. 88, paras. 228-236; *see Szabó* v *Hungary*, *supra* n. 79, para. 56.

[91] ECtHR 4 December 2008, Applications Nos. 30562/04 and 30566/04, *S and Marper* v *UK*, especially paras. 99, 103, 119. *See* Boehm and Cole, *supra* n. 9.

In conclusion, in light of *Zakharov* and *Szabó*, there were strong reasons to believe in a substantial convergence between the positions of the two courts. However, this scenario seems to have been now definitively overtaken.

In June 2018, the Third Section of the European Court of Human Rights assessed the compatibility of the Swedish legislation on signals intelligence with the Convention.[92] The Swedish system allows competent authorities to directly intercept, in bulk, communications content and related traffic data.[93] The Court held that legislation providing for the bulk interception of communications falls within the margin of appreciation that each state enjoys in deciding how to protect national security.[94] The Strasbourg judges underlined that both bulk and targeted interception systems can be potentially abused by national authorities and that, consequently, in both cases, the law should sufficiently determine their scope of application.[95]

After only three months, in September 2018, the First Section of the Court delivered its first judgment specifically related to the national authorities' access and use of traffic data collected by communications service providers in the case *Big Brother Watch and Others* v *United Kingdom*.[96] More generally, the Court had been asked to verify whether the whole UK secret surveillance system in force at the time of the Snowden revelations respected the Convention. The Strasbourg judges reiterated that a system of bulk interception of communications is not *per se* inadmissible by virtue of the wide margin of appreciation of the state in the field of national security.[97] In this judgment, the Court refused to include in the list of minimum requirements that a national interception regime should satisfy some of the principles set in *Tele2 Sverige*, such as the need to provide evidence of reasonable suspicion before intercepting communications, the presence of judicial authorisation, and the obligation to notify the individuals subject to interception.[98] In relation to traffic data, the argumentation of the Court was lamentably laconic. By way of a sophistic reasoning, the judges argued that the British system of access and use of traffic data violated Article 8 of the Convention because it lacked some of the requirements prescribed by the Court of Justice, and it could not be therefore considered 'in accordance with the law'.[99] In this way, if on the one hand, the Strasbourg Court *de facto* invited the UK to respect the ruling of the Court of Justice, on the other hand, it did not explicitly embrace the position of this court with regard to bulk data retention.

In light of these two recent cases, it rather seems that the Strasbourg Court espoused the view suggested by the UK Investigatory Powers Tribunal in the *Privacy International* case.[100] According to this vision, the nature of dangers that contemporary society faces legitimises the use of bulk interception and collection of data, as only these techniques can really help uncover otherwise hidden threats. The very issue would instead lie in setting the appropriate guarantees delimiting the power of national authorities to exploit this unprecedented amount of data. In conclusion, such a position contrasts with the outright ban on bulk data retention so far maintained by the Court of Justice. However, as reiterated by the Luxembourg Court in *Tele2 Sverige*, EU law is not prevented from providing a level of protection higher than that guaranteed under the Convention. Therefore, from a legal perspective, nothing forces the Court of Justice to make a step back, and to eventually align its position with the Strasbourg judges. Nevertheless, this scenario of divergence between the two courts

---

[92] ECtHR 19 June 2018, Application No. 35252/08, *Centrum för rättvisa* v *Sweden*.

[93] *Ibid*., para. 7.

[94] *Ibid*., para 112. *See* M. Dawson, *The Governance of EU Fundamental Rights* (Cambridge University Press 2017).

[95] *Centrum för rättvisa* v *Sweden*, *supra* n. 92, paras. 113 and 118 ff.

[96] ECtHR 13 September 2018, Applications Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and Others* v *United Kingdom*.

[97] *Ibid*., paras. 314-316.

[98] *Ibid*., para. 316. *Cf Tele2 Sverige*, *supra* n. 3, paras. 119-121.

[99] *Big Brother Watch* v *UK*, *supra* n. 96, paras. 466-467.

[100] *See* text to n. 80 *supra*.

could be *de facto* mitigated if, in *Privacy International*, the Court of Justice modulated its ban on bulk data retention, as we have described in Scenario B, adopting, in this way, a decision more in line with *Big Brother Watch.*

CONCLUSION

Bulk data retention is a product of our times: it has been made possible by the recent advancements of technology, and it substantiates a long-lived idea of preventive state. The fact that it is a common technique to many law enforcement strategies explains why the principles laid down by the Court of Justice in *Digital Rights Ireland* with regard to a European directive are gradually being applied to other areas of law. The recent opinion of the Court in the EU-Canada PNR Agreement and the pending case referred by the UK Investigatory Powers Tribunal are emblematic of a twofold expansive potential of the *Digital Rights Ireland* principles. On the one hand, horizontally, other EU acts implying bulk data retention techniques are under threat; and on the other hand, vertically, the principles developed by the Court risk affecting established practices at national level, especially in the domain of national security. The Luxembourg judges are conducting a proactive policy, courageously overtaking potential limitations imposed by the limited scope of application of EU law. In this way, traditional strongholds of member states' power, such as public and national security, are being swallowed up into the scope of application of EU law in order to apply the principles of the Charter of Fundamental Rights. Taken alone, this expansive trend of the Court's principles seems to suggest an imminent twilight of the model of bulk data retention. One may think that it is a matter of physics that, once a couple of cards are removed from the base of the house, the entire construction will collapse.

However, practically, the Trojan horse fabricated by the Court of Justice to eradicate bulk data retention in Europe shows a series of flaws. A deeper analysis of the case-law reveals that this expansive trend is fragmented, and that the apparently unescapable destiny of bulk data retention is more uncertain. Firstly, the very architecture of the European judicial system, which does not allow the Court of Justice to go beyond the questions referred by national courts and prevents it from quashing national legislation, slows down and fragments the effective application of the data retention principles at national level. As we have seen in *Ministerio Fiscal*, for instance, the Court could say nothing about the presence of a generalised system of bulk data retention in Spain. Secondly, the outright ban on bulk data retention seems to be loosened in situations, such in the PNR data case, which involve data processing of alleged lower vulnerability, or where strict substantive and procedural rules on access are present. A circumstance that leads to detect a progressive fragmentation of the position of the Court in relation to the model of bulk data retention. Thirdly, an even more complex scenario is emerging after the recent change of course in the case-law of the Strasbourg Court. Until recently, one could have described the relationship between the two courts as symbiotic in relation to bulk data retention. Only in 2016, the Strasbourg judges held that general surveillance could no longer be considered as the '*deus ex machina*' in fighting terrorism and serious crimes, and reiterated their warning against an Orwellian nightmarish future society.[101] Nevertheless, the European Court of Human Rights, in two 2018 cases, seems no longer demonising bulk data retention. On the contrary, the Strasbourg judges temper the Court of Justice's position with pragmatism, arguing that bulk data use is not less intrusive than targeted surveillance and that, above all, it is a necessary technique in these times of terrorism and global crimes.[102]

[101] *Szabó* v *Hungary*, *supra* n. 79, para. 20.

[102] *Big Brother Watch* v *UK*, *supra* n. 96, para. 316.

In conclusion, a broader picture of this pan-European story provides plausibility for an imminent scenario of further confrontation between these opposite visions on bulk data retention.[103] Probably, a balancing exercise will eventually lead towards a mixed solution in which the ban on bulk data retention will be modulated according to the presence of specific guarantees or in relation to specific categories of data processing. In light of the recent jurisprudential trends, a similar scenario no longer seems to be a remote one. However, we know, sudden and unexpected changes in the plot are a characteristic of the best sagas.

[103] Beyond the *Privacy International* preliminary reference, there are other cases pending before both courts. *See* ECJ (pending), Case C-512/18**,** *French Data Network and Others*; ECtHR (pending), Applications Nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15, *Association confraternelle de la presse judiciaire* v *France* and 11 other applications; ECtHR (pending), Application No. 3599/10, *Tretter and Others* v *Austria*; ECtHR (pending), Application No. no. 50001/12, *Breyer* v *Germany*.