Reconsidering the blanket-data-retention-taboo, for human rights' sake?[1]

Belgian Constitutional Court offers CJEU chance to explain its puzzling Tele2 Sverige AB-decision

Compulsory retention, by ICT-providers, of all non-content user and traffic data, to ensure that that data will be available for subsequent use by law enforcement or intelligence, has been a controversial issue in the EU for several years now. On 19 July 2018 the Belgian Constitutional Court requested a preliminary ruling from the CJEU.[2] Basically, it asks the EU Court to further clarify its earlier case law. The Belgian constitutional judges indicate that they find some aspects of the CJEU's previous decisions puzzling and they also offer a new angle by explicitly linking the matter to the positive obligations of member states under the European Convention on Human Rights. The implied suggestion seems that the CJEU did not give those obligations enough weight when it found blanket data retention obligations disproportionate. Could this and other considerations push the CJEU to adjust its position as it continues to search for a legal regime that finds the right balance between data protection with law enforcement and intelligence interests?

1. 2006 Directive annulled by CJEU in '*Digital Rights Ireland*' (2014)

For detectives, communication and location data, from which they can deduce past correspondence partners or individuals' whereabouts at specific moments, have become a key source of information. Article 15(1) of Directive 2002/58/EC (also called *ePrivacy Directive*) allowed member states to enact **data retention legislation**, without making it compulsory.[3] To assure that such data would be available for law enforcement in all member states, the EU adopted in 2006 Directive 2006/24/EC which harmonised the data retention obligations of providers of electronic communication and networks.[4] In its landmark decision *Digital Rights Ireland* the CJEU found the Directive **incompatible** with the Charter of Fundamental Rights of the European Union (CFREU): '*By adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter*'.[5]

The decision sparked jubilant reactions from Big Brother-fearing NGO's and academics. Law enforcement agencies, intelligence services and governments reacted with disappointment verging on disbelief and sometimes even outright anger. Nuanced, yet optimistic academics[6] tried to bridge the gap by pointing out that the CJEU had not prohibited data retention as such. On the contrary, it

---

[1] This article was previously published at the European Law Blog, 1 October 2018, http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/.

[2] Belgian Constitutional Court 19 July 2018, no. 96/2018.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *OJ* 2002, L201, 46.

[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* 2006, L105, 54.

[5] Judgment Court of Justice 8 April 2014, C-293/12 and C-594/12, EU:C:2014:238, '*Digital Rights Ireland*', para. 69.

[6] 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", *E.L.Rev.* 2015, 40(2), 263-278 266; T. OJANEN, "Privacy is more than just a seven-letter word: the Court of Justice of the European Union sets constitutional limits on mass surveillance", *E.C.L. Review* 2014, 10(3), 528-541 540-541; 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", *E.L.Rev.* 2014, 39(6), 835-850, 848-849.

had explicitly allowed it,[7] albeit under **strict conditions** that definitely had not been met by the Directive.[8]

After the annulment of the 2006 Directive, the European Commission decided not to take any initiative for a new one. That implied that the matter was **left to the member states**, which could rely on the exemption in Article 15(1) of the ePrivacy Directive. Member states rewrote their legislation, taking into account the hints and reasoning of the CJEU in *Digital Rights Ireland*, but there was never any doubt that those new laws would also be challenged. Article 15(1) itself referred to the fundamental principles of EU-law and the annulment in *Digital Rights Ireland* was directly based on the CFREU. Hence, national legislation based on the ePrivacy Directive was obviously likely to face the same post-*Digital-Rights-Ireland*-scrutiny by the CJEU.

2. Member State Data Retention Legislation Incompatible with EU Law: '*Tele2 Sverige AB and Watson*' (2016)

Indeed, the CJEU did not have to wait long for member states' judges to request preliminary rulings on national data retention regimes. In its decision *Tele2 Sverige AB and Watson*, it found Swedish and British legislation incompatible with EU law.[9] If, using a boxing metaphor, *Digital Rights Ireland* had data retention legislation in the ropes, *Tele2 Sverige AB* really had it down on the canvas. Now everyone is counting to ten to see whether it is a definitive knock-out or whether data retention somehow manages to pull itself together and get to its feet again.

Recently, the CJEU has shed its light on the access to retained data, making clear that the preliminary question did not seek to determine if the retention itself was consistent with EU-law (para. 49).[10] In a case of violent robbery, the Provincial Court in Tarragona, Spain asked whether the seriousness of an offence, that can justify an interference such as access to personal data, can be determined by only taking into account the possible sentence. The Spanish Court moreover wanted to know what the minimum threshold would be in that case, for instance a minimum of three years' imprisonment.

The CJEU somehow rephrased this question into whether the access to data in order to identify the owners of SIM-cards activated with a stolen mobile phone, is a serious interference (para. 48). The Court has established that serious interferences can only be justified by the objective of fighting 'serious' crime (para. 56). Access to data that taken as a whole allow precise conclusions on the private lives of the persons whose data is concerned, entails a serious interference and can thus only be justified by the fighting of serious crime (para. 54). On the other hand, access to data leading to an interference that is not serious, can be justified by the fight against criminal offences in general (para. 57). In the view of the CJEU, the requested access to telephone numbers of SIM-cards and the identity of the owners of those numbers, could not entail a serious interference, because those data do not concern the content of the communication or the location of the phone (para. 59). Therefore, the objective of fighting crime in general is capable of justifying it.

This decision does not really convince, as the CJEU did not answer the preliminary question of the Spanish court. It is logical that more serious crimes justify more invasive interference. Nevertheless,

[7] "*It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest*." Judgment Court of Justice 8 April 2014, C-293/12 and C-594/12, EU:C:2014:238, '*Digital Rights Ireland*', para. 44.
[8] Judgment Court of Justice 8 April 2014, C-293/12 and C-594/12, EU:C:2014:238, '*Digital Rights Ireland*', para. 69.
[9] Judgment Court of Justice 21 December 2016, C-203/15 and C-698/15, ECLI:EU:C:2016:970, '*Tele2 Sverige AB and Watson'*.
[10] Judgment Court of Justice 2 October 2018, C‑207/16, ECLI:EU:C:2018:788.

the CJEU ducked the issue of how to determine the seriousness of an offence, by deciding that the interference in this case was not serious.

Another question on the scope of the *Tele2 Sverige AB* decision is pending at the CJEU.[11] In the United Kingdom, bulk communications data is only retained by the State's Security and Intelligence Agencies after the period of the ordinary business requirements. Non-targeted bulk techniques are said to be essential for the protection of the national security of the United Kingdom, mainly for counter-terrorism, counter-espionage and to counter nuclear proliferation. According to the national court, the safeguards surrounding the use of this data are consistent with the requirements of the ECHR. The requirements of the *Tele2 Sverige AB* judgment[12] would, in the opinion of the national court, frustrate the measures taken to safeguard national security. Therefore, the UK Investigatory Powers Tribunal judge asked the CJEU whether the requirement to providers of electronic communications networks that they must provide bulk communications data to the Security and Intelligence Agencies falls within the scope of the ePrivacy Directive. If so, the national court seeks to know how and to what extent the requirements of the *Tele2 Sverige AB* judgment apply, taking into account the necessity of bulk acquisition and automated processing techniques to protect national security. Meanwhile, the ECtHR has cast doubts on the starting point of the UK judges, i.e. the presumed consistency of the UK safeguards with the ECHR. It decided in the *Big Brother Watch a.o/United Kingdom* case that UK legislation on bulk interception and the regime for obtaining communications data from communications service providers violated both Articles 8 and 10 ECHR. A request for referral to the Grand Chamber of the ECtHR is pending.[13]

3. Belgian Law Challenged: Debate on the Interpretation of *Tele2 Sverige AB*

Belgium's first law on compulsory data retention had been struck down in 2015 by the Belgian Constitutional Court, in a judgment that almost copy-pasted *Digital Rights Ireland*.[14] A new version of the law, enacted on 29 May 2016, **quickly tried to solve the problems** identified by the Constitutional Court.[15] The Belgian federal government had sponsored the Bill and it was, already during the drafting process, very explicit that it tried to heed some of the suggestions made by the CJEU in *Digital Rights Ireland*.[16] But it also admitted that it had found it hard, and in some respects impossible or pointless, to follow all of them. The government's frustration reached a fever pitch when *Tele2 Sverige AB* decision explicitly banned blanket retention.

Belgium's Constitutional Court has to rule on a fresh series of requests for the annulment of the 'unconstitutional' data retention legislation, filed by NGO's and some professional associations. The latter felt that their fundamental right to secrecy and privileged communication had been violated, because no exceptions were made for the communications of lawyers, medical doctors or tax consultants.

---

[11] Reference for a preliminary ruling from the Investigatory Powers Tribunal - London (United Kingdom) 31 October 2017, C-623/17.

[12] Specified in § § 119-125.

[13] ECtHR 13 September 2018, nos 58170/13, 62322/14 and 24960/15, Big Brother Watch And Others/United Kingdom; R. CHESNEY, "The 'Big Brother Watch' Ruling on U.K. Surveillance Practices: Key Points from an American Perspective", 9 October 2018, https://www.lawfareblog.com/big-brother-watch-ruling-uk-surveillance-practices-key-points-american-perspective.

[14] Belgian Constitutional Court 11 June 2015, no. 84/2015.

[15] Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *Off.Gaz.* 18 July 2016.

[16] Wetsontwerp van 11 januari 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *Parl.St.* Chamber 2015-16, no. 54- 1567/001.

The Belgian Constitutional Court decided, in its decision of 19 July 2018, to ask the CJEU some interesting questions. It was no surprise that this 76 page decision contained extensive references to or quotations from the CJEU's decisions and the opinions of the Advocates General in *Digital Rights Ireland* and *Tele2 Sverige AB*. The Belgian constitutional judges **diagnosed the debate between those who challenged the 2016 law and the government who defended it** as a clash of different interpretations of *Tele2 Sverige AB*.

The **challengers** pointed out that after *Tele2 Sverige AB* there could be no doubt that compulsory retention of all data related to all people (so-called **blanket data retention) was as such, by definition, disproportionate**.[17] The CJEU would only allow data retention for preventive purposes in respect of specific groups and/or specific geographic areas with clear links to the purpose of data gathering: the fight against very serious crime and terrorism. Even for 'targeted retention practices', the petitioners stated, enough guarantees should be offered by law and – according to some of the Belgian petitioners – privileged professionals should get an overall exemption, or at least extra protection against the retention of metadata. The extra guarantees mentioned by the CJEU therefore only refer to 'focused', 'limited' retention duties. Blanket retention would be impossible because Article 15(1) ePrivacy Directive makes data retention the exception which has to be interpreted strictly. A generalised gathering obligation would turn that exception into the rule. It would therefore still be possible to order data retention in relation to a group of suspects or suspect communication tools or systems, in relation to and for the duration of a major event (sports, high profile or controversial visitors, concerts…). Even that kind of data gathering would be subjected to strict legal rules and control mechanisms.

The **Belgian government,** on the other hand, had its own reading of *Tele2 Sverige AB*. The CJEU had listed a number of shortcomings in the data retention rules which, ***taken together***, made the whole system disproportionate in its infringements of privacy and data protection rights. The Belgian government claimed that it was *wrong to single out* one of the elements in the list of shortcomings (for instance, the **blanket nature of the retention**) and decide that it, in itself, irremediably rendered the practice incompatible with the CFREU.[18] The challengers of the 2016 law, by contrast, made reference to the opinion of the Advocate General in in *Tele2 Sverige AB*, stating that the requirements set out in *Digital Rights Ireland* were mandatory, cumulative and minimal.[19]

4. Having the Data for Future Retroactive Use, Not Just for Terrorism or Serious Crime

The Belgian government suggests that the CJEU has not fully gripped the key feature of data retention laws as an addition to the already existing measures of focused, targeted gathering of data in the present or future. It is there to **make sure data from the past will still be available for (targeted) access**. When a **previously unknown** person drives a truck or van into tourists in Nice or Barcelona or another one dies in what at first impression had seemed a gas explosion, the authorities will try to go back and find out whom they talked with, where they have been, who rented the van etc. When a school child attempts suicide after having been bullied, or when its mother's private pictures are spread through social media, law enforcement wants to be sure the electronic traces that can help to identify or locate the perpetrator, will still be there. If a 15-year-old has gone missing, locating the mobile phone, the last activities and contacts through electronic communication will be crucial leads in the effort to find him or her. If a body is found after some

[17] O. LYNSKEY, "Tele2 Sverige Ab and Watson et al: Continuity and Radical Change", 12 January 2017, www.europeanlawblog.eu.
[18] Belgian Constitutional Court 19 July 2018, no. 96/2018, para. A.10.4.
[19] Belgian Constitutional Court 19 July 2018, no. 96/2018, para. A.9.3; Opinion of Advocate General Saugmandsgaard øe 19 July 2016, C‑203/15 and C‑698/15.

weeks and a suspect is identified after yet another few weeks, investigators should be able to control the whereabouts, alibi or communications in the period surrounding the alleged offence.

In the procedure before the Constitutional Court, the Belgian government insisted that you cannot know in advance which data you will need. That is why it deems it impossible to limit the gathering to defined groups or areas.[20] It even suggests that the definition of 'target groups' at the moment of gathering is likely to be (perceived as) discriminatory (paras A.8.3 and A.13.3). Immediately excluding all data related to lawyers, doctors or other privileged groups would be unfair, as they can also perpetrate offences or be victimised (para. A.5.7). Hence, the Belgian law maintains the obligation to make sure that all data will be retained (blanket retention), but only a very small portion of that data will actually be open to law enforcement requests or orders when the need arises. The only limitation on the gathering of these non-content data is a temporal one. In principle, the maximum term is 12 months.[21] The other human rights guarantees will therefore be available in the strict regulation of access and use. Only for the more serious offences or threats the authorities will be able to go back in time for 12 months. Regarding traffic data, they relate to the terrorist offences as defined by the Belgian Criminal Code. For access to data which might endanger legal or medical privilege, some extra guarantees are built in. Traffic data, for instance, can only be accessed if the lawyer or medical doctor is suspected of having committed an offence punishable by at least one year of imprisonment, or an offence committed within the framework of a criminal organisation, or if third persons are suspected of having committed such an offence, using their communication means. Moreover, the president of the bar council needs to be informed. Data covered by the privilege will not be included in the written report.[22]

The Belgian authorities thus strongly defend the rule that all data are kept, but only specific data will be accessed upon procedures with (some) guarantees. It is worthwhile noting that this rule also applies to access by intelligence services, which in Belgium are subject to quite strict regulations and quasi-judicial control.[23]

In its decision of 19 July 2018, the Belgian Constitutional Court decided to send three questions to the Court of Justice. First, it asks whether a general data retention obligation that is provided with storage and access safeguards, can be compatible with EU-law, when it is not only aimed at fighting serious crime, but also intended to safeguard national security, defence, public security, and to prevent, investigate, detect and prosecute other criminal offences. Second, the Court asks the same question as regards data retention legislation that would enable the state to fulfill its positive obligations to identify perpetrators of sexual child abuse, when they made use of electronic communication means, in order to effectively investigate and prosecute these crimes. When the Court of Justice should come to the conclusion that the Belgian legislation violates EU-Law, the Constitutional Court finally asks whether the consequences of the 2016 law can be maintained, in order to enable the further use of previously stored data, so that legal uncertainty can be avoided.

As such, the contested Belgian legislation might seem less invasive than the UK legislation at issue in the Reference for a preliminary ruling from the Investigatory Powers Tribunal - London (United Kingdom) made on 31 October 2017 in the case of *Privacy International v. Secretary of State for*

[20] Belgian Constitutional Court 19 July 2018, no. 96/2018, para. A.5.12.

[21] For identification data the starting point of this 12 months period is the latest date on which communication through the used service was possible (Art. 126 (3) Wet van 13 juni 2005 betreffende de elektronische communicatie, *Off.Gaz.* 20 June 2005) resulting in a much longer retention period than 12 months as was pointed out by one of the challengers (Belgian Constitutional Court 19 July 2018, no. 96/2018, para. A.3.4).

[22] Art. 88*bis* Code of Criminal Procedure.

[23] Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, *Off.Gaz.* 18 December 1998.

Foreign and Commonwealth Affairs and Others.[24] The UK intelligence community states that it actually needs the bulk data, albeit only those related to cross-border communication, i.e. that it has to analyse all the data to detect and find threats. That has a far bigger 'Big Brother ring' to it, but on the other hand the UK has traditionally adopted a stricter regime on the use of intelligence data: they cannot be used as evidence in criminal cases. Still, it would be quite remarkable if the CJEU accepted the UK's arguments while finding the Belgian law in violation of EU law.

Interestingly, all three member states which have made requests for a preliminary ruling in the aftermath of *Tele2 Sverige AB* - the UK, Spain and Belgium - stress that data retention is **not just needed for serious crime or terrorism**. The Belgian government, for instance, pointed out that the finding of missing persons (even when there is no suspicion of a criminal offence, for instance missing minors or mentally ill) might require access to the data. Emergency call handlers and authorities dealing with nuisance or abuse calls also profit, albeit that the access will be very specific and limited. The government even added that the invasion of privacy might favour not only victims, but also some suspects.[25] One can indeed think of situations where access to past data will allow the authorities to check or confirm whereabouts, to identify witnesses which could confirm their alibi, to establish that a suspect's computer system was tampered with, etc. Since CJEU stated in *Tele2 Sverige* that EU law precluded "national legislation which, *for the purpose of fighting crime*, provides for general and indiscriminate retention", other purposes are stressed by the Belgian government. Moreover, the ePrivacy Directive does also list other goals: to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC, that is no longer in force.[26]

It remains to be seen whether the proportionality test used by the CJEU will be affected by these considerations. Those who challenged the Belgian law, using quotes from the *Tele2 Sverige AB* decision, seem confident that if even terrorism and organised crime cannot justify blanket retention, *a fortiori* minor offences or issues cannot.

5. Positive Human Rights Obligation to Create Data Retention Legislation?

The most interesting aspect in the Belgian discussion is the use of **human rights as an argument in favour of data retention**. As it appears from the well-established case law of the European Court of Human Rights ('ECtHR'),[27] data retention and law enforcement access to that data can be necessary to ensure the effective protection by the member states of certain fundamental rights, especially with respect to (vulnerable) victims of crime. The ECtHR also seems to accept certain forms of bulk data gathering by States for the purposes of surveillance, as its 19 June 2018 decision in the *Centrum för Rättvisa v. Sweden* case has shown.[28] This does however not mean anything goes: in the recent *Big Brother Watch a.o/United Kingdom* case, the ECtHR decided that the UK legislation on bulk interception and the regime for obtaining communications data from communications service providers violated both Articles 8 and 10 ECHR.[29]

[24] Reference for a preliminary ruling from the Investigatory Powers Tribunal - London (United Kingdom) 31 October 2017, C-623/17.
[25] Belgian Constitutional Court 19 July 2018, no. 96/2018, para. B.20.1.
[26] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* 1995, L 281, 31.
[27] ECtHR 2 December 2008, no. 2872/02, K.U./Finland.
[28] ECtHR 19 June 2018, no. 35252/08, Centrum För Rättvisa/Sweden.
[29] ECtHR 13 September 2018, nos 58170/13, 62322/14 and 24960/15, Big Brother Watch And Others/United Kingdom.

Whereas economic freedoms and competition were at the heart of the historic case law of the CJEU, over the last decades and especially in the 21st century, the Court of Justice has insisted on the Union being built on core values, human rights, the rule of law and democracy. It becomes clear from decisions like *Kadi and Al-Bakaraat* (even the UN Security Council cannot simply override core EU fundamental rights),[30] the advisory opinion on the accession of the EU to the ECHR,[31] and from its concerns regarding the rule of law in Poland, accepting the refusal of mutual recognition if another EU member state does not respect judicial independence.[32] Some values may be accepted globally (at least in theory), other **fundamental rights** and especially their interpretation and power to limit the freedom of legislators and governments, are **distinctly 'European'**. The refusal of the death penalty is one of them[33], but nowadays **privacy and data protection** are probably the flagship. The CJEU has shown it is willing to play hardball in many sensitive cases: *PNR*,[34] *Google Spain*,[35] *Schrems*,[36] etc. *Digital Rights Ireland* and particularly *Tele2 Sverige AB* were yet another strong statement of the Court, especially after the Snowden and other revelations had shown that governments had secretly been eroding most of the fundamental privacy and data protection guarantees.[37]

With its first question (*supra*) the Belgian Constitutional Court somehow asks the CJEU whether, in its eagerness to stress data protection and the protection of privacy as a core EU value, it may perhaps have overstated its case. Should blanket data retention be banned whatever the interests are and even if strict storage, access and use regimes mitigate the impact on privacy and data protection?

That blanket data retention might be **necessary because of (positive) human rights obligations** of the member states under the ECHR, is a nice way to alter the framing of the problem. From a vertical conflict, between the authorities and the citizen who has to be protected against the massive powers, it becomes a horizontal conflict, in which one person's human right might be infringed as the price to protect another person's human rights. The ECtHR has insisted that positive obligations of member states are important for those individual rights to be effective. And effectiveness is of course also a key concept in the CJEU case law. The Belgian Constitutional Court refers to the decision in *K.U. v. Finland*, in which the ECtHR explicitly told member states to prioritise the protection of minors against (sexual) bullying over the protection of privacy of Internet users.[38] That seems difficult to render compatible with the blanket ban on data retention, so member states

[30] Judgment Court of Justice (Grand Chamber) 3 September 2008, C-402/05 P and C-415/05 P, 'Yassin Abdullah Kadi and Al Barakaat International Foundation'.
[31] Opinion Court of Justice (Full Court) 18 December 2014, no. 2/13, ECLI:EU:C:2014:2454.
[32] Judgment Court of Justice (Grand Chamber) 25 July 2018, no. C‑216/18 PPU, ECLI:EU:C:2018:586; S. MIRANDOLA, "European Arrest Warrant And Judicial Independence In Poland: Where Can Mutual Trust End? (Opinion Of The Ag In C-216/18 Ppu L.M.)", 24 July 2018, www.europeanlawblog.eu.
[33] E. VANDEBROEK and F. VERBRUGGEN, "The EU and Death Penalty Abolition: The Limited Prospects of Judicial Cooperation in Criminal Matters as an External Policy Tool", *New J.Eur.Crim.L.* 2013, 481-505.
[34] Opinion Court of Justice (Grand Chamber) 26 July 2017, no. 1/15, ECLI:EU:C:2017:592; A. VEDASCHI and C. GRAZIANI, "PNR Agreements Between Fundamental Rights And National Security: Opinion 1/15", 23 January 2018, www.europeanlawblog.eu.
[35] Judgment Court of Justice (Grand Chamber) 13 May 2014, Case C‑131/12, ECLI:EU:C:2014:317; O. LYNSKEY, "Rising Like A Phoenix: The 'Right To Be Forgotten' Before The Ecj", 13 May 2014, www.europeanlawblog.eu.
[36] Judgment Court of Justice 6 October 2015, C-362/14, ECLI:EU:C:2015:650; F. COUDERT, "Schrems Vs. Data Protection Commissioner: A Slap On The Wrist For The Commission And New Powers For Data Protection Authorities", 15 October 2015, www.europeanlawblog.eu.
[37] The curiousity that the *Tele2 Sverige AB and Watson* case was initially *Tele2 and Davies* is symbolicly important. David Davies, later a chief Brexiteer and minister for Brexit, actually invoked EU-law and in particular the CFREU against the UK legislation, adopted by the sovereign parliament in Westminster. Later on he was removed as an applicant from the case. One could forgive the CJEU for gloating a little over that irony and the recognition of the Charter's value even in the eyes of some of its most outspoken critics.
[38] ECtHR 2 December 2008, no. 2872/02, K.U./Finland.

would be caught between their obligations under the ECHR and under the CFREU. The CJEU has always been keen on avoiding such situations and on adjusting its judgments to the case law of the ECtHR to the largest extent possible. Avoiding dissonance between the Luxembourg and Strasbourg Courts is so fundamental to the rule of law in the EU that it might well deserve an elegant U-turn (if *Tele2 Sverige AB* banned all blanket data retention per se, which is to be clarified; *supra*) or at least a nuance of its *Tele2 Sverige AB* decision (if it did not).

6. Consequences of Illegal Gathering of Data: Exclusion of Evidence?

The answer to the final question (*supra*) from the Belgian Court will have an enormous practical impact if the CJEU explicitly (re)states the ban on blanket data retention: can the evidence be used in spite of the illegal gathering? Unlike the ECtHR, which has always given member states quite some leeway in the use as evidence of information gathered in violation of Article 8 ECHR, the CJEU seems to have used **effectiveness as an argument for an exclusionary rule** for evidence gathered in violation of fundamental rights.[39] It would be nice to know whether that 2015 judgment was a one off or that indeed the CJEU is willing to let some suspects walk away to underline the importance of the matter.

7. The Privacy Downside to Completely Ditching Blanket Data Retention

It is hard to predict whether the CJEU will speak out unequivocally against any blanket data retention, drawing a clear privacy line in the sand or rather adjust its position to align the human rights standards with those set by the ECtHR. Personally we would prefer the latter. Although we agree privacy is too easily dispatched with nowadays, a complete ban on blanket data retention, regardless of the conditions for subsequent access, might have undesired side-effects.

First of all, it will be hard to deny that law enforcement often needs the data. A radical prohibition of blanket retention will make EU member state authorities increasingly **dependent on (foreign) Internet service providers** ('ISPs'). For commercial or technical reasons, these private corporations may keep certain data for a certain period of time.[40] However, that will not necessarily be all the data law enforcement needs, as the commercial interests of the ISP's differ from the forensic ones of law enforcement. Ironically, public authorities would profit from the industry keeping more data than necessary. The ban on blanket retention would create a disincentive for governments to support their DPA's strict enforcement of data protection law, which often implies prompt deletion of data.[41] One could say that such a privacy-oriented policy is principled, but it might be counterproductive and therefore not exactly a smart policy for the era of 'smart technology'.

Another concern is that an EU-law-taboo on general data retention will also increase the dependence of **intelligence** agencies, especially those of small countries like Belgium, on information of foreign services that might not (or no longer) be bound by EU law or choose not to abide by it, for instance US, post-Brexit-UK or Israeli services which are important partners in the fight against terrorism and the so-called foreign fighters. Again, even if the human rights and accountability concerns behind the outright banning of blanket data retention are sincere, the remedy might be worse than the illness. Belgium has chosen to regulate data retention for both intelligence and law enforcement together in a single law. Should the CJEU inspire the Constitutional Court to annul the law, both would suffer. Whether a **national data retention obligation for intelligence purposes only** would be possible, is a very interesting question, as the matter of national ('internal') security is explicitly excluded from the

[39] Judgment Court of Justice 17 December 2015, C-419/14, ECLI:EU:C:2015:832, 'Webmindlicences'.
[40] For instance Art. 122 Wet van 13 juni 2005 betreffende de elektronische communicatie and Art. 5(1) ePrivacy Directive.
[41] Art. 6(1) and 6(2) ePrivacy Directive.

realm of Union law[42] and therefore beyond the protection of the CFREU. Whereas the Union through its annulled directive tried to create a level playing field for IT-service-providers in the single market, member state data retention regulations to protect national security might yet again fracture that market and complicate cross border business. Meanwhile, it will be interesting to see what the CJEU answers to the UK questions on the analysis of bulk data by intelligence services.

Finally, data retention regimes like the Belgian one oblige ISPs to keep and protect the data, while strictly regulating the access to that data by a restricted group of compliance officers within the corporation on the one hand, and by law enforcement authorities on the other hand. This set-up **avoids the storage of bulk data in a single, central government-run database**. Consequently, in the event of data leaks or hacking, compromising the integrity of the data, the damage will be more limited and easier to contain.

8. Conclusion

In the *Tele2 Sverige AB* decision, the CJEU seemed adamant when it ruled against blanked data retention as such. In its eagerness to stress data protection and the protection of privacy as a core EU value, the Court may have overstated its cases. For that reason, the Belgian constitutional judges offered a new angle by explicitly linking the matter to the positive obligations of member states under the ECHR. The Belgian Court suggested that the CJEU did not give those obligations enough weight when it found the blanket data retention obligations disproportionate.

Furthermore, the CJEU limited its decision to data retention for the purpose of fighting crime. If blanket data retention could exist for reasons of national security falling outside the scope of EU-law, the answer to the first question of the *Tele2 Sverige AB* decision would become moot. In some member states blanket data retention would probably continue to exist and that would again raise questions on the access to those data by law enforcement authorities. If it comes to that, the CJEU would do better to focus on guarding the rules on access to data that are already retained. In that regard, not only the answer to the questions in the Belgian case, but also to those asked by the UK Investigatory Powers Tribunal, are worth looking forward to.

Written by Frank Verbruggen, Sofie Royer and Helena Severijns

Frank Verbruggen is professor of European and International Criminal Law at the Institute of Criminal Law, KU Leuven. He studies the challenges posed to criminal law and procedure by digitisation.

Sofie Royer is a research and teaching assistant at the Institute of Criminal Law, KU Leuven, where she is working on a PhD thesis, “Criminal Seizure: Digiproof and (Multi)functional?” (Strafrechtelijk beslag: digiproof en (multi)functioneel?), under the supervision of prof. dr. M. Panzavolta and prof. dr. F. Verbruggen. Sofie is a member of the editorial board of the annotated criminal law code Strafrecht geannoteerd and frequently writes for the news section of the Belgian/Dutch journal, Tijdschrift voor Computerrecht. Sofie studied law at KU Leuven and spent one year at the University of Liège.

Helena Severijns recently joined the Leuven Bar Associaton. She works for ‘Viktor Advocaten’, a law firm specializing in criminal law and tort law. From 2016 to 2018 Helena was a fulltime research and teaching assistant at the Institute of Criminal Law at KU Leuven. She was a researcher for Eksistenz, a project funded by the EU Commission concerning identity fraud. Currently she is participating in a

[42] Art. 72 TFEU, recital 11 and Art. 15(1) ePrivacy Directive, recital 16 in the preamble to the GDPR.

study concerning the cooperation of service providers in criminal investigations. Helena still holds a part time assistant mandate at the KU Leuven.

Categories: Criminal law – Data Protection and Digital Governance – Fundamental Rights

Tags: Belgian Constitutional Court 19 July 2018 – Case no. 96/2018 – Data Retention – Prejudicial Question – Digital Rights Ireland – Tele2 Sverige AB and Watson – ePrivacy Directive