TILT (TILBURG INSTITUTE FOR LAW, TECHNOLOGY, AND SOCIETY)
LAW & TECHNOLOGY
WORKING PAPER SERIES

The Retention of Communications Data in Europe and the UK

Eleni Kosta

Tilburg Institute for Law, Technology, and Society (TILT)

e.kosta@uvt.nl

TILT Law & Technology Working Paper No. 001/2019
12 February 2019, Version: 1.0

7

The Retention of Communications Data in Europe and the UK

Eleni Kosta*

I. Introduction and Chronological Background

In the last chapter, we began to examine the state surveillance landscape that has evolved, diversified and expanded over the almost two decades since 9/11 and the rise of the 'war on terror'. In that, and previous chapters, we also highlighted the controversy and disquiet that has followed the whistleblowing revelations from Edward Snowden in 2013 of mass blanket surveillance of Internet users, in the EU and elsewhere, by a number of US and EU intelligence agencies.[1] In the backlash and loss of public trust that has followed these disclosures, the European Court of Human Rights (ECtHR) at Strasbourg and the Court of Justice of the European Union (CJEU) have played a major role in Europe in attempting to rein in unconstitutional powers used by state law enforcement and intelligence agencies to investigate crime and terrorism, using Art 8 of the European Convention of Human Rights (ECHR) and Arts 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR) as tools to restore confidence in fundamental rights.

In the last chapter, we focused on looking at the developing human rights scrutiny of state surveillance in these courts, notably the need for incursions into Art 8 of the ECHR in the name of security to be in accordance with law; undertaken for legitimate purposes; and 'necessary in a democratic society', ie proportional to the social need. Following this rubric, a number of far-reaching cases have effectively limited state powers of interception of the *content* of communications and access to *meta-data* connected to communications. In particular, in the last chapter, we highlighted the recent and crucial case of *Tele2/Watson*[2] in

* The author would like to thank Magda Brewczyńska for her assistance in the collection of the material for the writing up of this chapter, as well as Judith Rauhofer, who authored the relevant chapter for a previous edition of the book, and the editor, Lilian Edwards, for her invaluable feedback, insightful comments, assistance and guidance. Very helpful comments on a final draft were also received from Graham Smith of Bird and Bird. This chapter was completed before the decision in *Liberty v UK* [2018] EWHC 975 (Admin) on 27 April 2018.

[1] See further Ni Loideann at n 82 of the last chapter.
[2] Case C-203/15 and C-698/15 *Tele2/Watson* [2016] ECLI:EU:C:2016:970, Judgment of 21 December 2016.

the CJEU which lead (inter alia) to the UK Data Retention and Investigatory Powers Act (DRIPA) being declared invalid.

In this chapter, we focus on laws concerning *data retention* as opposed to interception or access. Communications data[3] (meaning *not* content, but data *about* communications, such as the time a call was made and from where, or to whom an email is sent) has historically been collected by those who provided communications services, ie telecommunications operators (fixed line and mobile) and Internet service providers (ISPs). More recently, other types of service providers, using the Web and the Internet as a medium for both text and voice communications (eg Facebook Messenger, WhatsApp, Skype) have become significant loci for private communications.

Historically, telecoms providers and ISPs only retained customer data for long enough to fulfil billing and complaints functions. There was no business case to do more, and storage costs. As a result, European governments, especially the New Labour UK Government lead by Tony Blair from 1997 to 2007, began to feel the need for laws to compel such providers to retain communications data longer, so it could be accessed by law enforcement agencies (LEAs) and intelligence agencies as this became necessary, eg when a terrorist incident occurred. Such data retention laws, were (and are), however, directly opposed to the data protection (DP) laws we studied in previous chapters which assert as a key principle that personal data should not be retained for longer than is necessary for the original purposes of processing. This patent conflict was partly resolved in Art 15 of the Privacy and Electronic Communications Directive 2002 (PECD)[4] which is discussed further below. The Madrid bombings in 2004 and the London subway bombings in 2005 then helped create a political environment which drove a pathway to a harmonised data retention law for the EU, and this new Data Retention Directive (DRD) was proposed as part of a package of measures during the UK presidency of the EU, at the end of 2005.[5]

---

[3] See further below for discussion of the exact meaning of this term and its equivalents in UK legislation.

[4] European Parliament and the Council of the European Union, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 (PECD) (31 July 2002). See also Chapter 5 of this volume.

[5] European Parliament and the Council of the European Union, Directive 2006/24/EC 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 [2006] OJ L105/54 (DRD) (15 March 2006). A draft framework Decision on Data Retention had been proposed in 2004, suggesting retention periods of one to three years, but this was rejected by the European Parliament.

The DRD[6] was adopted in 2006 and placed an obligation on providers of publicly available electronic communications services and of public communications networks (communication service providers or 'CSPs') to retain certain communications data for law enforcement purposes. The Directive regulated the retention of traffic and location data, as well as data necessary to identify the subscriber or registered user by CSPs, while making it clear that no *content* data should be retained under its provisions.

Article 15 of the PECD[7] allowed Member States, even before the adoption of the DRD (and still does), to adopt legislative measures for the retention of traffic and location data when such measures 'constitute [...] a necessary, appropriate and proportionate measure within a democratic society to safeguard national security […], defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system'.[8] These conditions under which data retention measures may be adopted significantly resemble the exceptions to the right to privacy laid out in Article 8(2) of the ECHR.[9]

The DRD met significant resistance during its adoption process by human rights organisations, privacy advocates and citizens regarding its compatibility with fundamental rights, and more specifically with the rights to privacy and data protection. After its adoption, numerous national courts declared unconstitutional specific provisions of the national laws transposing the Directive on the basis that they violate the rights to privacy and data protection.[10]

---

[6] DRD, *ibid.*

[7] PECD (n 4).

[8] Article 15(1) PECD. However, while the Directive was in force, a new Article 15(1a)—now defunct—effectively exhausted that right with regard to the retention of communications data for crime prevention purposes. That right therefore only resurged on the part of the Member States after the Directive was declared invalid in Case C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* ECLI:EU:C:2014:238, CJEU Judgment of 8 April 2014.

[9] Article 8 ECHR: '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

[10] Some of the early court decisions include judgments issued by the Bulgarian Supreme Administrative Court, the Romanian Constitutional, the German Constitutional Court, the Czech Constitutional Court and the Supreme Court of Cyprus.

In April 2014, in the case *Digital Rights Ireland*, discussed in detail below, the CJEU marked a turning point in the debate by invalidating the DRD.[11] The CJEU ruled that the DRD entailed a serious interference with the fundamental rights to privacy and data protection as protected in the CFR and that the EU legislature exceeded 'the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter'.[12] Mandatory safeguards were enumerated to protect privacy in any case of data retention legislation by the EU. The judgment of the CJEU did not automatically result in the invalidation of national implementations of the DRD. However, in some countries (such as the UK—see below) such laws were indeed open to challenge for loss of the empowering authority of the DRD after *Digital Rights Ireland*.[13]

In the UK, the main Act authorising UK authorities to carry out surveillance and investigation at the time of *Digital Rights Ireland* (and interestingly, promulgated even before 9/11) was the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA was a complex Act which had to be read with many other existing legislative acts, in particular, the Intelligence Services Act 1994, the Police Act 1997 and the Human Rights Act 1998.[14] RIPA dealt with both *interception* of the content and metadata of communications, and powers to *access communications data* (metadata) as well as the *grounds* for such access by various state agencies, were not always limited to LEAs or intelligence agencies.[15] Notably, under RIPA, the authorisation of interception was by executive power alone, with no judicial warrant needed; this was also the case in relation to authorising access to communications data, and indeed, in respect of some data, access was automatically permitted for a large number of state bodies including local authorities, health and safety authorities, etc. By many Continental standards, this was a highly permissive regime for the executive, with a very low degree of independent oversight, although as we noted in the last chapter it passed muster in the pre-Snowden days of *Kennedy v UK*[16] by virtue of having independent *post factum* review by the Investigatory Powers Tribunal (IPT).

---

[11] *Digital Rights Ireland* (n 8).

[12] *Digital Rights Ireland* (n 8) [65] and [69].

[13] For eg the Austrian Constitutional Court, the Constitutional Court of the Republic of Slovenia, the District Court of The Hague and Constitutional Court of the Slovak Republic ruled on (provisions of) the national data retention laws in light of the CJEU *Digital Rights Ireland* judgment.

[14] Explanatory notes to RIPA, para 5.

[15] Explanatory notes to RIPA, Ch 23, para 4. It also dealt with a number of non-digital investigative powers such as covert human intelligence sources and these parts of RIPA remain in force to this day—see discussion in Chapter 6.

[16] *Kennedy v UK* (2011) 52 EHRR 4. See discussion in Chapter 6.

RIPA did *not* deal with mandatory retention by telcos. At the time of, and prior to, the passing of the DRD, interception and access to data were seen as powers not delegated by states to the EU and part of their vital domestic security apparatus. As a result they were not harmonised across the EU and varied considerably among Member States. Retention on the other hand became, as a result of the above initiative and justified by the connection to EU e-privacy law in Art 15 (see chapter DP3), part of the corpus of EU law. In the UK, the DRD was implemented by a series of delegated statutory instruments, most notably the Data Retention Regulations 2009 (DRR 2009).[17] The 2009 Regulations required any public communications provider generating or processing communications data in the UK to retain the specific categories of data pertaining to its type of network or service[18] for up to 12 months.[19]

Historically, literature in the UK has thus tended to treat the issues of *retention* of data and *access* to data, as separable to some extent. However, as we saw in the last chapter, and will see further below, following *Tele2/Watson*, access and retention rules have become inextricably connected; and readers will have to decide if the separation of the topics in this book remains useful (arguably so, at least for UK readers, as access and retention are still dealt with in separate chapters of RIPA's successor, the Investigatory Powers Act 2016 (IPA)). Notably, the IPA now includes interception of communications, access to communications data *and* retention of such all in one instrument for the first time.

Following the annulment of the DRD by the CJEU in *Digital Rights Ireland*, confusion briefly reigned as to the status of national transpositions of the DRD. The UK initially maintained that the DRR 2009 might be independently viable[20], but fairly quickly plugged the gap by passing new emergency legislation, DRIPA in July 2014. The Act, confusingly, also took the opportunity to amend some parts of RIPA relating to interception and access to data which had become particularly sensitive (ie possibly illegal) in the light of the Snowden revelations and the *Digital Rights Ireland* case. Most of RIPA however at this point remained in force along with a plethora of various codes and guidance which had been developed alongside it.

[17] Data Retention (EC Directive) Regulations 2009, SI 2009/No 859.
[18] *Ibid*, reg 4. But see exemption in reg 10.
[19] *Ibid*, reg 5.
[20] Hansard HC Deb, 16 June 2014, c445W.

In December 2014, Members of the UK Parliament (MPs) Davis and Watson challenged the new 2014 UK data retention legislation in the courts.[21] The High Court issued a seminal decision declaring s 1 of DRIPA void on the basis, following *Digital Rights Ireland*, that it violated the mandatory safeguards laid down in that case, ie that (a) use of data retained was not restricted to purposes relating to *serious crime* only, and (b) access to data retained was not dependent on *prior review* by a court or independent body.[22]

On appeal, the Court of Appeal disagreed to some extent with the Divisional Court and felt there was room for doubt that *Digital Rights Ireland* had been intended to lay down mandatory rules for *national* legislation on access, as opposed to merely EU legislation (such as the DRD). It referred this and other questions to the CJEU, which were dealt with alongside similar questions relating to Swedish legislation, in December 2016, in *Tele 2/Watson*. Here, the CJEU took the position that the legality of mandatory data retention was dependent in part on the safeguards around *access* to data retained, which was not a matter harmonised by EU law. National data retention laws had to lay down 'clear and precise rules' about when access to retained data could be granted.[23] Such laws could not therefore be legal unless the important safeguards on access, which had been foreshadowed by the CJEU in *Digital Rights Ireland*, were in place.[24] This raised clear questions on the compatibility of the UK DRIPA with rights to privacy and data protection.

DRIPA, as emergency legislation, was set to expire on 31 December 2016.[25] At the end of 2016, on 29 November, in the nick of time before this 'sunset' clause cut in, an updated framework for the use of investigatory powers for interception, access and retention requirements was enacted in IPA.[26] Only a month later however, on 21 December 2016, the CJEU decided *Tele2/Watson* which, to the dismay of the UK Government, immediately made precarious the already controversial new rules of the IPA. The validity of the IPA, which in

---

[21] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092 (Admin), [2015] WLR(D) 318, Interveners' submissions, CO ref: CO/3794/2014, available at www.openrightsgroup.org/assets/files/legal/Intervention%20submissions%20ORG%20and%20PI%20in%20DRIPA%20case%2023.12.14.pdf.

[22] *Davis & Ors v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) [83], available at www.judiciary.gov.uk/judgments/david-davis-and-others-v-secretary-of-state-for-the-home-department; L Woods, 'High Court Strikes Down Data Retention Laws in Ruling on DRIPA' (2015)1 EDPLR 236 .

[23] *Tele2/Watson* (n 2) [109].

[24] Case C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C:2016:970, Judgment of 21 December 2016. See discussion in Chapter 6.

[25] DRIPA, s 8(3).

[26] IPA, Ch 25.

many parts replicated what had already been law in RIPA and DRIPA and in many places expanded further state power, has thus been controversial from day one.

The IPA received Royal Assent on 29 November 2016. The Investigatory Powers Act 2016 (Commencement No 1 and Transitional Provisions) Regulations 2016 (IPA Regulations 2016)[27] specified a number of provisions of IPA which would enter into force on 30 December 2016. Timing was critical here if a gap was not to be left in which data retention had no legal basis, in the eyes of the UK Government. Retention of communications data by CSPs in Part 4 of the IPA was thus in the main brought into force on 30 December 2016,[28] thus plugging the gap before DRIPA expired.[29]

Meanwhile, other parts of the IPA have been and are being brought in at a slower pace, as considerable work is involved, eg setting up and training the new Judicial Commissioners (see below). Chapter I of Part 1 of RIPA concerning *interception of communications* was replaced by Part 2 of IPA and Chapter I of Part 6 thereof. Acquisition of (access to) communications data from CSPs previously regulated by Chapter II of Part 1 of RIPA, is replaced by Part 3 of IPA. As of 8 March 2018, four delegated instruments[30] bringing into force parts of the IPA have been passed, including, on that date, the first provisions requiring 'double lock' oversight by Judicial Commissioners (see below). As we shall discuss below, the challenges, which killed the DRD and then the UK's DRIPA, are still very much alive, and may yet invalidate parts of the UK's new IPA.

II. The Data Retention Directive

Following a vigorous debate on whether the retention of traffic and location data was an issue that should be regulated under the first pillar, as an internal market instrument, or under the

[27] The Investigatory Powers Act 2016 (Commencement No 1 and Transitional Provisions) Regulations 2016, SI 2016/No 1233 (C 85).
[28] See n 24.
[29] Accordingly there is no need to refer to any non-mandatory codes on data retention which existed before RIPA or DRIPA such as the Voluntary Code on data retention made under Part 11 of Anti-terrorism, Crime and Security Act 2001 (ATCSA). Interestingly however, that Voluntary Code only required retention for 6 months, half the length of time the subsequent IPA regime can demand.
[30] See supra n 30SI 2017/No 17; SI 2017 No 859; SI 2018/ No 341.

third pillar, as an instrument relating to justice and home affairs,[31] the DRD was finally adopted on 15 March 2006.

The main aim of the DRD was the harmonisation of national laws on CSPs' obligations to retain communications data generated or processed by them so that they would be available for the purpose of investigation, detection and prosecution of serious crime.[32] The DRD itself did not include a definition of the term 'serious crime', which was left to the Member States to regulate in their national legislation. However the Council urged the Member States to have due regard to the criminal offences listed in Article 2(2) of the Framework Decision on the European Arrest Warrant[33] and crime involving telecommunications.[34]

The data to be retained were traffic data, location data and data necessary to identify the subscriber or registered user.[35] The content of a communication was specifically excluded from the retention requirement.[36] Crucially, traffic data relating to web browsing were *not* to be retained, as this invoked concerns that content not metadata was being retained. With regard to Internet traffic, the Directive only covered data relating to Internet access, Internet email and Internet telephony. The Directive provided that the data should be retained for a period between six months and two years from the date of the communication, with discretion left to Member States as to what period they chose within these bounds and for what type of data.[37]

The DRD required that retained data were to be provided only to the competent national authorities and in accordance with national law. Notably, the Directive left it to the Member States to specify the procedures to be followed and the conditions to be fulfilled in

---

[31] See *inter alia* Project de décision cadre sur la conservation des données – Analyse juridique' – (SEC(2005) 420) (March 22, 2005) and Commission Staff Working Document 'Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC Extended Impact Assessment' COM(2005) 438 final**,** available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005SC1131&from=EN (21 September 2005).

[32] DRD, Art 1(1).

[33] Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States [2002] OJ L190/1.

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

[35] A detailed list with the categories of data to be retained is contained in Article 5 of the DRD.

[36] DRD, Art 5(2).

[37] DRD, Art 6.

order for the competent national authorities to gain *access* to retained data.[38] These procedures and conditions had to be defined by Member States in accordance with the requirements of necessity and proportionality, in the light of the ECHR as interpreted by the ECtHR.[39]

A. Invalidation of the Directive

The controversy over the European regulation of data retention was apparent from the start with an early challenge in July 2006 from Ireland to the CJEU asking for the annulment of the DRD on the grounds that it had not been adopted on an appropriate legal basis for 'law- enforcement purposes'.[40] The Court however ruled that Article 95 of the Treaty of the Functioning of the European Union (TEC) was indeed the right legal basis for the data retention instrument and dismissed the case.[41]

National laws transposing the DRD were challenged in several Member States and in a number of cases from 2008 onwards, national courts declared them unconstitutional.[42] Eventually, the CJEU was requested to deliver preliminary rulings on data retention by the High Court of Ireland and the Austrian Constitutional Court. The CJEU summarised the main questions referred to it by the national courts as 'asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter'[43] and on 8 April 2014 delivered a seminal judgment that invalidated the DRD, commonly known as *Digital Rights Ireland*.[44]

The CJEU found that the obligation to *retain* the data already constituted interference with the right to privacy in itself[45] and that the data that could be retained under the Directive

---

[38] DRD, Art 4.

[39] *Ibid.*

[40] ECJ, Case C-301/06, ECR 2009 p I-593 *Ireland / Parliament and Council* ECLI:EU:C:2009:68, Judgment of 10 February 2009 [91].

[41] *Ibid* [93] and [94].

[42] Some of the early Court decisions include judgments issued by the Bulgarian Supreme Administrative Court, the Romanian Constitutional, the German Constitutional Court, the Czech Constitutional Court and the Supreme Court of Cyprus.

[43] *Digital Rights Ireland* (n 8) [23].

[44] *Digital Rights Ireland* (n 8).

[45] *Digital Rights Ireland* (n 8) [34].

were very detailed, allowing for the drawing of significant information about the citizens' habits and activities[46] including 'the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them'.[47] The Court found that the *access* of the competent national authorities to the retained data constituted a further interference with the right to privacy.[48] It thus found a *prima facie* interference with Articles 7 (private life) and 8 (processing of personal data) of the CFR, and then looked to see whether the interference with these could be justified under Article 52(1) CFR which allows interference where 'necessary and genuinely meet[s] objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.[49] However this interference also has to be proportional.

The CJEU found that the objective of the DRD, ie to contribute to the fight against serious crime and consequently to public security, was indeed an objective of general interest.[50] Proportionality was assisted by the requirement that retention of data was to be used only for fighting serious crime.[51]

However, the DRD as a whole resoundingly did not meet the standards of necessity and proportionality. First, the DRD provided for the *blanket retention* of the data of all citizens.[52] The Directive covered:

> … in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.[53]

It thus inevitably applied to some individuals whose conduct was not linked by any evidence to serious crime, and provided none of the exceptions that might be expected, eg for

---

[46] *Digital Rights Ireland* (n 8) [27].
[47] *Digital Rights Ireland* (n 8) [26]–[27].
[48] *Digital Rights Ireland* (n 8)[35].
[49] *Digital Rights Ireland* (n 8)[38].
[50] *Digital Rights Ireland* (n 8) [41] and [44].
[51] *Digital Rights Ireland* (n 8)[49].
[52] *Digital Rights Ireland* (n 8)[59].
[53] *Digital Rights Ireland* (n 8)[57].

communications subject to an obligation of professional secrecy such as between lawyer and client.[54]

Second, it facilitated *unlimited access* of competent national authorities that could further use the data 'for the purposes of prevention, detection or criminal prosecutions'[55] restricted only by the notion of serious crime. As that concept was not defined in the DRD, this left dubiety as to whether national rules would be proportionate.

Third, the CJEU criticised the fact that substantive or procedural conditions for *access to* and *use of* retained data were left to the national competent authorities and not mandatorily laid down by the DRD.[56] A crucial point in the CJEU judgment was the *absence of a requirement for a prior review* by a court or an independent administrative body before the competent authorities gain access to the data or use them.[57]

Fourth, the CJEU stressed the lack in the DRD of '*objective criteria* in order to ensure that [the retention period was] limited to what is strictly necessary'[58] Instead, states were given an unfettered discretion to set a data retention period without making any distinction between categories of data, based on either their potential value for the purposes pursued, or on the basis of the type of person involved.[59]

Fifthly, the CJEU criticised the fact that the level of protection and security of the data could be compromised due to economic considerations and in particular the lack of an obligation to irreversibly destroy the data at the end of the retention period. [60] Finally, the CJEU criticised the lack of a requirement for data to be retained within the EU, which might involve consequent lack of oversight.[61]

Following this reasoning, the CJEU concluded that "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"[62] and declared the DRD invalid. The DRD was declared

---

[54] *Digital Rights Ireland* (n 8) [58]–[59].

[55] *Digital Rights Ireland* (n 8)[60].

[56] *Digital Rights Ireland* (n 8)[61].

[57] *Digital Rights Ireland* (n 8)[62].

[58] *Digital Rights Ireland* (n 8) [64] (italics added).

[59] *Digital Rights Ireland* (n 8)[63].

[60] *Digital Rights Ireland* (n 8)[67].

[61] *Digital Rights Ireland* (n 8)[68].

[62] *Digital Rights Ireland* (n 8)[69].

retrospectively invalid from the date when it entered into force.[63] This did not directly or automatically affect the validity of all national data retention legislation,[64] but led to such invalidaiton following national court decision.[65]

III. UK Reaction to the *Digital Rights Ireland* Case

In the aftermath of the *Digital Rights Ireland* judgment, as outlined in the Introduction, the UK Government after a bare four days of Parliamentary process adopted in July 2014 DRIPA and its secondary legislation, the Data Retention Regulations 2014 (DRR 2014).[66] Two MPs, Davis and Watson, challenged DRIPA in the courts, claiming that DRIPA failed to meet the clear requirements of *Digital Rights Ireland*. Special attention was drawn to the width of the powers in DRIPA and the lack of concern for the confidentiality of communications with solicitors and constituents. [67]

On 17 July 2015, the High Court of Justice (Divisional Court of the Queen's Bench Division) declared[68] that as DRIPA was 'an identically worded domestic statute' to the repealed Regulations made under the DRD for the UK, it must be found, like the DRD, invalid.[69] Like the DRD, it did not meet the safeguards laid down by the CJEU in *Digital Rights Ireland*, particularly in relation to access, especially the lack of restriction to serious

---

[63] This was also confirmed in the Press Release of the Court on the cases: Court of Justice of the European Union, Press Release No 54/14, Luxembourg, 8 April 2014, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, n 2. See J Rauhofer and D Mac Sithigh, 'The Data Retention Directive Never Existed' (2014) 11 *SCRIPTed*; available at http://script-ed.org/?p=1480.

[64] Council of the European Union, 'Note from Eurojust to Council delegations on "Eurojust Analysis of the EU Member Stated" Legal Framework and Current Challenges on Data Retention', Brussels, 26 October 2015, 13085.

[65] Ibid p 4: The data retention legislation, or specific provisions of it, was invalidated in Austria, Belgium, Bulgaria, Germany, Lithuania, The Netherlands, Poland, Romania, Slovenia, Slovakia and the UK.

[66] Data Retention Regulations 2014, SI 2014/No 2042.

[67] *Davis* (n 22) [1].

[68] *Davis* (n 22).

[69] *Davis* (n 22) [83].

crimes, and the lack of independent prior review.[70] The High Court thus issued an order disapplying section 1 DRIPA from 31 March 2016.[71]

The UK Secretary of State for the Home Department appealed to the Court of Appeal[72] which decided to stay the proceedings and refer the case to the CJEU for a preliminary ruling. The CJEU was requested to answer whether the *Digital Rights Ireland* judgment laid down 'mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8' CFR.[73] This resulted in the next crucial CJEU judgment in this story, the *Tele2/Watson* judgment of December 2016, where the questions sent by the UK Court of Appeal were conjoined with a similar application from the Administrative Court of Appeal of Stockholm in Sweden.

IV. The *Tele2/Watson* Judgment

The questions the CJEU thus eventually examined asked in the round if *national* data retention legislation had to abide by the safeguards laid down in *Digital Rights Ireland* or whether they only restricted *EU* legislation.

The CJEU concluded that the list of objectives listed in Article 15(1) of PECD is exhaustive and that only the objective of fighting serious crime is capable of justifying access to retained data to safeguard 'the prevention, investigation, detection and prosecution of criminal offences'.[74] Any legislative measures taken to meet this objective should not exceed the limits of what was strictly necessary, in accordance with the principle of proportionality[75]

---

[70] *Davis* (n 22) [83].

[71] *Davis* (n 22) [122].

[72] *Secretary of State for the Home Department v Davis MP & Ors* [2015] EWCA Civ 1185, [2016] HRLR 1, [2016] 1 CMLR 48.

[73] *Ibid* [118]. The UK Court of Appeal asked a second question on the relation between Articles 7 and 8 CFR and Article 8 ECHR and in particular whether the *Digital Rights* judgment expands the scope of Articles 7 and/or 8 CFR beyond that of Article 8 ECHR, as established in the jurisprudence of the ECtHR. However, the CJEU in its 21 December 2016 judgment found the second question inadmissible.

[74] *Tele2/Watson* (n 2) [115].

[75] *Tele2/Watson* (n 2) [116].

and should contain specific rules on the circumstances and the conditions for access to retained data by competent national authorities.[76]

In particular, in *Tele2/Watson*, the CJEU clearly held that *national* legislation that permits *access* to mandatorily retained communications data must satisfy key minimum safeguards required by the CFR.[77] We examined these in part in the last chapter in relation to access and acquisition of data[78] but to recapitulate, *Tele2/Watson* addressed the issues of whether national legislation must:

- Require prior review by a court, or an independent administrative authority before access to or use of retained data can be made.[79]
- Only allow access to retained data in relation to individuals that are 'suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime'.[80]
- Require notification to affected persons as soon as such notification will not jeopardise the investigation.[81]
- Provide for a high level of protection of the retained data; providers shall take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Furthermore, data has to be retained within the EU and be destroyed at the end of the retention period.[82]

After *Tele2/Watson*, it became clear that DRIPA s 1 was effectively dead and that there would also be grave resulting challenges to the new IPA. In January 2018, the Court of Appeal formally declared that DRIPA s 1 was inconsistent with EU law, but explicitly only on the grounds that it did not restrict access to data only on the grounds of fighting serious crime, and that access was not subject to prior review by a court or an independent authority. As Ni Loideain noted in the previous chapter,[83] both of these findings left no doubt that Part 4 of the IPA on retention would now need to be urgently amended.[84]

---

[76] *Tele2/Watson* (n 2) [117].

[77] *Tele2/Watson* (n 2) [125].

[78] See Chapter 6 at xxx.

[79] *Tele2/Watson* (n 2) [120] and [123].

[80] *Tele2/Watson* (n 2) [119].

[81] *Tele2/Watson* (n 2) [121].

[82] *Tele2/Watson* (n 2) [122].

[83] See Chapter 6 at pXX.

[84] *Secretary of State for the Home Department v Tom Watson MP & Others* [2018] EWCA Civ 70.

Meanwhile in November 2017, after a year's intense work and consultation after *Tele2/Watson*, the UK Home Office published a package of suggestions for reform of the IPA to meet the *Tele2/Watson* requirements along with a draft statutory instrument and an evidence case for the need for, and productivity of, retention of communications data.[85] A plethora of applications to national courts, the CJEU and the Strasbourg court, as detailed in the last chapter, are still to come. There is no doubt at all that the whole concept of a blanket national data retention law is massively under siege in the post-Snowden world.

However, some commentators would assert that the Court of Appeal did not go as far as one would expect following *Tele2/Watson*, in that it did not declare the blanket retention of data intrinsically unlawful, nor did it establish a requirement that retained data should remain in the EU or that such data should be destroyed at the end of the retention period. As Ni Loideain pointed out in the last chapter, these questions were quite notably sidestepped. We wait now to see which existing challenges come to the CJEU and indeed what the impact of Brexit will be on all this, which may remove the CJEU as a determining final court from the table and may in time even exclude the jurisdiction of the ECtHR. In the meantime however, we turn to the last question, which is, post-DRIPA, how the IPA now attempts to regulate requirements for retention of data for the benefit of UK authorities.

V. Retention of Communications Data under the IPA 2016

Part 4 of IPA regulates the mandatory retention of communications data.[86] Part 4 was in the main brought into force on 30 December 2016 to replace DRIPA.[87] Graham Smith has commented that this part, controversially, considering the demise of the DRD, actually 'extends existing powers under [DRIPA] and revives elements of the draft Communications Data Bill on which the pre-2015 Coalition government was deadlocked'.[88]

---

[85] See www.gov.uk/government/consultations/investigatory-powers-act-2016.

[86] As well as the main text, six new Codes of Practice are being drafted to deal with the IPA— see summary of responses to consultation issued December 2017 with revised draft Codes, *Investigatory Powers Act 2016: Response to Home Office Consultation on Investigatory Powers Act Codes of Practice*, available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/668943/Response_to_the_IPA_codes_consultation.pdf. However, the *Code of Practice on Access to Retained Communications Data* made under s 71(4) of RIPA and adopted in March 2015, which previously related to the powers and duties conferred or imposed under Part 1 of DRIPA and the DRR 2014, remains currently in force. See p 3 of December 2017 document.

[87] Investigatory Powers Act 2016 (Commencement No. 1 and Transitional Provisions) Regulations 2016, SI 2016/No 1233.

[88] See https://www.twobirds.com/en/news/articles/2016/uk/what-the-investigatory-powers-bill-would-mean-for-your-business.

A. Purposes for the Retention of Communications Data

Section 87 of IPA provides that the Secretary of State has the power to give retention notice to telecommunications operators[89] to retain relevant communications data. In particular, CSPs may be required to retain relevant communications data for the same purposes for which these data may be obtained, which are specified in section 61(7) IPA:[90]

a) In the interests of national security.
b) For the purpose of preventing or detecting crime or of preventing disorder.
c) In the interests of the economic well-being of the United Kingdom.
d) In the interests of public safety.
e) For the purpose of protecting public health.
f) For the purpose of assessing or collecting any tax, duty or levy.
g) For the purpose, in an emergency, of preventing death or of preventing or mitigating injury or damage to a person's physical or mental health.
h) To assist investigations into alleged miscarriages of justice.
i) Where a person ('P') has died or is unable to identify themselves because of a physical or mental condition, to assist in identifying P, or to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.
j) For the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

The above list of purposes is not a novelty of the IPA. It is based on RIPA, s 22(2) , which contained the first seven grounds, and was extended in the IPA with the addition of grounds (h), (i) and (j). The IPA tries to justify the inclusion of the interests of the economic well- being of the United Kingdom by explaining that such interests should also be relevant to the interests of national security.[91]

Fairly obviously, these purposes seem to go way beyond the notion of serious crime as a hard threshold for retention requirements which was specified as far back as the DRD itself and reviewed approvingly in *Digital Rights Ireland* and *Tele2/Watson*. In the Home Office's consultation on needed amendments to the IPA after *Tele2/Watson* of November 2017

[89] The provisions on the retention of communications data apply also to postal operators and postal services: IPA, s 96 2016.
[90] IPA, s 87(1)(a).
[91] IPA, s 61(7)(c).

(discussed in more depth below at section V. D.), this was somewhat grudgingly acknowledged and a new required definition of 'serious crime' proposed.

> In its present form, the IPA permits the retention of and access to data for 10 purposes. The Government considers that communication data should not be retained or acquired for trivial matters, and the important tests of necessity and proportionality in the Act prevent data being retained or acquired where it is not appropriate to do so. Nevertheless, the Government proposes to amend the Act to impose a serious crime threshold in relation to the retention and acquisition of events data for criminal purposes.[92]

B. Scope of Retention Requirements: Relevant Communications Data and Telecommunications Operators

The IPA, in section 261(5), provides that:

> 'Communications data', in relation to a telecommunications operator, telecommunications service or telecommunication system, means **entity data** or **events data** —
>
> a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—
>
> (i) is about an **entity** to which a **telecommunications service** is provided and relates to the provision of the service,
> (ii) is comprised in, included as part of, attached to or logically associated with a **communication** (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or
> (iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,
>
> b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or
> c) which—
>
> (i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,
> (ii) is about the architecture of a telecommunication system, and
> (iii) is not about a specific person,
>
> but **does not include any content of a communication** or anything which, in the absence of subsection (6)(b), would be content of a communication".[93]

[92] See Home Office *Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data* November 2017, available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf at para 102, p 15 (consultation closed on 18 January 2018).

[93] IPA, s 261(5) (emphasis added).

Effectively, according to the Home Office, 'entity data' corresponds roughly to what was subscriber data in RIPA and 'events data' to what RIPA described as traffic or location data.[94]

Section 87(11) of the IPA provides that only 'relevant communications data' can be required to be retained. This is defined as

> communications data which may be used to identify, or assist in identifying, any of the following
>
> (a) the sender or recipient of a communication (whether or not a person),
> (b) the time or duration of a communication,
> (c) the type, method or pattern, or fact, of communication,
> (d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or
> (e) the location of any such system, and this expression therefore includes, in particular, **internet connection records**.[95]

Internet connection records are a controversial novelty of the IPA. The explanatory notes define them as a 'record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet'.[96] According to many press reports, this meant that 'as the Investigatory Powers Bill passes into law, internet providers will be required to keep a full record of every site that each of its customers have visited'.[97] This looks somewhat like content as opposed to the metadata that the retention regime is designed for and some non-governmental organisations such as Liberty and Big Brother Watch have thoroughly protested this. On the other hand the Government assert that:

> An ICR is not a person's full internet browsing history. It is a record of the services that they have connected to, which can provide vital investigative leads. It would not reveal every web page that they visit or anything that they do on a web page.[98]

Like many other aspects of the IPA, this is likely to end up in court. The actual utility of ICRs is also contested: a similar scheme ran the Danish Internet Session Logging legislation but was reportedly scrapped for lack of effectiveness, although the UK Government purports that

[94] See Home Office *Investigatory Powers Act 2016* (n 91) at p 11.

[95] IPA, s 87(11) (emphasis added).
[96] Explanatory Notes to IPA, para 265.
[97] *The Independent* (24 November 2016).
[98] See factsheet at www.gov.uk/government/uploads/system/uploads/attachment_data/file/530556/Internet_Connection_Records_factsheet.pdf.

they studied the Danish model to learn lessons from it and increase the effectiveness of internet connection records.[99]

C. Retention Notices

IPA section 87(1) provides that the Secretary of State is empowered, subject to Judicial Commissioner approval, to give a retention notice to a telecommunications operator to retain relevant communications data. The Secretary of State can only issue such a notice if it is necessary and proportionate to the purposes for which communications data may be obtained, in accordance with IPA section 61(7), as discussed above.

Who can be obliged to retain data? This is significantly wider than it was in RIPA. Most of the Act's powers apply to 'telecommunications operators'. Telecommunications operators are defined as persons who offer or provide a telecommunications service to persons in the UK or control or provide a telecommunication system which is (wholly or partly) in the UK, or controlled from the UK.[100] This broad definition includes not just traditional telcos or network providers, but any provider of a service that facilitates the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system. This definition is intentionally broad, as can be seen from the draft Codes of Practice, which claimed that Internet-based services such as web-based email, messaging applications and cloud-based services were covered. Social media companies, such as Facebook or Twitter, will also intentionally be in scope.[101] One of the Government's repeated justifications for the reshuffle of the IPA was that criminals and terrorists were increasingly using facilities such as WhatsApp or Facebook Messenger to send private messages, often encrypted, rather than traditional CSPs, and thus putting themselves beyond the interception, access and retention powers of RIPA and the DRRs.

Section 87(8) of the IPA lists obligatory elements of retention notices, which are identical with those formerly contained in DRIPA. For instance, the notice must specify the

---

[99] See 'Comparison of Internet Connection Records in the Investigatory Powers Bill with Danish Internet Session Logging Legislation at www.gov.uk/government/uploads/system/uploads/attachment_data/file/504189/Comparison_of_ICRs_with_Danish_Session_Logging.pdf.

[100] IPA, s 261(1).

[101] See, eg, Interception Code of Practice at 2.6.: 'The Act makes clear that any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system is included within the meaning of "telecommunications service". Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.'

operator to whom it relates; the data which is to be retained; the period for which the data is to be retained; other requirements, or any restrictions, in relation to the retention of the data. The maximum retention period, specified in the retention notice, must not exceed 12 months.[102]

Section 88 of the IPA enumerates the matters which need to be taken into account by the Secretary of State prior to issuing a retention notice to a CSP. These include among others: the likely benefits of such a notice; the likely number of users of the telecommunications service concerned; the technical feasibility of complying with the notice; the likely costs of compliance; and any other impact that the notice may have on the CSP.[103] The Secretary of State is also obliged to take reasonable steps to consult a telecommunications operator before giving it a notice.[104]

D. Safeguards under IPA

Unlike the previous data retention regime under DRIPA and clearly with the attention of averting further challenge under *Digital Rights Ireland* and *Tele2/Watson*, Part 4 of the IPA contains an extensive list of safeguards which are here correlated to the mandatory safeguards enumerated after *Tele2/Watson*.

i. Prior Independent Review

Arguably the most crucial change in the IPA is that a retention notice must not only be approved by the executive but also by a Judicial Commissioner (JC),[105] who must review the Secretary of State's conclusions about the necessity and proportionality of the notice.[106] This 'double lock' approach is an explicit attempt to meet the 'prior independent review' requirements of *Digital Rights Ireland* and *Tele2/Watson* without passing the matter entirely to the capricious hands of ordinary judges, who might cause undue delay where national security was at stake.

What is the role of the JCs? They must 'apply the same principles as would be applied by a court on an application for judicial review' but also 'consider the matters ... with a

[102] IPA, s 87(3).
[103] IPA, s 88(1).
[104] IPA, s 88(2).
[105] IPA, s 87(2).
[106] IPA, s 89(1). See further discussion of the novel introduction of the Judicial Commissioners and their value or otherwise as independent reviewers, at Chapter 6, section V..

sufficient degree of care' so as to safeguard the rights of privacy of targets.[107] There was some doubt as to exactly what this meant. However recently issued guidance on the role and powers of JCs[108] makes it clear that the JCs will adopt the standard a court would if the decision came to them as a fresh case, *not*, as is the norm in administrative judicial review, only deny the request if they feel that no reasonable Secretary of State would have made it (known in English law as *Wednesbury*[109] unreasonableness); this would be clearly too limited a role to meet the requirements of *Tele2* in policing the discretion of the executive.

However if a JC issues a negative decision, the Secretary of State may ask the Investigatory Powers Commissioner (IPC) to decide whether to approve the decision.[110] In addition, any telecommunications operator who receives a notice may refer the retention notice (in its entirety or with regard to any aspect of it) back to the Secretary of State for a review.[111] Furthermore, although the Secretary of State is required under section 90(6) of IPA to consult both the Technical Advisory Board and a Judicial Commissioner in this kind of case, it is still the Secretary of State's own decision whether to withdraw, vary or confirm the effect of the notice. In these cases, approval of the IPC is also mandatory.[112]

These review provisions may potentially be seen as eating into the independent power of the JC and reducing their role below the standard required by the CJEU.[113]

ii. Provide for a High Level of Protection of the Retained Data

In more attempts to meet the standards of *Digital Rights Ireland* and *Tele2/Watson,* the IPA contains rules on data integrity and security, including obligations for the destruction of

---

[107] IPA, s 89(2).

[108] See IPCO *Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioner* 8 March 2018, available at www.ipco.org.uk/docs/20180308%20IPCO%20Advisory%20Notice%2012018%20v1.1.pdf.

[109] See *Associated Provincial Picture Houses Ltd v Wednesbury Corporation* (1948) 1 KB 223 and *ibid* at para 19. 'The purpose of the so-called "double lock" provisions of the Act are to provide an independent, judicial, safeguard as to the legality of warrants, in particular to their necessity and proportionality. In cases engaging fundamental rights, the Judicial Commissioners will not therefore approach their task by asking whether a Secretary of State's decision that a warrant is necessary and proportionate is *Wednesbury* reasonable, as this would not provide the requisite independent safeguard.'

[110] IPA, s 89(4).

[111] IPA, s 90(1)(2).

[112] IPA, s 91(1). The IPC needs to take the same matters into account as the JC, when approving the initial retention notice under s 89(2).

[113] See a more detailed discussion of the independence of the IPC and Judicial Commissioners, and the worth of *double-lock* in Chapter 6 at section V. C. iv.

data,[114] as well as an obligation to protect retained data against any unlawful disclosure.[115] Notably, however, it does not require that retained data be stored in the EU. In its November 2017 Consultation, the Home Office refused to give way entirely on this point on the ground that data retention requests might be made to overseas telecommunications operators, causing various problems if data had to be transported to the UK, but conceded that:

> we have nevertheless included additional proposed requirements in the code of practice which will ensure that where data is held outside the EU, it is retained to an adequate level of protection, comparable to that required by EU data protection laws.[116]

This leaves a number of crucial areas where the safeguards mandated by *Tele2/Watson* are still not apparently met by the IPA. As noted above, the Home Office produced a Consultation document in November 2017, which closed in January 2018, incorporating concrete suggestions for amendments to the IPA by statutory instrument.

iii. Notification after the Fact of the Affected Individuals

A key unresolved issue is the requirement in *Tele2/Watson* for notification of the affected individuals as soon as 'that notification is no longer liable to jeopardise the investigations being undertaken by those authorities'.[117] This matter was discussed by the UK Investigatory Powers Tribunal (IPT)[118] in the context of *Privacy International v Secretary of State for Foreign and Commonwealth Affairs.*[119] In its September 2017 judgment[120] the UK IPT acknowledged the notification requirement established in *Tele2/Watson*, finding it however to 'be very damaging to national security'.[121] The notification requirements would be especially difficult to enforce in relation to bulk data collection and retention requirements.[122] The Home Office's response on this matter in their November 2017 Consultation remained fairly obdurate: 'a general requirement to notify an individual that their data has been accessed

---

[114] IPA, s 92.

[115] IPA, s 93.

[116] See Home Office *Investigatory Powers Act 2016* (n 91) p 18.

[117] *Tele2/Watson* (n 2) [121].

[118] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016–2017] UKIPTrib IPT_15_110_CH.

[119] A request for a preliminary ruling in this case was sent by the IPT to the CJEU, but the main point referred relates to whether national security is excluded from CJEU competence. Order for reference to the Court of Justice of the European Union issued in case [2017] UKIPTrib IPT_15_110_CH www.ipt-uk.com/docs/IPT%20BULK%20DATA%20ORDER%20FOR%20REFERENCE%20TO%20CJEU.pdf.

[120] Judgment of 8 September 2017 [2017] UKIPTrib IPT_15_110_CH.

[121] Ibid [63].

[122] Ibid [64]. See discussion of these bulk powers in Chapter 6 at xxx.

would unnecessarily inform criminals, suspected criminals and others of the investigative techniques that public authorities use'. A safeguard for the fear that powers had been misused already existed in the shape of an application to the UK IPT. Simply because an investigation had ceased or an individual was ruled out of a particular investigation did not mean that notification would not be operationally damaging. Interestingly, the response did not explicitly refer to *bulk* powers as presenting any especial challenges.

E. Reimbursement of Costs of Telecommunications Operators

One of the many controversial aspects of the DRR 2014, made under DRIPA, was that it allowed, but did not require, the Home Secretary to reimburse any expenses incurred by public telecommunications operators in complying with retention notices.[123] Telcos and ISPs have with some reason long felt aggrieved about being asked to shoulder even part of the cost of defending national security which is not exactly part of their core business model.[124] The IPA stipulates that '[t]he Secretary of State *must ensure* that arrangements are in force for securing that telecommunications operators (…) receive an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate'.[125]

In contrast to the former regime, furthermore, such reimbursement is no longer conditional on the expenses having been notified to the Secretary of State and agreed in advance.[126] Instead, a retention notice given to a telecommunications operator must already specify the level of contribution the Secretary of State has determined in respect of the costs incurred, or likely to be incurred.[127] The Secretary of State may also require providers to comply with any audit that may be reasonably required to monitor the claim for reimbursement.[128]

F. Extra territorial Application

---

[123] DRR 2014 reg 13 with reference to s 1(1) to (6) DRIPA.

[124] Similar complaints surfaced, with possibly less inherent justice, during the 'graduated response' phases of the copyright wars when service providers were also asked to take part of the financial burden of defending the interests of copyright holders. See Chapter 9.

[125] IPA, s 249(1) (emphasis added).

[126] DRR 2014, reg 13(2)(a).

[127] IPA, s 249(7).

[128] IPA, s 249(4). (The same as it was according to DRR 2014, reg 13(2)(b) .)

Extra territorial jurisdiction is an extremely sensitive area in the IPA, not only in relation to interception but also access and retention. Similar to DRIPA, the IPA makes provision that most of the retention notice regime in Part 4 'may relate to conduct outside the United Kingdom and persons outside the United Kingdom'.[129] Similarly, the IPA provides for the extra territorial application of Part 3 of IPA relating to authorisations for obtaining communications data.[130]

VI. Conclusions

The UK has traditionally been a strong proponent of telecommunications data retention, being one of the initiators on the European initiatives for the adoption of a European data retention legal instrument and by reintroducing data retention legislation at national level, despite the scrutiny of the CJEU. This chapter aimed at sketching the complicated landscape on the European and UK data retention legislation and raising questions on the compliance of the European and in particular the UK rules on data retention with fundamental rights and the safeguards introduced by the CJEU in a number of courtcases, which is expected to become longer and longer.

Following the recent UK IPT's request for a preliminary ruling, the CJEU will have the opportunity to discuss the application in a national security context of the requirements it developed in *Tele2/Watson* and the safeguards established by the ECtHR, and to reflect on the upcoming judgment of the ECtHR on the secret surveillance activities of the UK intelligence agencies. The CJEU is explicitly requested to answer the question

> how and to what extent do those requirements apply, taking into account the essential necessity of the SIAs [Security and Intelligence Agencies] to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements.[131]

[129] IPA 2016, s 97(1).

[130] IPA 2016, s 85. See for a lengthier discussion of the difficulties with RIPA, s 8(4)'s use of foreign intelligence data, and its current challenge in the Strasbourg court, see Chapter 6.

[131] Order for reference to the CJEU issued in case [2017] UKIPTrib IPT_15_110_CH, 22.

In essence, this request for a preliminary ruling requires the CJEU to clearly take a position towards the stance of the ECtHR in surveillance cases. Will the two courts align their positions in the UK bulk surveillance cases or will they each establish their own system of requirements? The cross-references between the case law of the two courts in the last cases relating to secret surveillance allow me to hope that the two courts will join forces and deliver coherent judgments that will establish a robust system of checks and balances in cases of secret surveillance.

It should be borne in mind that Article 52(3) CFR requires that

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.[132]

This provision facilitates the CJEU to interpret the relevant European legislation in line with the case law of the ECtHR and could be the basis for judicial cross-fertilisation.[133]

In the recent consultation, the UK Government clarified that the consultation leaves out all issues related to national security, as they fall outside the scope of EU law. However, the continuous attempts of the UK Government to avoid introduction of strict safeguards in the regulation of powers of Security and Intelligence Agencies in the context of national security are a clear illustration of the unwillingness of the UK Government to follow the CJEU requirements. However, this situation may radically change depending on the impact of Brexit on the issue, as the CJEU may not be competent for UK cases anymore.

[132] EU Charter of Fundamental Rights, Art 52(3).

[133] 'These provisions may constitute a sound basis to interpret EU law in accordance with the model of protection underlying the ECHR': Oreste Pollicino and Marco Bassini, 'Bridge is Down, Data Truck Cannot Get Through…A Critical View of the *Schrems* Judgment in the Context of European Constitutionalism' in Giuliana Ziccardi Capaldo (ed), *The Global Community - Yearbook of International Law and Jurisprudence* (Oxford, Oxford University Press, 2016) 260.