Striking a Balance among Security, Privacy and Competition. The Data Retention and Investigatory Powers Act 2014 (DRIP)

di **Guido Noto La Diega**

Abstract: Following the ECJ decision that declared the Data Retention Directive invalid, the Data Retention and Investigatory Powers Act 2014 (DRIP) has been enacted. It is not undisputable whether the DRIP gives more powers to the intelligence services at the detriment of both citizens' privacy and freedom of enterprise or whether it simply clarifies the nature and extent of obligations that can be imposed on telecommunications service providers based outside the UK under Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA).

Il presente articolo si prefigge l'obiettivo di analizzare l'effettiva portata del Data Retention and Investigatory Powers Act 2014, che è stato accusato di fornire nuovi poteri ai servizi segreti per controllare specialmente le società straniere (ponendo, quindi, problemi di bilanciamento fra sicurezza, diritto alla riservatezza e libertà d'impresa), mentre nelle intenzioni dichiarate dal Governo si tratterebbe semplicemente di chiarire poteri preesistenti.

1. Introduction.

In an unprecedented hurry [1], in July 2014 the Data Retention and Investigatory Powers Act 2014 (DRIP or DRIPA) [2] has been enacted. The *occasio* [3]of the act is the European Court of Justice Judgment of 8 April 2014 in joined cases C-293/12 *Digital Rights Ireland* and C-594/12 *Seitlinger*, which declared the Data Retention Directive (2006/24/EC) [4] invalid [5]. Consequently, the DRIP provides the powers to introduce secondary legislation to replace the Data Retention Regulations 2009 (S.I. 2009/859) [6] that implemented the directive in domestic law [7].

2. The DRIP and the nature and extent of obligations that can be imposed on telecommunications service providers based outside the UK.

Anyway, what is more important from a comparative private law perspective is that the examined legislation clarifies the nature and extent of obligations that can be imposed on telecommunications service providers [8] based outside the UK under Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA) [9]. This Act ensures that any company providing communication services to customers in the UK is obliged to comply with requests for communications data [10] and interception warrants issued by the Secretary of State, irrespective of the location o the company providing the service.

2.1. The DRIP has many methodological flaws and more nuanced substantial characteristics.

For what it concerns the first ones, the process that led to the production of this legislation has been described as "a blot on our claim to be a democratic society" [11]. As is common knowledge, the UK Government could have waited the European Institutions to harmonise the law after the *Digital Rights Ireland – Seitlinger* ruling, but the situation has been considered an emergency.

First, if it were a proper emergency, waiting from April to July would have been very irresponsible. The truth is that the investigations have gone on as always and there has not been any immediate effect of the European ruling at

hand [12].

Second, there has been no consultation. Better, allegedly the Government took into consideration the communications industry, law enforcement and intelligence agencies as those affected by DRIP provisions". Nevertheless, the point is that it is not negligible that the citizens are, if not the first, for sure among the primary subjects of the mentioned legislation [13].

More in general, the behaviour of the Government appears to run with the hare and hunt with the hounds. It is an emergency so it is not important to wait for an act of the European Institutions (even though it could happen that the DRIP conflicts with the forthcoming EU legislation), but at the same time the Government adds a sunset clause, which has the effect of keeping this law in place for twenty-nine months. It is reasonable to ask oneself how can "a review in 30 months be adequate (30 weeks would be a long time), especially when it is clear that Parliament has little business to deal with between now and the election?" [14].

2.2. Some substantial remarks.

Let's move to the content. In the *Digital Rights Ireland – Seitlinger* judgement, the ECJ declares the Directive 2006/24 invalid because it required the telecommunications service providers to retain for up to two years all meta-data about emails, text messages and telephone calls of every EU citizen and to make these available to national security agencies. This was found in contrast with the rights to privacy and data protection consecrated in the Charter of Fundamental Right of the European Union.

Despite the hurry, the solution taken by the Government appears to be quite well balanced. On the one hand, in fact, the DRIP allows the security services to require a public telecommunications operator to retain communications data in line with the purposes of the RIPA. On the other hand, it limits the length of time such data can be retained to a maximum of twelve months [15], reduces the number of public bodies that can access the data collected, creates a privacy and civil liberties board to oversee the enforcement of the DRIP, provides the annual publication of a report on the amount of data intercepted and other less relevant provisions [16].

It is clear, nevertheless, that the statement that the Bill does not contain new powers is false. On this point, I espouse the ***Open letter on data retention and investigatory powers Bill ("DRIP") from UK privacy law academics*** *of 10*th July 2014 [17].

The Government is indeed authorised to compel any person or company outside the UK: i. To execute an interception warrant (also relating to conduct outside the UK) (4(2)); ii. To do anything, including complying with technical requirements, to ensure the ability, on a continuing basis, to assist the UK with interception at any time (4(6)); iii. To obtain, retain and disclose communications data also relating to conduct outside the UK (4(8)). Something is new under the sun: no extraterritorial effect was provided by the RIPA [18], now extraterritoriality is not negligible anymore.

Furthermore, it is true that the Secretary of State can only require retention of the same types of communications data that he could under the 2009 Regulations, but he may however "also make regulations which relate to the wider category of communications data retained by service providers under the voluntary code of practice under ACTSA, s 102" [19].

It is, eventually, been noted that the DRIP "does not meet the terms of the CJEU decision and breaches the Human Rights Act 2000 and the Charter Rights" [20].

3. The secondary legislation: The Data Retention Regulations 2014.

On 1st August 2014, the Data Retention Regulations 2014 came into force [21], completing the framework introduced by the DRIP. They provide that a communications service provider can be required to retain data only when target of a notice of the Secretary of State.

4. The aftermath: R (David Davis MP and Tom Watson MP) v Secretary of State for the Home Department and the proposed Counter-Terrorism and Security Bill.

There has already been an important occasion when the High Court judged on the DRIP. In a nutshell, the case had been brought by two Members of Parliament, with the intervention of the human rights activists of Open Rights Group (ORG) and Privacy International (PI) [22] seeked an order disapplying section 1 of the DRIP for breach of the Directive on privacy and electronic communications 2002/58/EC ("PECD").

In December 2014, in *R (on the application of David Davis MP and Tom Watson MP) v Secretary of State for the Home Department* [23], Mr Justice Lewis granted the Claimants permission to proceed to a substantive hearing, thus agreeing that the DRIP can be challenged by judicial review.

As a reaction [24], the Government is proposing to use the Counter-Terrorism and Security Bill (CTSB) [25] to extend their remit to cover data generated as a result of internet communications. In fact, part 3 of the CTSB deals with the data retention: what is more important is not that clause 17 amends the DRIP, but the point is that security and the battle to terrorism are once again used to restrict people's privacy. This is meaningful not only from an axiological point of view, but also from a programmatic one, as art. 1 PECD provides for an individual right to confidentiality, erasure and anonymity of one's 'communications' or 'traffic data,' specifying the obligations of the Member States in the following articles, which can be derogated from Article 15 PECD, by which Member States can exceptionally restrict the mentioned rights when "necessary, appropriate and proportionate [...] to safeguard national security (i.e State security), defence, public security, and the prevention, investigation, detention and prosecution of criminal offences or of unauthorised use of the electronic communications system".

5. Conclusion.

It appears clear the difference between the UK approach and the EU one. It is sufficient to read the Article 29 Working Party Data Protection Group Opinion 5/2002 [26] where it is provided that retention of traffic data for purposes of law enforcement should meet strict conditions under Article 15 (1) of the Directive: i.e. in each case only for a limited period and where necessary, appropriate and proportionate in a democratic society. Where traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse. In conclusion, "systematic retention of all kinds of traffic data *for a period of one year* or more would be clearly disproportionate and therefore *unacceptable in any case*" [27].

As a matter of fact, in conclusion, the DRIP introduces "powers that are not only completely novel in the United Kingdom, they are some of the first of their kind globally" and applies it to a very wide target, so the above-mentioned counterweights risk to be a red herring. Eventually, with the purpose (or with the excuse, some might dare to say) of protecting privacy (which is in fact violated by the Secretary of State allegedly for security reasons), the freedom of enterprise is left to bite the dust [28].

Note:

[1] Introduced on 14th July, it has received the royal assent three days later with little parliamentary debate.

[2] Here the official full name: "An Act to make provision, in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, about the retention of certain communications data; to amend the grounds for issuing interception warrants, or granting or giving certain authorisations or notices, under Part 1 of the Regulation of Investigatory Powers Act 2000; to make provision about the extra-territorial application of that Part and about the meaning of "telecommunications service" for the purposes of that Act; to make provision about additional reports by the Interception of Communications Commissioner; to make provision about a review of the operation and regulation of investigatory powers; and for connected purposes". The DRIP is available at http://www.legislation.gov.uk/en/ukpga/2014/27/enacted?view=plain (accessed 9th January 2015).

[3] See the Impact Assessment of the Home Office of 27th June 2014 at http://www.legislation.gov.uk/ukia/2014/266/pdfs/ukia_20140266_en.pdf (accessed 9th January 2015). From a comparative perspective, it has been noted that in Switzerland, even though there is a 6-months-retention regime, the Swiss Federal Council stated that the European Court ruling had no effect on Swiss laws (see

Emergency data retention law to be challenged, in *P. & D.P.* 2014, 14(8), 1,17 and, on the wider implications of the European Court's ruling see the article published in Volume 14, Issue 7 of *Privacy & Data Protection*).

[4] The Data Retention Directive (DRD), whose *occasion* are the terrorist attacks in Madrid in 2004 and London in 2005 (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm), can be read at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (both accessed 9th January 2014). On the DRD see, for example, I. Brown, *Communications Data Retention in an Evolving Internet*, in *International Journal of Law and Information* Technology, 2011, II, 95; T. Konstadinides, *Destroying Democracy on the Ground of Defending It? The Data Retention directive, the Surveillance State and Our Constitutional Ecosystem*, in *European Law* Review, 2011, V, 722 and A.R. Servent, *Holding the European Parliament responsible: policy shift in the Data Retention directive from consultation to codecision*, in *Journal of European Public Policy,* 2013, VII, 972.

[5] Judgment of the Court (Grand Chamber) of 8 April 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria)) — *Digital Rights Ireland Ltd* (C-293/12) *v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* (C-594/12), not yet published, but readable at http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN (accessed 9th January 2015). The ECJ ruled that "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 is invalid". On the judgement see F. Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, Tilburg Law School Research Paper No. 15/2014, forthcoming in 28 *Harvard Human Rights Journal* (2015), available at ssrn.com/abstract=2482212 (accessed 9th January 2015).

[6] The Data Retention Regulations 2009 are available at http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksi_20090859_en.pdf (accessed 9th January 2015).

[7] See the Data Retention Regulations 2014 of 30 July 2014 (http://www.legislation.gov.uk/uksi/2014/2042/pdfs/uksi_20142042_en.pdf, accessed 17th January 2015), that sets out what information must be included in retention notices served to telecoms and Internet companies.

[8] On this point, the DRIP amends the RIPA definition of telecommunications service to provider allegedly to include the webmail, but potentially referring today also to cloud providers and social media ones.

[9] The RIPA, enacted in July 2000 and last modified in February 2010, moving from the necessity to address the technological evolution, deals with the public surveillance and the interception of communications. The official full name is "An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes". It can be read at http://www.legislation.gov.uk/ukpga/2000/23/contents (accessed 9th January 2015). On the RIPA see, for example, J. Hörnle, *How to control interception-does the UK strike the right balance?*, in *Computer Law and Security Report*, 2010VI, 649; H. Fenwick, *Covert surveillance under the Regulation of Investigatory Powers act 2000*, in *Journal of Criminal Law*, 2001, VI, 521; Anonymous, *First RIPA convictions over disclosure of encryption keys*, in *Computer Fraud and Security*, 2009, IX, 3; A.S. Reid-N. Ryder, *For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers act 2000*, in *Information and Communications Technology Law*, 2001, II, 179. To understand the relation between the DRIP and the RIPA one can read also in R. Jay, *The Data Retention and Investigatory Powers Act 2014 – Recent Developments*, in *Computers & Law,* 15-1-2015, where it is said that "RIPA is the legislation that governs *access* to retained communications data as well as

powers to intercept the content of communications. DRIPA amends definitions in RIPA and covers the extent of the powers of the UK to serve notices on telecommunications service providers that are based outside the UK, but provide services within the UK".

[10] Data", in the sense of the Data Retention Directive, are "traffic data and location data and the related data necessary to identify the subscriber or user" (art. 2.2, a)). Now, the RIPA definition appears to be way wider, as it encompasses any information held or obtained about those whom services are provided to. According to sec. 1 suppl., (1) of the DRIP, "communications data" has the "meaning given by section 21(4) of the Regulation of Investigatory Powers Act 2000 so far as that meaning applies in relation to telecommunications services and telecommunication systems". The clause 17 of the proposed Counter-Terrorism and Security Bill would extend the concept to data which relate to an internet access service or an internet communications service.

[11] L. Eastham, *Editorial*, in *Computers & Law*, 2014, III, 2.

[12] It sounds quite unreal what stated in the above cited Impact Assessment: "without this Bill, *vital* evidence from telephones and the internet (sic!) that is needed by the police on a day to day basis might be lost. More crimes, including the most serious such as *child sexual exploitation*, may go *unpunished*" (italics mine).

[13] This behaviour appears even stranger if one reads the *Impact Assessment*, that names the "groups affected", the last of them being "the general public, whose safety and security are affected by the capabilities of the police and other agencies to prevent and detect crime, and whose privacy needs to be protected". One may read a certain degree of paternalism in these lines, where the citizens are treated as objects rather than as subjects of rights.

[14] Ibidem

[15] Previously, the fifth of the Data Retention Regulations 2009 provided that "The data specified in the Schedule to these Regulations must be retained by the public communications provider for a period of 12 months from the date of the communication in question". From a comparative perspective, it can be useful to note that art. 132 of the Italian code of privacy (d.lgs. n. 196/2003), as modified by the d.lgs. n. 109/2008 (which enacted the Data Retention Directive in Italy), provides that "i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione di reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione" (24 months for the telephone communications, 12 months for the Internet ones, but see art. 123, paragraph 2 of the italian code of privacy, in so far as it concerns the data on billing, that can be retained for 6 months or more if necessary in case of a trial).

[16] For example, see the biennial review of the relevance of the RIPA, the accessibility to only data that is relevan and the maintenance that such data can no longer be gathered solely for the interest of the economic well-being o the UK.

[17] The signatories of the letter are Dr Subhajit Basu (University of Leeds), Dr Paul Bernal (University of East Anglia), Professor Ian Brown (Oxford University), Ray Corrigan (The Open University), Professor Lilian Edwards (University of Strathclyde), Dr Theodore Konstadinides (University of Surrey), Professor Chris Marsden (University of Sussex), Dr Karen Mc Cullagh (University of East Anglia), Dr. Daithí Mac Síthigh (Newcastle University), Professor David Mead (University of East Anglia), Professor Andrew Murray (London School of Economics), Professor Steve Peers (University of Essex), Julia Powles (University of Cambridge), Professor Burkhard Schafer (University of Edinburgh), Professor Lorna Woods (University of Essex). Please find the letter here http://www.law.ed.ac.uk/__data/assets/pdf_file/0003/158070/Open_letter_UK_internet_law_academics.pdf (accessed 9th January 2015).

[18] In the Explanatory Notes it is asserted that the RIPA had implicit extraterritorial effect.

[19] Jay, *The Data Retention and Investigatory Powers Act 2014*, cit.

[20] Ibidem

[21] See., more specifically, reg. 1., sec. 2 and 3.

[22] The human rights organizations have been given permission to make a further written intervention.

[23] See https://www.openrightsgroup.org/ourwork/reports/open-rights-group-and-privacy-internationals-submission-in-dripa-case (accessed 17 January 2015).

[24] This is the interpretation provided by Jay, *The Data Retention and Investigatory Powers Act 2014* cit.

[25] The "Bill to make provision in relation to terrorism; to make provision about retention of communications data, about information, authority to carry and security in relation to air, sea and rail transport and about reviews by the Special Immigration Appeals Commission against refusals to issue certificates of naturalisation; and for connected purposes" can be found at http://www.publications.parliament.uk/pa/bills/lbill/2014-2015/0075/15075.pdf (accessed 20th January 2015). On 13 January 2015 there has been the second reading at the House of Lords (the general debate on all aspects of the Bill), the Committee stage (line by line examination of the Bill) has begun on 20 January.

[26] Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, 11 October 2002, WP 64. It can be read at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp64_en.pdf (accessed 20 January 2015).

[27] See, more recently, the Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) (2011/C 279/01) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1421770645538&uri=CELEX:52011XX0923(01)) and the Article 29 Working Group Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, 13 July 2010, WP 172. It is available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf (both accessed 20 January 2015).

[28] On privacy and competition, s. C. Kuner-F.H. Cate-C. Millard-D.J.B. Svantesson-O. Lynksey, *When Two Worlds Collide: The Interface between Competition Law and Data Protection*, in *International Data Privacy Law*, 2014, IV, 247.

LEGGI

On porn censorship and liberal ethics in the UK. Brief notes on the Audiovisual Media Services Regulations 2014

21 gennaio 2015