A COMPARATIVE ANALYSIS OF THE JURISPRUDENCE OF THE EUROPEAN COURT OF JUSTICE AND THE ROMANIAN CONSTITUTIONAL COURT ON METADATA RETENTION

Valentin STOIAN[*]

Abstract:

The aim of the paper is to compare and contrast the jurisprudence of the European Court of Justice and the Romanian Constitutional Court on the topic of metadata retention. The paper will argue that both Courts, when considering the effect on the right to privacy, essentially see metadata retention and use as on a par with the interception of the content of communication.

Firstly, the paper will commence with a summary of the directive and will discuss its main provisions. Further, the centerpiece of the paper will be the comparison of the Digital Rights Ireland decision and the RCC decisions. The common arguments of the two courts will be drawn out and systematized in a table. This will be presented according to the character of the action of metadata retention and to the type of infringement detected by the Court (essential rights violation or disproportionality).

Keywords: *jurisprudence, European Court of Justice, Romanian Constitutional Court, metadata retention*

Introduction

April 2014 represented a major blow for those advocating the regulation of metadata retention at the European level. In an unprecedented decision (Digital Rights Ireland v. Minister of Communications, C-293/12 and C-594/12), the European Court of Justice (Luxembourg) declared Directive 2006/24/EC on electronic communication null and void. Rather than merely annulling the directive *ex nunc* (for the future), the Court extended the temporal applicability of its decision also *ex tunc* (for the past) (Rauhofer & Sithigh, 2014). Thus, the 2006 Directive was treated as though it never existed, outstanding infringement procedures against states that had failed to implement it were withdrawn and Sweden was returned a 3 million Euro fine

[*] National Institute for Intelligence Studies, "Mihai Viteazul" National Intelligence Academy.

it had had to pay as a penalty for non-implementation (Luxembourg Weekly, 17.05.2014).

Yet, well before the Luxembourg court had handed down its decision, the topic of metadata retention was controversial in many of the EU's member states. Legal challenges against metadata retention took the form of constitutional court cases against laws transposing the directive in national legislation. Thus, in 2008, the Bulgarian Supreme Administrative Court invalidated the Bulgarian law implementing the directive, in 2010 the German Constitutional Court abrogated the corresponding German law (De Vries et al., 2011) while the same occurred in 2011 in Cyprus and the Czech Republic (Guild & Carrera, 2014; Kosta, 2013, p. 339). Romania proved a particularly interesting case as the Romanian Government attempted to implement the directive not once, but twice and to supplement the legal framework of caller identification yet another time. All three attempts were thwarted by the Romanian Constitutional Court (RCC) in three separate decisions (1258/2009, 440/2014, 461/2014). Thus, the „way to Luxembourg" (Kosta, 2013) was littered with several decisions that judged national laws on metadata retention and use as incompatible with human rights.

The aim of the paper is to compare and contrast the jurisprudence of the European Court of Justice and the Romanian Constitutional Court on the topic of metadata retention. The paper will argue that both Courts, when considering the effect on the right to privacy, essentially see metadata retention and use as on a par with the interception of the content of communication.

Firstly, the paper will commence with a summary of the directive and will discuss its main provisions. Further, the centerpiece of the paper will be the comparison of the *Digital Rights Ireland* decision and the RCC decisions. The common arguments of the two courts will be drawn out and systematized in a table. This will be presented according to the character of the action of metadata retention and to the type of infringement detected by the Court (essential rights violation or disproportionality).

The Directive 2006/24/EC on data retention and the „way to Luxemburg"

Adopted in the wake of the Madrid and London bombings of 2004 and 2005, Directive 2006/24/EC represented, from the time of its adoption to April 2014, the key act at the European level regulating communication metadata retention (Brown, 2010). It created an obligation incumbent on the

member states to create a legislative framework that forced telephone and internet services providers to store, for a period of minimum six months and maximum two years "traffic and location data on both legal and natural persons and the related data necessary to identify the subscriber or registered user" (Directive 2006/24/EC).

The specified obligation extended to a wide array of data such as the telephone number and address of both the one making and the one receiving the call (the obligation also extended to unanswered calls as they might be used for triggering explosive devices by terrorist groups (Guarino, 2014, p. 249-255), the user ID, IP address and name and address of both parties engaged in online communication, time and duration of telephone call and time of log-on and log-off of the Internet access service, data necessary to identify the equipment and location of the communication - International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), digital subscriber line (DSL), cell ID, etc. (Guarino, 2014, p. 249-255). Finally, the Directive required member states to ensure that data are protected from unauthorized use and are available only to authorized government personnel and that they are destroyed at the end of the storage period. Yet, it left the regulation of the access to the data at the discretion of the member states, stating only that "The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR [European Convention on Human Rights] as interpreted by the European Court of Human Rights" (Guarino, 2014).

In its preamble, the Directive set out two major goals for itself: to harmonize national legislation on metadata retention and to provide tools for the "investigation, detection and prosecution of serious crime" (Directive 2006/24/EC). To justify the adoption of this measure, the directive expressly referred to the European Council's statement of 13 July 2005, which condemned terrorist attacks on London and reaffirmed the need to adopt common measures on the retention of telecommunications data as soon as possible. Furthermore, the directive's preamble declared that metadata retention has to take into account the right to privacy as set out by both the European Convention on Human Rights (Article 8) and the (at time of the directive's adoption, not binding) Charter of the Fundamental Rights of the European Union (Articles 7 and 8), but that this right can be limited for reasons such as "national security or public safety, for the prevention of

disorder or crime, or for the protection of the rights and freedoms of others". Thus, the Directive's preamble proclaimed that "Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organized crime and terrorism", its regulation at the European level, while respecting human rights, is a necessary undertaking (Directive 2006/24/EC).

The first challenge to the Directive came from the Government of Ireland and concerned not the substantive provisions of the Directive, but the grounds on which it was adopted. Ireland brought a complaint before the Luxembourg court, expressing the view that the directive should not have been adopted under the first pillar of the EU decision-making procedures[1], but under the third, given that its main aim was combating serious crime and terrorism while "preventing distortions or obstacles to the internal market was only its "incidental" goal (Kosta, 2013). The ECJ rejected this approach, arguing that the directive did not regulate access to the data by national law-enforcement, but only addressed its regulations to private providers of internet and telephony services. This represented, in the view of the Court, evidence enough that the main purpose of the directive was concerned with regulating the internal market (Ireland v. European Parliament and Council of the European Union).

Even before the 2014 ECJ decision, national legislation transposing the directive was struck down by several national Courts. The Bulgarian Supreme Administrative Court focused on the fact that law enforcement agencies could have, within the Bulgarian national legislation, warrantless access to the data from a dedicated computer terminal. This was found by the Bulgarian Court in violation of Article 32(1) of the Bulgarian Constitution and of the Article 8 of the European Convention on Human Rights (Kosta, 2013). In its 2010 decision, the German Constitutional Court did not evaluate the Directive *per se*, but found that the obligation to store data indiscriminately (irrespective of whether the person whose communication data is to be stored is suspected of a crime) and the lack of judicial oversight for the access and use of data is a disproportional violation of Article 10(1) of the German Basic Law protecting the secrecy of correspondence. According to the German Constitutional Court, data retention per se is not unconstitutional, but it infringes the right to

[1] When the directive was adopted and when this initial challenge was brought, the EU was operating under the three-pillar system, distinguishing the European Communities, the Common Foreign and Security Policy and the Justice and Home Affairs cooperation. This was abolished by the Lisbon Treaty.

privacy and should therefore be subject to a "rigorous proportionality check" (Kosta, 2013). A similar approach was taken by the Czech constitutional Court in 2011, which argued that the duties imposed on telecommunications providers are vague, and that the indiscriminate access to data was unacceptable, as this had to be based on "well-founded suspicions" (Kosta, 2013, p. 355). Also in 2011, the Supreme Court of Cyprus dealt with a civil complaint of persons who had their communications data requested by the police. The Court rejected the applications of the police in three out of four cases arguing that the disclosures violated the right to the secrecy of communication (Kosta, 2013, p. 354).

Digital Rights Ireland v. Ministry of Communications and the Romanian Constitutional Court Decisions.

In its April 2014 decision, the Court began from the premise that the retention of a wide range of metadata is bound to engage the right to privacy (Article 7 of the Charter) and the right to the protection of personal data (Article 8 of the Charter). The main reason why these rights are affected is that "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained." (European Court of Justice, 8.04.2014). However, the engagement of those rights is not necessarily a reason for invalidating the Directive, given that Article 52(1) of the Charter allows for limiting rights as long as those limitations are „provided for by law, respect their essence and [are] subject to the principle of proportionality" (European Court of Justice, 8.04.2014). Thus, according to the Court, a proportionality check has to be undertaken, in order to verify the justifiability of the infringement.

Firstly, the Court proclaimed that the essence of the right to privacy is not violated, as the Directive does not allow for the acquisition of the content of communications. Moreover, the Directive serves a legitimate purpose, being aimed at „the investigation, detection and prosecution of serious crime." (European Court of Justice, 8.04.2014) Further, the Court decided that the crucial test the directive has to pass is that of proportionality of the interference with the right to privacy, which means that „acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives" (European Court of Justice,

8.04.2014). Given the seriousness of the interference, the Court proclaimed that the discretion allowed to the EU legislature has to be strictly limited.

In the second part of the judgment, the Court goes on to criticize the directive, grounding its arguments in the need to balance the right to privacy and the legitimate (yet not necessarily decisive) goals of the Directive. The ECJ noted the **generality** of the directive, which stipulates that data generated by all means of electronic communication of all the European population can be retained. Thus, the judgment focuses on the fact that the metadata of communications from persons who are not, even indirectly, in a situation "which is liable to give rise to criminal prosecutions" (European Court of Justice, 8.04.2014) can be retained under the directive and that no limitation of time, geographical area or personal circumstances is included. Further, the decision focuses on the **lack of limits on use of data**: no procedures (such as prior approval of a judicial or independent administrative body) or objective criterion limiting the access to data by national authorities is specified (European Court of Justice, 8.04.2014).

Issues related to **the storage** of the data are addressed by the Court in the following paragraphs. According to the ECJ, **no distinction** is made between useful and useless data is made, when deciding on the period of data retention. Finally, the Court argues that proper safeguards on preventing unauthorized access to the data are not implemented, as providers are allowed to take economic considerations into account when deciding „the level of security which they apply" (European Court of Justice, 8.04.2014) and the irreversible destruction of the data at the end of the period is not stipulated. Especially serious, in the view of the Court, is the fact that the directive does not impose the storage of data within the EU „with the result that it cannot be held that the control [...] by an independent authority of compliance with the requirements of protection and security [...] is fully ensured" (European Court of Justice, 8.04.2014).

The first Romanian law transposing Directive 2006/24/EC into Romanian law came in 2008. Law 298 created an obligation incumbent on providers of telecommunication and internet services to store "traffic and location data for natural and legal persons, as way as connex data, required for identifying the subscriber or the registered user" (Law 298/2008). It enumerated the data stipulated in the directive and chose to impose the obligation of storage for 6 months, the minimum retention period required by the directive. The law also created a distinction between the procedures for accessing the stored data by law enforcement and prosecutors, on the one hand, and that for "state organs entrusted with national security", on the other

(Law 298/2008). While the first had to request, from a competent court, a specific warrant to access the data, the latter were not required to do so.

The first decision rendered by the Romanian Constitutional Court on the matter came in October 2009, when adjudicating the constitutionality of law 298/2008 (Romanian Constitutional Court Decision no. 1258/October 2009). The Court begins its argumentation from a similar position as that of the later ECJ decision: that fundamental rights can be limited, as long as this limitation is necessary for a legitimate purpose such as national security, public order, the prevention and prosecution of crime, and as long as the limitation is proportional, non-discriminatory and does not eliminate the substance of the right (Romanian Constitutional Court Decision no. 1258/October 2009). The Court's first argument concerns the extent of the data to be retained under law 298. It stipulated that „the current law applies to traffic and location data, as well as to connex data, required for identifying the subscriber" (Romanian Constitutional Court Decision no. 1258/October 2009). The RCC found that the formulation „connex data" is too vague and does not specifically identify the data to be retained. This vagueness opens the space to arbitrariness and does not allow the addressees of the law to understand it and to adapt their behavior accordingly.

Moreover, the RCC also criticized the vagueness of the stipulation that "For protecting and combating threats to national security, state institutions in the field, in situations stipulated by the laws on national security, can access the data stored by telecommunications providers" (Romanian Constitutional Court Decision no. 1258/October 2009). As there is no specification of what constitutes threats to national security, the Court affirmed that this article also opens up the space to arbitrariness, as any action might be considered a threat to national security.

Yet, the more serious criticism of the law provided by the RCC is that the **continuous storage** coupled with the **absence of limits on the use of data** (no court warrant being required) represents an infringement of the very essence of the right to privacy. Furthermore, the Court also undertakes a proportionality test, arguing that a measure infringing on a right can be proportional only if its enforcement ceases once the cause that determined it disappears. However, as data concerning every person's communications is stored, this measure is not applied only when the justified need for it appears and does not cease when the same reason disappears. Further, the RCC also argues that the data of a person receiving a call is stored, exposing this person to unjustified intrusion. The RCC concludes that the **general and continuous** character of data storage is an unacceptable violation of the person's right to

privacy (Romanian Constitutional Court Decision no. 1258/October 2009). Yet, the decision leaves unclear whether the unconstitutionality of the law stems from it voiding the substance of the right altogether or due to the disproportional nature of the measures.

Romania again attempted to transpose the Directive in June 2012, through law 82. Law 82 clarified the expression "connex data" criticized by the RCC in the previous decision, by stipulating that the law applies to "traffic and location data of natural and legal persons, as well as to data necessary to identify a subscriber or registered user" (Law 82/2012). Moreover, the law expanded the scope of the application of the law, allowing the use of metadata for criminal investigations carried out in a wider array of crimes than before. Finally, Law 82 kept the distinction between law enforcement and national security agencies, requiring the former to request a warrant while exempting the latter.

This was again challenged before the Romanian Constitutional Court, and its decision came in June 2014, barely two months after the ECJ ruling. Firstly, the Court argued that the ambiguity present in the previous law was not eliminated, as law 82 stipulated that "the current law applies to traffic and location data of natural and legal person, as well as to the data necessary for user identification" (Romanian Constitutional Court Decision 440/2014). The RCC went on to compare the provisions of law 82/2012 to those of law 298/2008 and to argue that most of the reasons which determined the striking down of the latter are also present in the former. Thus, law 82 goes on to stipulate the **continuous character** of data retention as wells as the lack of any **judicial guarantees for their use by state authorities (**Romanian Constitutional Court Decision 440/2014).

Further, the RCC distinguished between retention and use, arguing that the first procedure, per se is not a violation of the right to privacy. Yet, the way that data is accessed is problematic for the Court. Law 82 establishes an obligation for law enforcement to request a warrant by a judicial authority when accessing metadata, **while creating no corresponding obligation** for "state institutions with responsibilities in the field of national security" (intelligence services) (Romanian Constitutional Court Decision 440/2014). Warrantless access to metadata is, therefore, seen by the Court as an unacceptable interference with the right to privacy. Further, the Court argues that the storage of data is not adequately guaranteed, as no real control on providers who store data is established (Romanian Constitutional Court Decision 440/2014).

An attempt was made to supplement the legislative framework on metadata retention, by requiring the identification of buyers of pre-paid telephony services (as opposed to subscriptions) and of those accessing free Wi-Fi internet services. A legislative initiative was put forward, but it was challenged by the Ombudsman before it could be promulgated. According to this law, those selling pre-paid cards or offering free access to the internet would have had to request personal identification data from their customers. The RCC was extremely critical of this approach, arguing that this expands both the number of people whose personal data would be collected (not only subscribers to telephony services but also buyers of pre-paid cards and those accessing the internet from Wi-Fi hotspots) but also the range of those collecting data (for example dealers of pre-paid cards or coffee shops offering free internet). This **extension did not come together with stricter obligations for confidentiality imposed on those collecting personal data**. This was reason enough, in the eyes of the Court to find the law unconstitutional, as it infringes on the very essence of the right to privacy (Romanian Constitutional Court Decision 461/16th September 2014).

A dissenting opinion signed by three Constitutional Court judges argued that the criticized law only concerns the storage and not the use of metadata. While appropriate guarantees for the use of metadata are indeed required, the three judges argued that since storage of metadata is not itself unconstitutional, expanding or reducing the scope of those who collect personal identification of telephone and internet users is not, *per se*, problematic from a constitutional point of view (Romanian Constiutional Court Decision 461/16th September 2014).

One of the main conclusions to be drawn from the analysis is that there is some confusion in the judgment rendered by the Romanian Constitutional Court. It is not particularly clear in the decision whether metadata retention and subsequent warrantless use infringes on the very existence of the right to privacy or on is a disproportional means employed to achieve a legitimate goal. The RCC seems to argue for both, despite these being logically inconsistent. An action destroying the very essence of the right to privacy cannot be at the same time a legitimate, but maybe disproportionate means towards a limited infringement of the right. Unlike the RCC, the ECJ draws this distinction, arguing that metadata retention is disproportionate but does not destroy the essence of the right.

The second conclusion to be drawn is that both courts do not see much difference between the interception of the content of communication and the retention and use of metadata. Both the RCC and the ECJ argue that because

metadata retention and use generates a legitimate fear of permanent surveillance, it should not be applied generally, but rather for specific persons, in specific situations, under judicial authorization.

Character of metadata storage and use **Reasons for invalidation**	Generality (about all persons)/ Indiscriminate	Continuous (long time limits)	Warrantless access by state authorities	No guarantees against unauthorized access
Destroys the essence of the right	RCC 1289/2009	RCC 440/2014 RCC 1289/2009	RCC 1289/2009 RCC 440/2014	RCC 461/2014
Is a disproportionate means for achieving a legitimate goal	*Digital Rights Ireland*	*Digital Rights Ireland*	*Digital Rights Ireland*	*Digital Rights Ireland*

Conclusions

According to the relevant analyses of both Courts, there are several reasons for which the directive and the laws transposing it have been struck down. Firstly, it has to be mentioned that both Courts distinguish between metadata retention and metadata use. While the first is a technical operation, only the second directly affects the right to privacy. Thus, both Courts found that access to metadata is problematic when it is general and continuous over a long period of time. They argued that the use of this type of data should be restricted to persons about whom there is a reasonable suspicion that they are involved in criminal activity. Alternatively, criteria such as limitations of the geographical area over which retention extends or of time periods could be added.

Another crucial reason for rejecting these laws came from the possibility of law enforcement or intelligence services accessing this data without a warrant issued by a judge. Similarly to the interception of the content of communication, the Courts found that metadata retention and use is a significant enough infringement of the right to privacy to require judicial

authorization. Finally, both courts argued, that strict guarantees against unauthorized access should be imposed on those storing the data, including making sure that the storage facilities are located in Europe.

References:

1. Brown, Ian (2010). *Communications Data Retention in an Evolving Internet*, in *International Journal of Law and Information Technology*, Vol. 19, No 2.
2. De Vries, Katja, Bellanova, Rocco, De Hert, Paul and Gutwirth, Serge (2011). *The German Constitutional Court Judgment on data retention: proportionality overrides unlimited surveillance (doesn't it?)*, in Gutwirth, S., Poullet, Y., De Hert, P., Leenes, R. (eds.) *Privacy and data protection: an element of choice*. Springer, 3-24, Available at: http://works.bepress.com/serge_gutwirth/53, Accessed on 15.01.2015.
3. 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, retrieved from http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, Accessed on 7.01.2015.
4. European Court of Justice, Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources, 8.04.2014 retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=125076 Accessed on 15.01.2014.
5. European Court of Justice, *Ireland v. European Parliament and Council of the European Union, retrieved from* http://curia.europa.eu/juris/document/document.jsf?text=&docid=72843&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=190003, Accessed on 15.01.2015.
6. Ganj, Cristian (2009). *The Lives of Other Judges: Effects of the Romanian Data Retention Judgmen*t (December 4). Available at SSRN: http://ssrn.com/abstract=1558043 or http://dx.doi.org/10.2139/ssrn.1558043, Accessed on 15.01.2015.
7. Guarino, Alessandro (2014). *What Now? Data Retention Scenarios after ECJ Ruling", in Helmut Reimer, Norbert Pohlmann, Wolfgang Schneider (eds.), ISSE 2014 Securing Electronic Business Processes,* Springer ViewegL: 249-255, available at http://www.academia.edu/7998655/What_now_Data_retention_in_the_EU_after_the_ECJ_ruling, Accessed on 15.01.2015.
8. Guild, Elspeth, Carrera, Sergio (2014). *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive* (May 29). CEPS *Liberty and Security in Europe Papers* No. 65. Available at SSRN: http://ssrn.com/abstract=2445901, Accessed on 15.01.2015.

9. Kosta, Eleni (2013). *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection,* SCRIPT- ed. 10/2013; 10(3):339. DOI: 10.2966/scrip.100313.339, http://script-ed.org/wp-content/uploads/2013/10/kosta.pdf, Accessed on 15.01.2015.
10. Law 298/2008, retrieved from http://www.cdep.ro/proiecte/2008/400/30/9/pr439_08.pdf, Accessed 15.01.2015.
11. Law 82/2012, retrieved from http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-nr822012-privind-retinerea-datelor.html, Accessed on 15.01.2015.
12. *Luxembourg Weekly*, (17.05.2014). *Reflections on EU law and CJEU jurisprudence* retrieved from http://luxembourgweekly.blogspot.ro/2014/05/c29312-and-c59412-digital-rights.html, Accessed 15.01.2015
13. Rauhofer, Judith, Sithigh, Daithi Mac (April 16, 2014). *The Data Retention Directive that Never Existed*. SCRIPT – ed., 2014, 11(1); *Edinburgh School of Law Research Paper* No. 2014/34. Available at SSRN: http://ssrn.com/abstract=2467244, Accessed on 15.01.2015.
14. Romanian Constitutional Court Decision 440/2014, retrieved from http://www.ccr.ro/files/products/Decizia_440_20141.pdf , Accessed on 15.01.2015
15. Romanian Constitutional Court Decision no. 1258/October 2009, retrieved from http://www.legi-internet.ro/jurisprudenta-it-romania/decizii-it/decizia-curtii-constitutionale-referitoare-la-legea-pentru-pastrarea-datelor-de-trafic-298-2008.html, Accessed on 15.01.2015.
16. Romanian Constitutional Court Decision 461/16th September 2014, retrieved fromhttp://www.ccr.ro/files/products/Decizie_461_2014.pdf, Accessed on 15.01.2015.
17. BBC.co.uk (6.05.2015), *French parliament approves new surveillance rules*, retrieved from http://www.bbc.co.uk/news/world-europe-32587377, Accessed on 6.05.2015.