UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW
No. 2/2015

Edited biannually by courtesy of the Criminal Law Departments within the Law Faculties of the West University of Timisoara and the University of Pécs

2015

ICT, Data Retention, and Criminal Investigations of Economic Crimes

DR. PHD SILVIA SIGNORATO [*]
Research Fellow in Criminal Procedure, School of Law,
University of Padua (Italy)
Lecturer in Criminal Procedure,
Institut für Italienisches Recht, University of Innsbruck (Austria)

Abstract:

The Information and Communication Technology nowadays plays a core role in the execution of crimes of economic criminality. This seems to be due to two factors, that can be defined as the structural factor and the instrumental factor. Moreover, every time we use the new technologies we leave behind us some sorts of "traces", i.e. the traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. Such data can be extremely useful in the context of criminal investigations. The regulation on the obligation of the States to require the retention of such data by service providers for investigative purposes, for the discovery and repression of crimes is called "data retention". Data retention has some general features that are valid at global level. Within the European Union the respective regulation set out by the Directive 2006/24/EC has been declared invalid by the Court of Justice of the European Union. Therefore it seems necessary to adopt a new European regulation on data retention, regarding to which the article traces in its conclusions the possible reference points.

Keywords: *criminal investigations, cyber investigations, economic crimes, data retention, Directive 2006/24/EC, judgment of the Court of Justice of the European Union of the 8th of April 2014 Digital Rights Ireland and Others, right to respect for private and family life, right to protection of personal data, right to freedom of expression and information.*

1. The use of the Information and Communication Tecnology by economic criminality

Economic criminality takes advantage – and will increasingly take advantage – of the Information and Communication Technology – "ICT" in short – in order to pursue its criminal purposes. This seems to be due to two factors, which can be defined as the "structural factor" and the "instrumental factor".

a) The first factor, *i.e.* the **structural factor**, is represented by the fact that the *Information and Communication Technology* nowadays plays a core role in the execution of economic activities.

We may consider, for example, the importance of informatics in the processes of industrial production, the management of banking data, the industrial accountability

[*] E-mail: *silvia.signorato@unipd.it.*

and the payment of taxes by industries to the State. Furthermore, the very same economic and financial transactions nowadays take place in a virtual way. In this regard it is necessary to recall not only systems of electronic payments such as payments by credit cards, *online* bank transfers or *paypal*, but also transactions carried out with real virtual currencies – the so-called *crypto-currency* – such as *Bitcoin* and *Litecoin.*

From the fact that the *Information and Communication Technology* nowadays takes on structurally a fundamental role in the execution of economic activities we can infer that also the criminal activities concerning economic activities[1] make use more frequently of the *Information and Communication Technology*.

b) The second factor of the use of informatics and the net for the purposes of economic criminality, *i.e.* the **instrumental factor**, is explained by the fact that the use of the new technologies facilitates the execution of crimes and renders their prosecution more difficult.

In particular the use of the net facilitates the anonymity in the execution of crimes. Moreover the acquisition of digital evidence is complex and it is necessary that investigators follow what are known as "best practices"[2], since an irregular acquisition of evidence can alter the evidence itself. Finally, the virtual nature and the non-territorial nature of the net can lead to relevant problems in determining the State that is effectively entitled to carry out the investigations.

It is therefore possible to say that the use of informatics for criminal purposes can result in an instrument that impedes investigative activities to the point of becoming a counter-investigative strategy.

2. The importance of *data retention* in the context of criminal investigations against economic criminality

The repression of economic criminality crimes is surely more difficult when these crimes are executed with the use of new technologies and, in particular, such new techniques as steganography[3] and cryptography[4], or computer programs that allow anonymization.

Nevertheless the repression of such crimes remains still possible, also thanks to the acquisition of certain types of data. In this regard it is necessary to recall that every time we use a *computer system* (such as, a computer, a notebook, a tablet, a last generation mobile phone, etc.) we leave behind a series of "traces". They represent the location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user and to traffic data. Moreover, as regards this latter

[1] For an analysis of economic crimes relating to the use of new technologies see U. SIEBER, *La delinquence informatique,* E. Story-Scientia, 1990, p. 7 et seq.

[2] E. Casey, *Digital evidence and Computer Crime: Forensic Science, Computers and the Internet,* Academic Press, 2011, p. 17r et seq.; S. SIGNORATO, *Electronic investigations in Italian criminal proceedings*, in *Analele universității de vest din Timisoara*, seria drept, 2014, n. 1, p. 10 et seq.

[3] D. Buso - D. Pistolesi, *Le perquisizioni e i sequestri informatici*, in F. Ruggieri – L. Picotti (eds.), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Giappichelli, 2011, p. 185; G. Costabile – M. Mattiucci – G. Mazzaraco, *Crittografia, steganografia e tecniche di analisi forense*, in S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco (eds.), *Computer forensics e indagini digitali, Manuale tecnico-giuridico e casi pratici*, vol. III, Experta, 2011, p. 633 et seq.

[4] G. Ziccardi, *Crittografia e diritto*, Giappichelli, 2003 and, as regards the purely technical aspects of cryptography, see D. R. STINSON, *Cryptography, Theory and Practice*, 3rd edition, CRC Press, 2005.

data, under article 1, letter d), of the *Convention on Cybercrime* «"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service»[5].

Such data can play a fundamental role for investigative purposes. For this reason many States require that those who provide publicly available electronic communications services or public communications networks to retain this data for the purposes of the investigation, the detection and the prosecution of crimes. This occurs irrespective of the fact that the crime relating to whose investigations such data can be useful may already have been committed. The data storage activity takes place indeed regardless of the fact that a crime has been committed and of the existence of a *notitia criminis*, i.e. of a crime report.

This preventive storage activity telematics data is defined as ***data retention***[6].

Relating to the subject at hand it seems appropriate to point out the following aspects, that relate in general to the retention of data, regardless of the fact that such data are being retained by providers of publicly available electronic communications services or of public communications networks subject or not subject to the law of the European Union.

a) The persons whose data is being retained. Everybody's data is being retained, even if it relates to persons who are not suspects and who will never become suspects. Not even their age matters. Therefore it represents a collection of data carried out *erga omnes*, i.e. towards everyone.

b) The persons who store the data. The data is being stored by service providers and by telephone line managers. It is necessary to stress that such persons are normally not public entities, but private individuals. They follow market reasons, not justice ones. This can lead to some problematic aspects, also on the level of security of the storage of data itself.

c) The global nature. If a communication takes place in a certain State, it is not granted that the respective traffic and location data on persons and to the related data necessary to identify the subscriber or registered is retained by providers of services that have their seat in the same State. On the contrary such electronics *data* is stored always more frequently in a different State from the one where the communication took place. This entails that in the investigative context it is often necessary to acquire *traffic*

---

[5] See art. 1, d), of the Convention on Cybercrime of the Council of Europe, signed on the 23rd of November 2001. «Traffic data» do not concern the content of communications. It is however necessary to point out that while, as regards traditional telephone communications, it is possible to distinguish between data relating to and data not relating to the content of a communication, such a distinction becomes blurred in the context of those forms of communication that use new technologies. See L. BACHMAIER WINTER, *Criminal investigation and right of privacy: the case-law of the European Court of Human Rights and its limits*, in Lex ET Scientia, Juridical Series, vol. II, 2009, p. 12.

[6] «Data retention is distinct from data preservation (also known as 'quick freeze') under which operators served with a court order are obliged to retain data relating only to specific individuals suspected of criminal activity as from the date of the preservation order. Data preservation is one of the investigative tools envisaged and used by participating states» under the art. 16 Convention on Cybercrime of Council of Europe. See *Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC),* Brussels, 18.4.2011, COM(2011) 225 final, p. 5.

data retained in another State[7]. That is however possible by recurring to a letter rogatory or other tools eventually foreseen for cross-border gathering of evidence[8]. In this regard it is furthermore necessary to point out how the use of such tools usually leads to an extension of the time necessary to obtain evidence.

d) The length of data retention. Traffic data is retained for the time foreseen by the State on whose territory the *service provider* or the telephone line manager storing this data has its seat.

Moreover every State has its own different regulation on *data retention*. In this regard it seems possible to identify three groups of States.

A first group seems even unwilling to adopt a regulation on *data retention* or foresee really very short periods of time to retain data.

On the contrary a second group of States foresees that data be retained for extremely long periods of time, to the point that such data are not just investigative instruments but seem almost functional to a sort of mass control over the citizens.

On an intermediate level there is finally a third group of States that foresees a period of retention of data wavering between 6 months and 24 months[9].

The fact that every State foresees such different periods of retention of data can however constitute a problematic aspect for criminal investigations.

e) The violation of fundamental rights. *Electronic data* is no neutral data. It is data that, if combined with other data, can allow to go back up to several features of a person, including personal relationships, professional relationships, social relationships, religious beliefs or political views. It is therefore a very personal data and it determines an interference in one's *privacy*.

In this regard it is however necessary to point out that not all States consider *privacy* in the same way.

On the one hand there are States – such as the Member States of the European Union – that consider privacy as a fundamental right in its double nature of *right to be let alone* and *right to have control over access to personal information*. Moreover, the European Convention on Human Rights foresees in article 8 the right to respect for private and family life. Furthermore also the Charter of Fundamental Rights of the European Union recognizes in article 7 the right to respect for private and family life and in article 8 the right to protection of personal data.

On the other hand there are States where the right to privacy has however only recently been established, since for a long time such right has been considered as breaching the ethical tradition[10].

---

[7] On the transnational dimension of electronic investigations see M. SIMONATO, *YP Special Report, Defence rights and teh use of information technology in Criminal procedure,* in *Revue international de droit Pénal,* 2014, p. 279 et seq.

[8] On cross-border gathering of evidence see M. DANIELE, *Ricerca e formazione della prova,* in R. E. KOSTORIS (ed.), *Manuale di procedura penale europea,* 2 edition amended and extended, Giuffrè, 2015, p. 355 et seq.

[9] As indicated in the *Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, Brussels, 18.4.2011, *COM(2011) 225 final*, Table 3, p. 14, by the time of the report among the Member States of the European Union that foresee the same period of retention of the various kinds of data, Poland foresees a two-year-retention period of retention; Latvia established a 1-and-a-half-year period of retention; Bulgaria, Denmark, Estonia, Greece, Spain, France, Netherlands, Portugal, Finland, United Kingdom set out a period of retention of one year; finally, Cyprus, Luxembourg, Lithuania foresee a period of retention of six months.

3. The invalidity of the Directive 2006/24/EC on data retention

In European Union data retention[11] has been last regulated by the Directive 2006/24/CE[12]. Since its adoption it has been a highly controversial directive from the point of view of its conformity to fundamental rights and, in particular, the right to *privacy*[13].

Nevertheless, on the basis of the Directive 2006/24/CE many European States have foreseen or amended their national regulation on data retention. However precisely those national regulations implementing this directive have raised some constitutional issues. This lead to the Constitutional Courts of Romania[14], the Czech Republic[15] and Germany[16] declaring non-constitutional their national dispositions implementing the directive on data retention[17].

Even though the judgments of these three Constitutional Courts present some differences, it can be pointed out that the non-constitutionality aspects were related especially to the lack of proportionality of the regulation on data retention, the absence of a precise list of subjects authorised to request such data and the general referral to "serious crime" without any further clarification.

After the judgments of the Constitutional Courts of Romania, the Czech Republic and Germany declaring as non-constitutional the respective national implementing regulations, the Court of Justice of the European Union (ECJ) received a request for preliminary ruling from the High Court of Ireland and one from the Austrian Constitutional Court concerning the validity of the Directive 2006/24/CE[18].

---

[10] This is what happened in the People's Republic of China. In this regard see S. WU, *La tutela penale della privacy nell'epoca di Internet. Esperienze italiane e cinesi a confronto*, Edizioni Scientifiche italiane, 2012, p. XXI.

[11] See E. D. Busser, *European initiatives concerning the use of it in Criminal procedure and data protection,* in *Revue international de droit Pénal*, 2014, p. 213 et seq.

[12] 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.

[13] In the system of European legal sources, directives foresee an obligation of result. It is then up to the every single Member State to determine how to achieve such a result.

For an overall view of the plurality of legal sources in the context of European criminal procedure, see R.E. KOSTORIS, *La dimensione reticolare delle fonti*, in R.E. KOSTORIS (ed.), *Manuale di procedura penale europea*, 2nd ed. amended and extended, Giuffrè, 2015, p. 68 et seq.

[14] See Constitutional Court, judgment n. 1258 of the 8th of October 2009.

[15] See Constitutional Court, judgment of the 22nd of March 2011.

[16] See Constitutional Court, judgment of the 2nd of March 2010. See R. Flor, *Le recenti sentenze del Bundesverfassungsgericht e della Curtea Constituțională sul data retention*, in L. Violante - T. Galiani - A. Merli (eds.), *Oggetto e limiti del potere coercitivo dello Stato nelle democrazie costituzionali*, in *Annali della facoltà giuridica*, Camerino, 2013, p. 308 et seq.

[17] See also Supreme Administrative Court of Bulgaria, decision n. 13627 of the 11th of December 2008; Supreme Court of Cyprus, actions nn. 65/2009, 78/2009, 82/2009 and 15/2010-22/2010, of the 1st of February 2011; constitutional action brought on the 2nd of June 2008 in Hungary by the Hungarian Civil Liberties Union.

[18] Also the Slovenian Constitutional Court has been requested to rule on the constitutionality of its national regulation (Articles 162 to 169 of the Electronic Communications Act - Official Gazette RS No. 109/12 -) implementing the Directive 2006/24/EC. Moreover, the Slovenian Constitutional Court ruled by order on the 26th of September 2013 that the proceedings to review the constitutionality of Articles 162 to 169 of the Electronic Communications Act should be stayed until the Court of Justice of the European Union adopts a decision in Cases C-293/12 and C-594/12. For the order see http://www.us-rs.si/media/u-i-65-13.-.order.pdf

Following these requests for a preliminary ruling, on the 8th of April 2014 the Grand Chamber of the Court of Justice of the European Union[19] considered firstly the relevance of Articles 7 (Respect for private and family life), 8 (Protection of personal data) and 11 (Freedom of expression and information) of the Charter of fundamental rights of the European Union with regard to the question of the validity of the Directive. It has then proclaimed the existence of an interference with the rights laid down in articles 7 and 8 of the Charter and has examined whether such an interference was justified and proportionate.

Having regard to such an analysis the Court of Justice concluded by ruling that the Directive 2006/24/CE was invalid, since it did not comply with the principle of proportionality examined in the light of articles 7, 8 and 52 (Scope of guaranteed rights), par. 1, of the Charter of fundamental rights of the European Union.

With regard to such invalidity the judgment considered that there was no reason to examine also the validity of the directive in the light article 11 of the Charter[20].

4. Towards new European horizons of data retention

The judgment of the Grand Chamber of the Court of Justice of the European Union pronounced on the 8th of April 2014 has represented a fundamental judgment not only at a European level, but also at a global level, since it has become a significant reference point in data retention matters.

Following this judgment two kinds of issues arose at a European level. Firstly, one finds the issue of understanding the fate of the national regulations implementing the directive declared invalid. Secondly, one finds the issue relating the increasing need for the European Union to adopt a new regulation on data retention. The attention will be focused on the latter need.

In order to determine the reference points of the new regulation it is necessary to start by examining the rights that have a prominent role. In this regard it is necessary to point out that every regulation on data retention can lead to at least a double restriction of rights.

Firstly, we witness a strong interference with the **right to privacy**[21]. As specified by the Court of Justice of the European Union, the mere fact that service providers retain data constitutes in itself an interference[22] with such a right. As regards data retention, the subsequent access of national authorities to the data constitutes therefore a further interference with the right to privacy[23].

Secondly, data retention can cause also a restriction of the **right to freedom of expression**. Since their data is being retained, private individuals can in fact use the means of communication in a more limited way or anyway in a different way than the one they would have opted for had the regulation on data retention not existed[24].

---

[19] See Court of Justice of the European Union (Grand Chamber) of the 8th of April 2014, *Digital Rights Ireland and Others*, Joined Cases C-293/12, C-594/12.

[20] See Court of Justice, 8th April 2014, C-293/12 and C- 594/12, *cit.,* paragraph 70.

[21] «To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way». See, to that effect, Court of Justice, 20 May 2003, *Österreichischer Rundfunk and Others,* Cases C-465/00, C-138/01 and C-139/01, paragraph 75.

[22] See Court of Justice, 8th April 2014, C-293/12 and C- 594/12, *cit.,* paragraph 34.

[23] See Court of Justice, 8th April 2014, C-293/12 and C- 594/12, *cit.,* paragraph 35.

[24] See Court of Justice, 8th April 2014, C-293/12 and C- 594/12, *cit.,* paragraph 28.

Both the right to privacy and the freedom of expression are protected by the Charter of Fundamental Rights of the European Union as well as the European Convention on Human Rights.

These are rights that can be legitimately limited only in accordance with a legal disposition. Furthermore, as regards the right to privacy, such a restriction is legitimate only if it is necessary in a democratic society, in the interests of national security, public safety or the economic wellbeing 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[25]. While, as regards the freedom of expression, such a restriction is legitimate if it is necessary in a democratic society in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary[26].

Moreover, these rights can be limited only so long as they respect the principle of proportionality. Therefore, every European regulation on data retention will have to comply firstly with the principles of proportionality and necessity.

5. Conclusions

In my opinion, at a European level it would be necessary to adopt two separate and different regulations, on the one hand, for data retention and, on the other one, for the subsequent activity of data acquisition by the national authorities.

In particular, as regards the **activity of data retention**, it would seem appropriate that the new European regulation would:

a) precisely define the subjects that have to retain data;

b) allow that the activity of data retention be carried out towards everyone, since it is not possible to determine a priori the subjects that may commit a crime;

c) point out the goals according to which the retention is carried out;

d) radically exclude the possibility of retaining the contents of communications;

e) define the period of data retention, which has to be neither too short nor too long, and establish the same period for the telephone traffic data as well as for the telematics data, since it seems unreasonable to set out different periods of time for these two kinds of data;

f) foresee that the data retention be carried out in those States of the European Union or in third countries that ensure a protection of the rights equal to or superior to the one foreseen within the European Union;

g) require the respect of the rules of security in the retention of data;

h)determine adequate guarantees to prevent abuses in the retention of data, including the illegal use of data[27], also as regards the automatic processing of data;

---

[25] See art. 8.2 of the European Convention on Human Rights.

[26] See art. 10.2 of the European Convention on Human Rights.

[27] See, to that effect, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, paragraph 62 and 63.

i) proclaim once more the necessity of the existence of an independent authority surveying the correct retention of data;

j) effectively contribute to the harmonisation of the dispositions of the Member States on data retention by those who provide publicly available electronic communications services or public communications networks.

II. On the other hand, various provisions should be adopted in relation to the subsequent **activity of acquisition of data by the national authorities**.

In this regard it would be appropriate that the respective regulation would:

a) precisely define the subjects entitled to acquire such data, limiting the number of persons authorised to have access to the data to what is strictly necessary;

b) require the judicial control over the request to acquire the data;

c) precisely determine the crimes that authorise the acquisition of data;

d) set out that the data acquired by violating the substantial and procedural requirements cannot be used in the context of a criminal proceeding.

If there do not seem to exist any doubts relating to the necessity to adopt a new European regulation on data retention, the issue however remains, as already mentioned, that data is often retained by service providers not located in a Member State of the European Union. Therefore, it would be necessary also to harmonise the regulations on data retention of the states that are not members of the European Union. This is surely a long path and one that is still partly to be walked through, but it could receive a significant impulse from the very same predisposition of a new European regulation on data retention, if it will be recognised that its regulation plays the role of relevant reference point on the matter.