Giuseppe Vaciago

The Invalidation of the Data Retention Directive: A balance of interests between security and fundamental rights

1. Introduction

There is a general tendency to consider content posted online by users as being anonymous. This is only partially true, as a person committing a crime online can be apprehended with the collaboration of Internet Service Providers (ISPs) which store subscribers' IP addresses[1] (that identify the individual devices from which the net is accessed) and web server logs[2] (that maintain a record of all the online activity conducted through each IP address).

Prosecutors generally obtain the IP address of a suspect's computer by subpoenaing the e-mail or hosting service provider in question to disclose the relevant data which can then be used to compel the Internet connectivity providers involved to reveal the precise location of the individual or business billed for the use of the corresponding web connection. The type of server log data that Internet Service Providers may be ordered to disclose varies in function of the specific offences under investigation.

Acknowledging that the storage of traffic and location data by connectivity and ISPs (data retention) is crucial to law enforcement, Europe has adopted stringent data retention regulations (Directive 2006/24/EC) under which IP addresses and server logs are subject to storage for periods of not less than six months and not more than two years from the date of the communication.

The application of these regulations was initially supposed to be limited to serious crimes, but in many Member States they were also applied to less important offences such as online defamation. The consequence of the fact that it is possible to identify those posting online in countries where defamation is a crime has been an increase in related litigation. For example, a public figure may protect his image through targeted legal actions against bloggers who berate this person for their actions. All this may have an impact on freedom of expression online.

[1] An IP address is a numerical identification code assigned to each and every device connected to an electronic network, comparable to a street address or a telephone number. Given a specific IP address and the time the net connection was established, an ISP can trace the personal data of the individual who signed the related connectivity service contract.

[2] The web server log is a log file containing the records of all the online activities undertaken by a given user.

Calls for similar regulations on the other side of the Atlantic were, however, met with vigorous opposition and loud protests, especially by the EPIC (Electronic Privacy Information Center) and the EFF (Electronic Frontier Foundation), and were further fired by the scandal that erupted in 2013 when the public got wind of the National Security Agency's secret deal with the largest national telecommunications carriers and Internet Service Provider. Naysayers warned that if data retention were legalized, there would be no end to the misuse of the stored information for purposes very different from the law enforcement goals pursued under the proposed regulatory framework, with the result that web traffic data could end up being subpoenaed at the drop of a hat, not least for censorship reason (Zittrain 2002).

In this complicated background, eight years after it was issued, on April 8 the Court of Justice declared the Data Retention Directive invalid by reason of the fact that it is contrary to fundamental human rights.[3]

2. The key points of the CJEU decision

Prior to 8 April 2014, the CJEU had to intervene in February 2009 (CJEU, Case C-301/06) rejecting the appeal brought by Ireland and Slovakia, which had filed for annulment of the much criticised Data Retention Directive. The application for annulment of the Data Retention Directive was based on the assumption that this Directive had not been issued to harmonise legislation in order to favour the domestic market in the electronic communications sector, but to promote the collection of data for public security purposes and in order to combat terrorism. In fact, these purposes are part of "judicial and police cooperation against crime" and ought not to have been regulated through a European Union directive.

Furthermore, between 2010 and 2013 the Constitutional Courts in a number of Member States (Bulgaria,[4] Germany,[5] Romania,[6] Czech Republic[7] and Cyprus)[8] had one after the other declared that their respective national laws transposing the Data Retention Directive were unconstitutional whilst some Member States (Austria and Sweden) had even refused to transpose the Data Retention Directive into their national legal framework.

[3] Court of Justice of the European Union, April 8th 2014, Judgment in Joined Cases C-293/12 and C-594/12 P Digital Rights Ireland and Seitlinger and Others.

[4] Decision by the Supreme Administrative Court of Bulgaria on 11 October 2008, http://edri.org/edrigramnumber6-24bulgarian-administrative-case-data-retention/.

[5] Decision by the Bundesverfassungsgericht [BVerfG] (Federal Constitutional Court), 2 March 2010, no. 256/08, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html. For further detail, see the press release issued by the German Constitutional Court, http://www.bverfg.de/pressemitteilungen/bvg10-011en.html.

[6] Decision by the Romanian Constitutional Court no. 1258 on 8 October 2009, http://snurl.com/28w8ylp.

[7] Decision by the Czech Republic Constitutional Court on 22 March 2011, http://www.concourt.cz/view/GetFile?id=5075.

[8] Decision by the Cyprus Supreme Court on 1 February 2011 regarding some of the provisions of Law 183/2007 on disclosure telecommunications data.

The reasons for invalidating the transposition of the Data Retention Directive stated by these national Constitutional Courts have now—almost verbatim—been taken over by the CJEU: the first point was the lack of proportionality in the storage of traffic data which was wrongfully considered less important than the contents of the communications, whilst the second one related to the absence of any precise list of those entitled to ask for this data; the third one concerned the vagueness of the expression "serious crime". These three points were already explored by the European Commission,[9] Council of Europe[10] and the Article 29 Working Party.[11]

2.1. Lack of proportionality

With regard to the first point (paragraphs 26-28 of the decision), it was specified that traffic data required under the Data Retention Directive make it possible to discover not only the identity of a user, but also where and when the user was. Those data, taken as a whole, may allow very precise conclusions about the private life of the individual, certainly when data has been retained such as 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. Even if the Data Retention Directive does not apply to the retention of the content of communications, it has long been argued that search queries themselves would be considered content rather than traffic data and the Directive would therefore not justify their retention. These observational possibilities, as the European Court of Justice correctly underlined, conflict with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

2.2. Eligibility of retained data

With regard to the second point (paragraphs 60-62 of the decision), article 4 Data Retention Directive established that "procedures to follow and conditions to be fulfilled for accessing data retained in accordance with criteria of need and proportionality are defined by every Member State in its national legislation, subject to the provisions of the European Union or international public law and specifically the Charter of Fundamental Rights

[9] Report by the European Commission to the Council of Europe and the European Parliament, *Evaluation Report on the Data Retention Directive (COM(2011) 225).*

[10] Council of Europe, Information Note, 5 May 2014, *Invalidation of 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.*

[11] With regard to this matter, the Article 29 Working Party drew up report 1/10 on 13 July 2010 entitled C*ompliance 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*. More recently the "Article 29" group intervened in this matter expressing two opinions: *Opinion 1/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* and *Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes.*

of the European Union, in accordance with the interpretation by the European Court of Human Rights." Greater harmonisation would have been advisable amongst the various European Union Members in respect of the right to access traffic data, as would greater clarity on the part of the relevant European Union legislation. Whilst it is true that in almost all the Member States (except for United Kingdom, Ireland and Malta) this right must undergo scrutiny by the prosecutor in charge of proceedings or by the court, it is also true that in fourteen countries[12] the request may also be made by the national security agencies or by other government authorities.

2.3. Vagueness of "serious crime"

With regard to the third point (paragraphs 41-43 of the decision), the uncertainty of the expression "serious crime" gave to the national legislator the difficult task of framing the definition within his national legislation back to the national legislator. In this case too, the result is particularly uneven: ten Member States[13] have effectively transposed into national legislation the concept of "serious crime", limiting the scope of application of the Directive to crimes carrying a certain custodial sentence or to crimes contemplating the application of precautionary custodial sentences or directly listing unlawful cases where it was possible to access data; instead, eight Member States[14] have failed to transpose these indications, whilst the remaining four[15] included the expression "serious crime" in their national legislation without however defining it.

Such widespread access to potentially sensitive data in the absence of a clear, well-defined European Union directive, in the opinion of the CJEU, gives rise to conflict with articles 7, 8 and 52 of the European Charter of Human Rights and Fundamental Freedoms, also in view of the case law precedents of the European Court of Human Rights. In fact, the European Court of Human Rights has already emphasised, prior to application of the 2006/24/CE Directive, that there was a possible conflict with articles 7 and 8 of the Convention on Human Rights in cases where the memorisation of potentially sensitive data regarding one's private affairs is not expressly regulated.[16] Hence the declaration invalidating the 2006/24/EU Directive.

However, even if there is a conflict with the European Charter of Human Rights, it cannot be denied that this law represents a valid tool for criminal justice and judicial police, because traffic data constitutes an evidentiary element which, when detected with other evidence, might allow for the identification of a criminal or a connection between two or more people under investigation. For example, it should be considered that in

[12] The countries contemplating this option are: Bulgaria, Estonia, Finland, Greece, Ireland, Latvia, Lithuania, Luxemburg, Malta, Poland, United Kingdom, Spain, Hungary and Slovenia.

[13] The countries defining the concept of "serious crime" are: Bulgaria, Estonia, Ireland, Greece, Spain, Latvia, Luxemburg, Hungary, Holland and Finland.

[14] The countries failing to transpose the concept of "serious crime" are: Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia and Slovenia.

[15] The countries that have not given a clear definition of the concept of "serious crime" are: Cyprus, Malta, Portugal and the United Kingdom.

[16] Amann v. Switzerland, 2000-II Eur. Ct. H.R. 247, [section] 65 e Copland v. United Kingdom, 2007, 45 Eur. Ct. H.R. 253, [section] 43.

2008, in Belgium, the kidnappers of an employee of Antwerp law-court have been convicted thanks to the analysis of the criminal defendants' traffic data; similarly, in 2009, in Czech Republic, thanks to the IP addresses provided by the ISPs many people involved in the trafficking of child pornographical abuse images and videos were arrested.[17]

3. THE TECHNOLOGICAL LIMIT: RELIABILITY

The problems with data retention are not merely of a legal nature: having obtained the dynamic IP address of a person under investigation (often with great efforts), judicial police officials frequently find themselves faced with three additional technological problems (circumvention of the data retention investigation, abuse of the identity, and lack of respect in digital forensics procedure), which seriously raise the risk of investigations being conducted against the "wrong person". Besides the not too small risk of starting an investigation on a false second in time, there are three further aspects.

3.1. Circumvention

One serious problem is the numerous ways in which to circumvent the retention of one's traffic data. The perhaps best known way for hiding one's activities online is using a proxy server. Another way includes the use of "anonymous re-mailers", for example, which are servers receiving e-mail messages and resending them in accordance with specific instructions included in the messages, without revealing their original provenance.[18] A perhaps banal and easily used technique is to merely leave an e-mail in draft form in any webmail service and provide the recipient with the password for accessing the service in order to avoid producing any data traffic.

3.2. Abuse

Techniques for fraudulently using a person's computer identity are particularly widespread; and in these cases the person committing an unlawful act not only hides his or her identity, but creates the conditions according to which his conduct appears as that of another user. A hacker can acquire identity and password of an unsuspecting innocent user and surf online under false identity. The acquisition of identity and password can take place either "old fashionedly" (by managing to glean the user's details directly or by accessing an unprotected wireless network) or digitally (by using special malware referred to as "Trojan horses"). Such applications are seemingly innocuous and invisible but they are installed on computers with the aim of monitoring and spying on system operations, in order to acquire ID characteristics.

[17] European Commission, *Evaluation Report on the Data Retention Directive (COM(2011) 225)*, p. 24.
[18] For more information on this matter, see Danezis, Dingledine and Mathewson 2003.

3.3. Digital forensics

In addition to these technological restrictions making it significantly more difficult to identify the perpetrator of an unlawful act,[19] we should also draw attention to limitations pertaining to failure to comply with digital forensic procedures, in other words a set of rules designed to allow and subsequently demonstrate that digital evidence has been acquired without being altered or modified. To this we should underline that, often, ISPs forward traffic data to law enforcement agencies without considering the best digital forensics practices[20] designed to ensure that evidence that has been sent has not been altered.

4. IMMEDIATE IMPACT AND CHALLENGES

The CJEU has not determined the invalidity of any Member State's legislation governing the retention of data. Pursuant to Article 267 of the European Union Treaty, the CJEU's jurisdiction may directly cover only European Union actions, and not national ones.

It is not possible to forecast the timeframe for issuing a new directive on data retention, in part due to the degree of complexity which such legislation entails and in part because Parliament's priority is to approve the European regulatory framework governing the protection of personal data. Therefore, the transitional regime is likely not to be short term, unless there is:

- a deliberate legislative decision by the Member States or
- a decision of the national Constitutional Court declaring the national rules on data retention unconstitutional and void because of their conflicts with individuals' fundamental human rights.

These two eventualities may occur over the short term, even though it is more likely that Member States will simply wait for a new directive on data retention to be issued which is capable of clarifying the issue of uncertainty as well as the issue of legitimacy which was raised by the CJEU.

In case a national law is declared unconstitutional in a Member State or a new law concerning data retention is approved, it is legitimate to wonder if the traffic data collected when the law implementing Directive 2006/24/EC was in force could be excluded from trial. In this case it is appropriate to consider the "fruit of the poisonous tree"[21] theory. It is a legal metaphor used to describe evidence that has been obtained illegally implying that if the source of the evidence is tainted, then anything gained from it is tainted as well.

[19] On this point see the shadow report issued by the European Digital Right in Europe association, EDRI, *Shadow Evaluation Report on the Data Retention Directive (2006/24/EC)*, 17 April 2011, http://www.edri.org/files/shadow_drd_report_110417.pdf.

[20] OLAF, *Guidelines on Digital Forensics Procedures for OLAF Staff*, 1 January 2014, http://ec.europa.eu/anti_fraud/documents/forensics/guidelines_en.pdf.

[21] See Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385 (1920).

This theory is applied in almost all Member States[22] in case of irregularly obtained evidence and it is confirmed by the case law of the ECtHR, which, in some cases, excluded from trial the evidence obtained in cases of violation of human rights.[23]

Nevertheless, it should be mentioned that in case of data retention the evidence acquisition would be considered irregular *ex post* following the European Court of Justice decision, whilst usually the "fruit of the poisonous tree" theory applies when there is a violation of a law in force. Moreover, the judges apply this theory with adequate caution because of the effect that it can have on the result of the trial.

However, it is question that might be raised in the future as the Court of Justice believes the Data Retention Directive is in contrast with fundamental rights (articles 7 and 8 of ECHR).

5. Implication for US providers?

The "Snowden" revelations have certainly shaken up European citizens with regard to the manner in which the large US providers, which account for almost 3 billion users throughout the world, manage data. Nevertheless, it should be borne in mind that these providers are under no duty to comply with legislation governing data retention, by reason of the fact that they provide data to the European courts and government authorities on a voluntary basis, in accordance with section 2702 (b) (7) of the US Electronic Communication Privacy Act. This law entitles providers to reveal to courts, including in other countries, data traffic belonging to their users only when there is evidence that such data may be linked to the commission of a crime.[24]

It is therefore likely that American providers will not change their policies which were already in place prior to the arrival of the Data Retention Directive, but it cannot be ruled out that this decision may lead them to adopt a much "colder" attitude with regards to collaborating with European law courts.

However, one very interesting aspect of the decision, and which is in line with the currently proposed provisions in the Draft EU Data Protection Regulation,[25] relates to paragraph 68 of the decision in which the CJEU specifies that the scope of the Data Retention Directive should only concern traffic data in Europe. This modification, together with the fact that the currently proposed version of a regulation governing the protection of personal data put forward by the European Commission may impose supervision by an

[22] Only Spain and Poland have a specific exclusion of the "fruit of the poisonous tree". See Celine and Galli 2013.

[23] ECtHR, 1 June, 2010, Gafgen v. Germany, Application no. 22978/05.

[24] 18 US Code § 2702, "A provider described in subsection (a) may divulge the contents of a communication to a law enforcement agency if the contents: (i) were inadvertently obtained by the service provider; (ii) appear to pertain to the commission of a crime".

[25] Article 41 of the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

administrative authority over the legitimacy of traffic data acquired by law courts, significantly complicates investigations in the various Member States, especially in cases where traffic data originates from a jurisdiction outside Europe.

6. EU REFORM ON DATA RETENTION?

The CJEU has laid down a number of guidelines that have to be considered when a new data retention directive will be drafted. Amongst these guidelines, most important seem two: the need to limit the retention period (no more than six months) and the need to introduce clear procedures for accessing traffic data on the part of national authorities. Both of these needs must be fulfilled in compliance with the principles of traceability and security.

The fact remains that the declaration invalidating the Data Retention Directive gave rise to a regulatory vacuum at European Union level; this could be filled by focusing on considerations made by the European Commission in 2010[26] and by a number of commentators.[27] In order to guarantee respect for fundamental human rights, the EU Commission maintains that it is necessary to significantly intervene in the following critical aspects:

- restricting and harmonising the purposes of data retention and the types of crimes triggering the possibility to access and use traffic data;
- ensuring greater uniformity at a European level in respect of the data retention periods;
- limiting the number of those authorised to access this data and reducing the categories of data to be retained;
- supervising by means of an independent authority, procedures applied in the various Member States for accessing data;
- introducing guidelines for technological and organisational measures to access data and the use of this data, paying particular attention to the risk of data mining.[28]

The examination carried out by the EU Commission is certainly an excellent starting point for reaching a compromise between the need to safeguard state security and the need to safeguard the protection of European citizens' personal data. Against this background, it appears preferable to put a priority on two specific areas.

Procedural requirements. The first one concerns the procedures for submitting a request. In fact, if all the Member States required scrutiny by a judge and not by a public prosecutor or, in certain cases, the judicial police, a necessary condition for granting access to

[26] See the communication by the COM commission (2010) 573/4, *Strategy for the effective implementation of the Charter of Fundamental Rights of the European Union* and the report by the European Commission to the Council of Europe and the European Parliament, *Evaluation Report on the Data Retention Directive (COM(2011) 225)*.

[27] P. Hustinx, *The moment of truth for the Data Retention Directive*, speech during the conference "Taking on the Data Retention Directive", held at Brussels on 13 December 2010.

[28] To gain a better understanding of the potential offered by data mining techniques in investigations see Ngai et al. 2011.

traffic data, it would be possible to ensure that information which potentially affects an individual's fundamental human rights is considered and thus regulated in accordance with the same guarantees required in many Member States for obtaining wiretapping warrants.

Reduced scope of Directive. The second area concerns the need, at least nationally, to limit the scope of the Directive in particular with regard to defamation and privacy violation which, except for few extreme cases, cannot be considered "serious crimes". In fact, if these categories of crime were excluded, the number of requests to access traffic data made to ISPs would be significantly reduced.[29] This would benefit not only the ISPs, but also law enforcement professionals who seem to spend most of their time dealing with defamation and privacy issues rather than "serious crime". Also consider how hard it is for United States ISPs who voluntarily comply with legislation on European data retention to conceive of a crime "of opinion" when in their legal system freedom of expression is a fundamental value of the Constitution. The Section 230 of the Communication Decency Act (1996) is a landmark piece of Internet legislation in the United States that provides immunity from liability for providers and users of an "interactive computer service" who publish information provided by others.

Truthfully, the surveillance programmes are not only in the United States. In Europe, the Communications Capabilities Development Programme has prompted a huge amount of controversy, given its intention to create a ubiquitous mass surveillance scheme for the United Kingdom in relation to phone calls, text messages and e-mails and extending to logging communications on social media. More recently, on June 2013, the so called programme TEMPORA showed that UK intelligence agency Government Communications Headquarters (GCHQ) has cooperated with the NSA in surveillance and spying activites. These revelations were followed in September 2013 by reports focusing on the activities of Sweden's National Defense Rio Establishment (FRA). Similar projects for the large-scale interception of telecommunications data by both France's General Directorate for External Security (DGSE) and Germany's Federal Intelligence Service (BDE).

It will be interesting to observe how European intelligence services react to this ruling because those agencies have long defended the lawfulness of bulk collection of communications data through programmes such as TEMPORA, precisely because they involve retaining metadata rather than content, and the data is adequately protected. A first answer will be given by the case before the European Court of Human Rights brought by the "Privacy Not Prism Coalition" of UK civil society groups against these surveillance programmes.[30]

[29] The major US ISPs have created a transparency report in which are listed the entire requests they receive from the Law Enforcement. For more information see Google Transparency Report, http://www.google.com/transparencyreport/removals/government/?hl=it.

[30] Application no. 58170/13 to the European Court of Human Rights made by Big Brother Watch, Open Rights Group; English PEN, Dr. Constanze Kurz v. United Kingdom.

7. BIG DATA AND SURVEILLANCE

To stay on the topic of surveillance tools, it is worth mentioning that it is increasingly possible for courts and government authorities to monitor users' online activity through analysing open sources online. There are two interesting cases of the Big Data collection through OSInt (Open Source Intelligence) tools for crime prevention purposes.

The first is the "PredPol" software initially used by the Los Angeles police force and now by other police forces in the USA (Palm Beach, Memphis, Chicago, Minneapolis and Dallas). Predictive policing, in essence, cross check data, places and techniques of recent crimes with disparate sources, analysing them and then using the results to anticipate, prevent and respond more effectively to future crime. Even if the software house created by PredPol declares that no profiling activities are carried out, it becomes essential to carefully understand the technology used to anonimyze the personal data acquired by the law enforcement database. This type of software is bound to have a major impact in the US on the conception of the protection of rights under the Fourth Amendment, and more specifically on concepts such as "probable cause" and "reasonable suspicion" which in future may come to depend on an algorithm rather than human choice (see Ferguson 2012).

The second example is X1 Social Discovery software.[31] This software maps a given location, such as a certain block within a city or even an entire particular metropolitan area, and searches the entire public Twitter feed to identify any geo-located tweets in the past three days (sometimes longer) within that specific area. This application can provide particularly useful data for the purpose of social control. One can imagine the possibility to have useful elements (e.g. IP address) to identify the subjects present in a given area during a serious car accident or a terrorist attack.

From a strictly legal standpoint, these social control tools may be employed by gathering information from citizens directly due to the following principle of public: "Where someone does an act in public, the observance and recording of that act will ordinarily not give rise to an expectation of privacy" (see Gillespie 2009).

In the European Union, whilst this type of data collection frequently takes place, it could be in contrast with ECHR case law which, in the Rotaru vs. Romania case,[32] ruled that "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities". As O'Floinn and Ormerod (2011) observe: "Non-private information can become private information depending on its retention and use. The accumulation of information is likely to result in the obtaining of private information about that person".

In the United States, this subject has been addressed in the case People v. Harris,[33] currently pending in front of the Supreme Court. On January 26, 2012, the New York County District Attorney's Office sent a subpoena to Twitter, Inc. seeking to obtain the Twitter records of user suspected of having participated in the "Occupy Wall Street" movement. Twitter refused to provide the law enforcement officers with the information requested and sought to quash the subpoena. The Criminal Court of New York confirmed the application made by the New York County District Attorney's Office, rejecting the arguments put forward by Twitter, stating that tweets are, by definition, public, and that a war-

[31] See http://www.x1discovery.com/social_discovery.html.
[32] See Rotaru v. Romania (App. no. 28341/95) (2000) 8 B.H.R.C. at [43].
[33] See 2012 NY Slip Op 22175 [36 Misc 3d 868].

rant is not required in order to compel Twitter to disclose them. The District Attorney's Office argued that the "third party disclosure" doctrine put forward for the first time in United States v. Miller was applicable.[34]

There is still a question mark surrounding this issue, but it is undoubtedly of great current ethical and legal interest.

8. Conclusion

The decision handed down by the Court of Justice of the European Union has undeniably had an indirect impact on the discussion as to how to balance an individual's fundamental human rights and the need to acquire tools to ensure their safety.

However, the enormous volume of data which is constantly posted online can only give rise to new forms of surveillance and monitoring. Therefore, in the author's opinion, the problem is not only setting out the surveillance boundaries, preventing abuse from being committed, but also tackling the problem at its root, preventing people from being prosecuted for offences that may potentially curb freedom of expression and other essential human rights.

In conclusion, out of all the various proposals for action, it should be a priority to concentrate on two specific areas.

The first one concerns the procedures for submitting a request. In fact, if all the Member States made scrutiny by a judge and not by a public prosecutor or, in certain cases, the judicial police, a necessary condition for granting access to traffic data, it would be possible to ensure that information which potentially affects the individual's fundamental human rights is considered and thus regulated in accordance with the same guarantees required in many Member States for obtaining wiretapping warrant.

The second concerns the need, at least nationally, to limit the scope of the Directive in particular with regard to defamation and privacy violation which, except in extreme cases, cannot be considered "serious crimes".

References

Bigo D., Carrera S., Hernanz N., Jeandesboz J., Parkin J., Ragazzi F. and Scherrer A. (2013), *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, Study for the European Parliament, PE 493.032, September

Brown I. (2013), *Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK*, 27 September, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336609

Celine C. and Galli F. (2013), "Comparative Law Paper on Data Retention Regulation in a Sample of EU Member States", in *Surveillance FP7 Project*

[34] See United States v. Miller (425 US 425 [1976]).

Danezis G., Dingledine R. and Mathewson N. (2003), "Mixminion: Design of a Type III Anonymous Remailer Protocol", in *IEEE Security&Privacy*

Ferguson A.G. (2012), "Predictive Policing: The Future of Reasonable Suspicion", *Emory Law Journal*, http://www.law.emory.edu/fileadmin/journals/elj/62/62.2/Ferguson.pdf

Gillespie A. (2009), "Regulation of Internet Surveillance"*, European Human Rights Law Review*, 4, pp. 552-565

Ngai E.W.T., Yong Hu, Wong Y.H., Yijun Chen and Xin Sun (2011), "The Application of Data-mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature", *Decision Support Systems*, 50, 3, pp. 559-569

O'Floinn M. and Ormerod D. (2011), "Social Networking Sites RIPA and Criminal Investigations", *Criminal Law Review*, 24, 10, pp. 766-789

Zittrain J. (2002), *Beware the Cyber Cops*, http://www.forbes.com/forbes/2002/0708/062.html