What now? Data Retention Scenarios After the ECJ Ruling

Alessandro Guarino

StudioAG
a.guarino@studioag.eu

Abstract

In its first part the paper recalls the history of data retention legislation in the European Union. The directive was born in the post 9/11 world, when fear of terrorism peaked. This is the context of the 2006 legislation and the subsequent implementations by the member states. The paper examines the directive and the rationale behind the two-years conservation of metadata. Further on the paper will examine the reasons for the directive annulment, its privacy implications and the proportionality principle.

In its second part the paper maps the consequences of the repealing. At the policy level this marks a growing concern about civil rights and a more rational view of security necessities. Commission and Parliament will have to take this into account. On the other hand the national legislations that implemented the invalid directive are still in place and possible scenarios should be examined as to their validity.

Repercussions will probably influence the data protection reform -voted by the European Parliament in first reading- and the Trade and Investment Partnership, for which negotiations are ongoing and that should regulate the data flows between EU and the USA. The new scenario will be important also for business, from the telco companies to the growing "Big data" industry, where data generated by mobile networks was to be leveraged for a lot of uses. As the major reason for the retention was criminal investigations, digital forensics will be influenced too, seen that the big datasets were a key enabler in many respects.

The position paper ends with some proposals on what can be done now to rebalance correctly the security and investigation necessities with fundamental liberties, recognising that the directive was in fact unbalanced but also that some level of retention is probably needed. On the backdrop obviously loom the 2013 NSA scandals, from which we learned that also from anonymised metadata is very easy to identify individual users.

1 Motivation

The European Court of Justice declared in early 2014 the 2006 Data Retention Directive invalid because its formulations infringe on citizens' fundamental right namely on privacy and personal data protection. With data retention we usually mean the processing and storing of detailed informations about phone calls and Internet communications – e.g. visit to web sites, emails, chat conversations... - by network operators for a predetermined time period, in order for it to be available to law enforcement and security agencies for the purpose of criminal investigations. The Directive allowed for a retention period of up to two years, for all categories of data. The declaration of invalidity opens new scenarios in the ongoing debate on the regulation of online activities for the sake of security versus the individual right to privacy. This position paper traces the mo-

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2014), 249-255

tivation and structure of the Directive, details the reasoning at the base of the ECJ's decision and proposes some policy guidelines for the future.

2 Data Retention Legislation

The European Directive on data retention (2006/24/EC of 15 March 2006) was born at the peak of the post-9/11 historical period, where terrorism was perceived as an existential threat to free societies on both sides of the Atlantic. Fear for the consequences of terrorist attacks, fuelled also by the London and Madrid bombings, at the time skewed the priorities of legislation towards security concerns, while limiting individuals' privacy was considered a small price to pay.

The rationale behind the 2006 regulation of data retention and the consequent transpositions by EU Member States lies in the extreme usefulness of the information generated in the course of operations of mobile and ICT networks for criminal investigations in general and particularly for those regarding organised crime and terrorism, where reconstructing networks of contacts and relationships is important.

The Directive of course had to comply with an already existing legislative context, in particular the Data Protection directive (95/46/EC) and the directive on data processing by network service providers of 2002 (2002/58/EC). The stated object of data protection legislation is to protect individuals from misuse of personal data. Privacy is a fundamental right recognised both by the Charter of the European Union and the U.N. Universal Declaration of Human Rights. The approach taken in the 1995 Directive is not ideologic but very pragmatic and risk-based. Controllers of personal data can assess risks and, if they so choose, accept a residual risk of misuse. Economic concerns in implementing security controls are also taken into consideration. Not all member states, when transposing the directive, followed this lead however. Italy is a blatant example of a national legislation not only extending the notion of "data subject" to legal persons -causing a myriad of problems in the process- but also totally eschewing the risk-based approach to security controls in favor of a detailed, rigid, prescriptive one. As for directive 58, from the point of view of the promoters of the data retention discipline its main shortcoming was that data on unsuccessful phone calls was outside its scope. Making a phone "ring", even if the call is not answered, is one of the ways an explosive device can be triggered, so from the standpoint of counter-terrorism, having access to this kind of information, was – and still is - considered very useful.

Technically speaking, EU Directives should be motivated by the need to remove obstacles to the realisation of the single internal market, in this case for electronic communications: this is the motivation laid down in the recital, articles 6 and 21, where the need to harmonise providers' obligations in different member states is stated. But the real reasons are also clearly explained in the text, from the mention of crime prevention, to the to the Council Declaration of 2004 on terrorism, to an explicit mention of the London attacks of 2004. There is also a justification for the long-term retention of data under the necessity principle. In general this legislation was mainly promoted as part of pan-european police cooperation.

2.1 Scope

Only what is commonly known as "metadata" – as opposed to the actual communication content – was covered in the Directive. Regulating the acquisition of communication content by investi-

gators would have meant reforming the discipline of lawful interceptions. Only traffic and location data – necessary "to identify the user" - are covered, both for telephone networks (cellular) and the Internet. These kinds of information include (both for the source and the destination of a communication):

- User ID and/or telephone number
  - if the destination number is rerouted, also the final destination;
- Name and physical address of the subscriber;
- Date and time of the beginning and end of the communication
  - beginning and end of the voice call for phone networks
  - time of log-in and log-out in the case of Internet session;
- IP address (static or dynamic) for Internet sessions;
- Terminal equipment or Internet service used;
- Data identifying equipment used:
  - IMSI and IMEI numbers of both caller and called
  - for prepaid phones: date and time of the initial activation of the service, cell ID where it was initially activated
  - for Internet access: dial-up number or xDSL endpoint;
- Cell ID at the start of the communication with its geographical location.

Each provider is mandated to only retain data generated on its own network in the course of normal operations – this is the base for declaring the data processing proportionate. Of course the text stated that data protection legislation applies and that the directive respected fundamental rights. Plainly the authors were very well aware of the controversial nature of such a wide-ranging retention of metadata. The period of retention should have been "no less than six months and not more than two years". The exact quantification was left to member states.

Each member state was mandated also to designate a supervising (independent) authority responsible for monitoring the implementation of the directive and the security controls adopted by providers. In the period of validity of the directive it does not seem these authorities were very much effective.

3 The European Court of Justice Judgment

The judgment of the European Court if Justice, dated 8 April 2014 [ECJ14], finds its origin in two cases – joined – brought to the European level by national courts in Ireland and Austria. In Ireland Digital Rights, a privacy advocacy, challenged the legality of data retention national law, based on Directive 24 (the data protection Directive). The High Court chose to refer the case to the ECJ. In Austria, the Kartner local government with a sizable number of individual citizens also challenged the national legislation transposing the 2006 directive.

3.1 The question

The European Court had to answer the question as to wether the provisions contained in the data retention Directive are contrary to the European Union Treaty, in other words if they are necessary and proportionate to achieve its stated objectives: ensuring the proper functioning of the internal market and that certain data be available for the purposes of criminal investigation.

More specifically, in terms of the Charter of Fundamental Rights of the European Union – which is an integral part of the EU Treaties, what the Court had to decide was if the Directive was in contrast with the rights to privacy (laid down in Article 7), and to the protection of personal data (Article 8), as well as the right to freedom of expression (Article 11). Also in question was the compatibility of data retention discipline with the right to move and reside freely inside the Union and the right to a good administration.

3.2 Interference with fundamental rights

The Court reasoning starts with assessing the relevance of Articles 7,8 and 11 of the Charter as to the validity of the directive. As we will see, this will be more than enough to reach a decision.

The Court judgment states a very important fact, grounded on legal reasoning, that until then was mainly maintained by privacy advocates and the information security community: metadata processing, when done on a massive scale, is enough to infringe on individuals' personal lives and privacy, even possibly limiting their right to freedom of expression. Huge datasets containing all the information on communications listed above allow the analyst very precise profiling of the behaviour of individuals, up to conclusions about their personal life. Also it should be noted that data retained under the Directive's provisions are not anonymous or anonymised in any way, unlike in the bulk metadata collection allegedly carried out by the NSA in the United States.

As for interference with the rights to privacy and data protection, it does not matter if the information retained is sensitive or not – the Court explains – or even if the person concerned is actually inconvenienced in any way to configure an infringement on those rights. The obligation to retain data (Art. 3 of the Directive) and the stated periods of retention (Article 6) were therefore by themselves an interference with the right to privacy. Furthermore also the allowed access by national authorities by itself is an interference on the rights to data protection because it allows for processing of personal data.

The factual conclusion is that the interference on fundamental rights allowed by the Directive are so wide ranging as to generate a feeling that personal lives are constantly under surveillance. The main reason for this is that data is retained and subsequently used without the persons concerned being informed in any way.

3.3 Justifications provided

The Fundamental Charter states the conditions under which a right it protects and considers fundamental can be limited: any limitation must be provided by law, necessary to meet objectives of general interest recognised by the EU (or the rights of others) and proportionate to said objectives.

Data retention is clearly mandated by law, so that criterion is clearly satisfied. The Court also states that data retention *per se* – while a "particularly serious interference" - does not affect the rights to privacy and data protection, if only metadata is processed and appropriate security measures are mandated and implemented.

The object stated is of course of general interest: to contribute to the fight against serious crime, in particular organised crime, and ultimately to public security – which is also a fundamental

right protected by the Charter. Also the fight against terrorism has ultimately the objective of protecting international peace and security. Both are clearly of general interest and the means are appropriate, given the ubiquity of electronic communications.

3.4 Necessity and Proportionality

Under these premises, the question of the proportionality of the detailed provisions for retention remains to be examined, because under European law the legislature discretion is limited when fundamental rights are involved. In this case the law exceeded what was necessary to reach the stated objective and the Court goes on to list in which ways:

- Directive 24 goes beyond necessity because the scope of retention envisioned "involves practically the entire EU population without any discrimination". No differentiation, limitation or exception were detailed in the text.
- No relation was requested between the retained data and a specific threat to security, for instance a date or time interval, a geographic zone or specific group of (suspected) users. To all intent and purposes it was dragnet surveillance.
- No limitations to data access by national authorities were specified, and no objective criteria by which access could be limited to a strictly necessary number of persons. Moreover access was not dependant on a ruling by a Court of Law or an independent administrative body.
- The minimum retention period of six months, without distinction with regard to categories of data or usefulness for investigations was deemed to be excessive.
- The maximum period was fixed at two years but without objective criteria for determining the exact within the allowed range.

To summarise, no clear defined rules were governing the extent of the interference with fundamental rights protected in the Charter (privacy and data protection). In the Court's words, a "Wide ranging and particularly serious interference with these fundamental rights" was allowed without it being precisely limited or circumscribed.

Also, regarding in particular data protection, no clear safeguards for the protection of retained information by the providers were specified. This point is important, especially because of the vast quantity of data involved, their sensitive nature and the high risk of unlawful access to them.

The conclusion of the Court was that the Directive "*[...] has exceeded the limits imposed by compliance with the principle of proportionality [...]*" and is declared invalid.

4 The Consequences of the Decision

At policy level, the ruling marks a growing concern in the European Union for civil rights and privacy. This decision may be seen as a step towards a more balanced and rational view of what is needed to ensure adequate security levels to European citizens, both in cyberspace and the real world. Maybe we can finally acknowledge that terrorism is not the number one strategic threat to Europe, and the Atlantic community as a whole, anymore, after the frantic decade following the 9/11 attacks. Both the EU co-legislative actors (the Commission and the Parliament) will have to take this into account. On the other hand the national legislations that implemented the invalid directive are still in place and possible scenarios should be examined as to their validity. Looking at the cooperation between the Union and the United States, this could be a first sign of a

"divorce" between Europe and America on the security vs. privacy debate, also considering that it comes right after the 2013 NSA scandal. It will probably also mark a distance between continental Europe and the UK, whose priorities are historically closer to the United States.

The national legislation that transposed the data retention Directive maintain their validity and will be in force until challenged in court. This already happened in Austria (one of the two originating countries for the cases referred to the ECJ) where the relevant national law was repealed. On the other side of the spectrum we have controversial efforts like the so-called "DRIP" bill in the UK that at a first analysis seems to allow for even stricter surveillance, including content and not only context. Right now, each member state retains its own data retention law and there is a clear danger of a "balkanised" european market.

For the telecommunications and network operators, nothing changes on the very short term, but until a new European framework is developed, they will have to monitor individual members' possible changes in the law and comply.

Metadata from telephone and the Internet has become of course a valuable tool both for criminal investigations and intelligence. So much so that the field of digital forensics has very well moved from analysis of single pieces of evidence to a Big Data effort[Guar13]. The analysis of huge datasets including time, location and equipment used (metadata) is a key enabler in the study of complex social networks, be them a transnational criminal organisation or a terrorist network made up of semi-independent cells. Social Network Analysis[Masy14] allows the investigator – among other results – to single out of a complex network the key players, the leaders and the facilitators, the communities that network fragment on, its geographical extent. It's possible even from anonymised data to profile single persons and study anomalies in their behaviour online. This is already controversial – as the 2013 revelations on metadata storing inside the U.S. has shown – but much more in the European case, where the metadata retained was not anonymised at all but included name, userID and physical address of subscribers and users. Working in a more targeted way, with judicial supervision, will probably render investigations a little less effective (if at all) but less intrusive on fundamental rights.

5 Conclusions and policy proposals

What is the path to follow to reach a needed rebalancing between the two fundamental rights of privacy and security – and avoid fragmenting the EU market?

A new Directive is needed, which should take into consideration the observations of the Court. Data retention as a concept is not going to go away, but better privacy provisions will need to be included:

- A shorter maximum retention period;
- Accountable procedures for accessing the data;
- Retention limitations (temporal, geographical or regarding persons targeted) to be supervised by a Court or a pan-European Independent Authority;
- Provisions for "right to be forgotten" to be implemented by simple request – if the person concerned is not subject to investigations.

In any case it would be advisable that the new Directive be the result of a wide multi-stakeholder consultation, to be conducted in an inclusive environment, not limited to the context of securi-

ty agencies and police cooperation. Many forums exist, technical and otherwise, where such a process could be in part conducted, for instance the CEN-CENELEC-ETSI Cyber Security Coordination Group [CSCG14] and the Multi Stakeholder Platform for ICT Standardisation. Data Retention should be in any case part of a general Cyber Security strategy that includes security and privacy concerns of the individual European citizens.

References

[CSCG14] CEN-CENELEC-ETSI Cyber Security Coordination Group: "Recommendations for a Strategy on European Cyber Security Standardisation", 2014 (http://www.cscg.focusict.de)

[ECJ14] European Court of Justice: "Judgment of the Court of 8 April 2014 in joined cases C-293/12 and C-594/12"

[EU06] "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 provisions of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC". In: "Official Journal of the European Union" 13.4.2006

[Guar13] Guarino, Alessandro: "Digital Forensics as a Big Data Challenge". In: "ISSE 2013 Securing Electronic Business Processes", Springer, 2013, p. 197-203.

[Masy14] Masys, Anthony (ed.): "Networks and Network Analysis for Defence and Security (Lecture Notes in Social Networks)", Springer, 2014.