Council of the European Union

Brussels, 7 March 2017
(OR. en)

6726/1/17
REV 1

LIMITE

JAI 175
COPEN 60
DAPIX 66
ENFOPOL 91
CYBER 25
EUROJUST 36

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Retention of electronic communication data

Further to the request of the Presidency at the meeting of the Working Party on General Matters and Evaluatons of 3 February 2017 concerning the item on retention of electronic communication data, delegations will find in the annexes to this note a compilation of the contributions provided by the Member States and Europol, as follows:

Annex I - Belgium
Annex II - Czech Republic
Annex III - Germany
Annex IV - Hungary
Annex V - Ireland
Annex VI - Portugal
Annex VII - Sweden
Annex VIII - Slovenia
Annex IX - Europol

ANNEX I

BELGIUM

Given the importance of access to electronic data in the course of criminal investigations, Belgium is of the opinion that the consideration of the impact of the recent ruling of the Court of Justice in the télé2 case should remain, as a matter of priority, on the political agenda of the European Union. At the same time, experts meeting should be organized as soon as possible in order to exchange views on possible ways forward.

Please find hereafter a summary of the current situation in Belgium:

Data retention in Belgium: general framework

The Belgian data retention legal framework has been recently amended by the Law of 29 May 2016 regarding the retention of data in the sector of electric communications. The Law was published in the "Moniteur Belge" on the 18th of July 2016, and you will find a link to the full text below.

To facilitate the reading of the provisions included in this Law, please also find references to the Belgian legislation regarding electronic communications, the Code of Criminal Proceedings, and the Intelligence Offices.

Main reasoning behind the 2016 legislation

The general objective of the new Law was to respond to the annulment of the previous Law of on data retention of 30 July 2013 by the Belgian Constitutional Court. The judgment of the Constitutional Court followed the arguments given by the European Court of Justice in its Digital Rights Ireland decision by which the European Data Retention Directive was declared to be invalid.

The Belgian government is aware of the fact that it is beyond doubt that a general data retention obligation is a significant limitation of the privacy of the persons subjected to this retention, and that important safeguards and conditions are absolutely necessary, both for the secure retention of the data and the access to the data. Therefore it is important to emphasize that, even if the new data retention Law concerns all citizens, the access and the use of their data will be strictly limited to a concrete criminal case, or an inquiry intended to obtain intelligence (in the case of the Intelligence Services). Access will only be granted after a judicial authority (in criminal proceedings) or an independent Commission (in intelligence cases) has authorized this access, taking into account the several conditions and safeguards that relate to these particular cases.

During the preparations of the new Law, the Belgian authorities have given due attention to the arguments of both the Belgian Constitutional Court and the European Court of Justice. Both Courts have concluded that a general data retention obligation is a violation of the proportionality principle. This violation is, according to the Courts, the consequence of a combination of 4 elements:

- The fact that the retention concerns all citizens;
- The absence of differentiation on the basis of the categories of data and their utility;
- The absence or the inadequacy of the rules regarding access to the data;
- The absence of rules regarding the secure retention of the data.

All of those four elements have been thoroughly examined during the preparations of the 2016 Law, and this examination has led to the following conclusions.

First of all, as far as the data retention obligation itself is concerned, we have come to the conclusion that a differentiated approach on the basis of a group of persons, a certain period, or a geographically limited zone is not feasible. This conclusion was confirmed by the Belgian Privacy Commission (DPA).

a) A limitation of the retention to persons who are already subject to a criminal investigation is meaningless, as this possibility already exists. Judicial authorities have the possibility to request traffic data and thus oblige service providers to retain these data for the future. The aim of the data retention is rather to guarantee that certain data remain available for a certain period in the past.

b) A differentiation on the basis of certain periods or limited geographical zones, or a certain group of people is not conceivable. A certain time period is not coherent with a lot of situations and types of serious crime for which data retention is of the most importance (e.g. child pornography). A limitation to a certain geographical zone or a certain group of persons would amount to discriminatory profiling.

Secondly, it is not stated in the decisions of the Constitutional Court and the European Court of Justice that the violation of one of the four elements described above is sufficient to conclude that the proportionality principle has been violated.

Therefore, the three other elements that were summed up by both Courts have been fully implemented.

- The new Law has introduced a differentiation on the ground of three categories of data: subscriber data, connection and localization data, and traffic data.
- A reinforcement of the safeguards and conditions for the access to the data was introduced. A differentiation was also introduced on the basis of the seriousness of the crime: even if the retention period is 12 months, for less serious crimes the data will not be accessible for this whole period. Such a differentiation has been introduced for access to the three categories of data described above.
- The new law has also reinforced the measures that should be taken by service providers to secure the data and the access to those data.

For more detailed clarifications on the content of the new Belgian data retention legislation, we can refer to the “exposé des motifs” that was published on the website of Parliament: http://www.dekamer.be/FLWB/PDF/54/1567/54K1567001.pdf.

Update of the situation

Following the decision of the European Court of Justice in the case Tele2, four claims for annulment of the new Belgian legislation have been introduced before the Constitutional Court.

The Belgian Government is currently scrutinizing the possible implications of the interpretation of the Court of Justice in Tele2 case on this legal framework. The arrest of the Belgian Constitutional Court is not expected before the end of the year.

The Belgian data retention legal framework has been recently amended by the « *loi du 29 mai 2016 relative aux communications électroniques" :*
http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2016052903&table_name=loi

To facilitate the reading of those provisions, please also find references to Belgian legislations that have been modified by the law of 2016:

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi

(loi du 13 juin 2005 relative aux communications électroniques) – **See Articles 126 and following + 145**

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808111730&table_name=loi

(Code d'instruction criminelle – articles 8 à 136quater) – **See Articles 46bis, 88bis and 90decies**

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1998113032&table_name=loi

(loi du 30 novembre 1998 sur les services de renseignement et de sécurité) – **See Articles 13, 18/3, 18/8.**

ANNEX II

CZECH REPUBLIC

According to the Czech law, an act on electronic communications clearly state authorities entitled to request the respective data (it should be police, intelligence services and Czech national bank); the period for storage of the respective data (basically, the categories of data that have been required by the former data retention directive 2006/24/ES) is six months; and finally data protection rules as clearly set in the data protection act shall be also applicable on this special act. According to Section 88a of the Criminal Procedure Code the respective data may be used only for investigations of a crime with a minimum sentence of three years, a intentional crime punishable according to the international treaty and exhaustive list of crimes which are usually committed with the use of mobile or internet (such as stalking). Courts (judge during investigation or chair of senate during trial) approval is necessary to obtain the data. Moreover it should be obligatory to give back information that the data has been obtained in the cases, where the person is known. Data keeping according to the directive are mainly key information in prosecution. In number of cases is the information about mobile number present at the scene of crime the only information that could lead to the person connected to the crime.

Right now we are waiting for the analysis of the EC as was mentioned at last GENVAL meeting. We are analysing the judgement but we do not have any clear solution how to ensure targeted retention. In other points, we are following the court's decision. Data retention is important for law enforcement because under strict conditions and for certain serious crimes it is possible to gain the data from the past. It is important that police is limited in access to the data; there is no push method to some storage. Police can obtain data only under strict conditions and after approval of the court. We were of the opinion that this should protect the privacy as well as help police to investigate. There is no list with phone numbers; one person can use many SIM cards and phones with different IMEI. Therefore from the technical point of view it is not easy to retain data just about persons convicted of a serious crime. It is even more difficult with the internet. Discussion about categories of data can be held; also data retained by the companies for their own purposes can be used for investigation; however the scope of retained data is not the same.

Data retention is also quite technical issue, so also technical experts should participate at the discussion.

ANNEX III

GERMANY

We are grateful for the opportunity to provide our comments to last sessions' topic "retention of electronic communication data". Two approaches on how to respond to the ECJ's judgment have been discussed during the meeting (and within the discussion paper distributed by the presidency).

1. Technical measures (discussion paper, question 1)

With regard to technical measures, it has to be noted that Germany has introduced new provisions on data retention in December 2015. The obligation to retain certain data will not enter into effect before July 2017. This means that at this point of time, there is no mandatory retention of data and access for law enforcement agencies is only available regarding data stored by providers for business purposes.

2. Legislative measures (discussion paper, question 2)

The new provisions on data retention in Germany have been formed on the basis of the requirements formulated by the Court within its Digital Rights decision in 2014. The Analysis of the new Tele2 judgment and its potential implications for Germany is still ongoing. KOM announced to provide guidance on the conditions national legislation has to fulfill in order to comply with the judgment which seems to be a reasonable next step on the EU-level. Germany strongly appreciates the Commission's efforts. Whether a harmonized approach seems to be favorable should be considered once the analysis of the judgment has proceeded further.

ANNEX IV

HUNGARY

Article 11 of the proposal for a new e-privacy Regulation could be an adequate response to the judgement of the Court at EU level. The wording of Article 11 is general enough to leave room for Member States to find various solutions in their national legislation, while it reflects properly on the requirements set out in the judgement. However, even on this basis, the challenge remains for national legislations to develop an effective and operative legal model consistent with the guarantees required by the judgement at the same time. There is a need for launching a more detailed guidance to Member States at EU level. Hungary is willing to contribute as soon as we have the outcomes of the evaluation of the Hungarian legislation against the judgement and our proposals for the possible national legal solutions.

ANNEX V

IRELAND

Retention of electronic communications data

It is incumbent on any police service to establish the truth in the context of a criminal investigation by bringing the best evidence before the courts so that all victims and suspects receive justice, and all citizens are protected from becoming victims of crime.

Having available to investigators if needed, under the appropriate conditions, all relevant electronic communications data relating to suspects, offenders, victims, and witnesses before, during, and after the commission of a crime, can be a key assistance to any police service in initiating successful strategies for the prevention, investigation, detection and prosecution of crime. Of necessity the conduct and course of an investigation always takes time, and depends on the specific circumstances surrounding the receipt of each piece of information and intelligence received. It cannot, therefore, readily be predicted in advance whose or what data will be required. The greater the restrictions upon the dataset that can be accessed, the greater the potential information deficit for investigators.

The fundamental rights of both victims and suspects to justice and fair procedures when engaging with the criminal justice system requires a properly balanced approach to be taken to privacy rights in the context of the long-term retention of electronic communications data. Evidence that could prove the guilt or innocence of a suspect could be lost to the criminal justice system.

A harmonised, co-ordinated approach by all the Member States could yield better results when considering the best EU legislation to have in place, balancing all citizens' rights to privacy, justice, proportionality and fair procedures when engaging with the EU's criminal justice systems.

When seen against Ireland's current model for regulating access to retained communications data for law enforcement services, the implications of the CJEU judgement in the *Tele 2* case have the clear potential to seriously hamper the investigation of serious crime and protection against security threats.

ANNEX VI

PORTUGAL

Following the discussions at the GENVAL meeting of 3 February 2017 on the "retention of electronic communication data", and after your request of 6 February, please find below our contribution to the questions raised by the Presidency, as already answered by H.E. the Minister of Justice of Portugal at the JHA Informal Council last January.

- The Portuguese legislation on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks complies with the case law of the Court of Justice of the European Union. In this respect any change in the domestic legal framework seems to be needed.
- Legislative amendments are not envisaged, since the legislation in force respects the case law of the Court of Justice, requiring that the retention and transmission of data can only take place for the exclusive purpose of investigating, detecting and prosecuting serious crimes and always requiring the intervention of the Investigating Judge, safeguarding the rights to data protection and to privacy enshrined in the Constitution of the Portuguese Republic.
- Portugal consider that a harmonized approach on data retention at European level is needed in order to avoid negative impacts on the effectiveness of criminal investigations and prosecutions, in particular as regards the validity and admissibility of evidence in court and in the field of judicial cooperation in cross-border cases of serious crime and terrorism.

ANNEX VII

SWEDEN

As a complement to the comments already made at the GENVAL working party on 3 Feb, SE would like to add the following. SE is positive to continue working at informal level. To start with, the Presidency should convene a meeting with a view to discuss a strategy to remedy the situation in the short-term as well as in the longer-term. With regard to the future Regulation on ePrivacy, this is clearly one piece of a solution. However, in the longer-term, further work is required in the EU law enforcement context, for instance by making the issue of proportionality a subject matter for the political level and in connection with preparing possible new cases before the Court.

ANNEX VIII

SLOVENIA

Following the discussion at the Genval meeting on 3 February 2017 on the "retention of electronic communication data", we are sending our contribution regarding two questions:

3. Considering the importance of access to electronic data for criminal law enforcement authorities, what technical measures do Member States envisage in order to enable access while complying with this Court judgment?

Shortly following CJEU's invalidation of the data retention directive back in May of 2014 (the C-293/12 Digital Rights Ireland judgment), the Slovenian Constitutional Court (CC) annulled the national implementing provisions in Chapter 13 of the domestic Electronic Communications Act (decision Nr. U-I-65/13-19 of July the 3rd 2014).

With the said decision of the CC the national providers of publicly available electronic communications services or public communications networks were no longer required to retain traffic and location data belonging to individuals or legal entities. Their existing data retention databases were to be immediately deleted.

Consequently, the police were no longer able to rely on the said (14- or 8-month long database, for phone and internet data respectively). Instead, they had to rely on what the operators themselves kept for billing and similar purposes (subject to Article 6 of the ePrivacy directive, and to Articles 151 etc. of the national Electronic Communications Act). For phone usage data, that amounted to approximately 3-4 months of data with both major national providers, while internet usage data varied from operator to operator. That being said, the police was able to keep existing technical arrangements in place, and was able to keep receiving phone traffic data thought existing secure channels. The legal basis for requesting the data (Article 149.b of the Criminal Procedure Act) was unaffected by the CC judgment.

There has since been an ongoing discussion as to whether data retention should be reintroduced into the Electronic Communications Act. However, the wording of the CC decision was rather strict on the fact that mandatory and indiscriminate data retention (might) be prima facie unconstitutional, so we decided to be rather careful regarding this.

That being said, the aforementioned loss of older phone data and consistent internet data has led the Ministries of Interior and Justice to work on preparing a draft amendment to the Criminal Procedure Act, to better help secure electronic evidence. The draft law is still in the legislative process and subject to change.

The draft amendment will provide for a comprehensive and differentiated legal basis for various types of investigative measures in order to obtain data on electronic communication of suspects.

According to draft law, investigative judge will be able to order the telephone/internet provider to deliver existing data on suspect's communication based on the state prosecutor's proposal supported by grounds. Furthermore the draft amendment provides for legal basis for investigative judge to order the telephone/internet provider to secure (freeze) data on suspect's communication. Request supported by grounds can is lodged by state prosecutor. This measure will be able to last up to 3 months.

Finally, draft amendment provides for legal basis for the court, police or state prosecutors to request the telephone/internet providers to hand over data on their users/subscribers who are suspects in serious offences or the data on the existence on their contract with the provider.

All these evidence gathering measures are subject to judicial review and time limitations while the request has to be specified and limited to the specific data and suspects in line with the above mentioned decision of the CC and also in line with TELE2 decision.

4. In terms of legislation, are Member States considering amending their respective national legislations? Should a harmonized approach be considered?

According to the present situation at the time, we are not considering amending our respective national legislation (Electronic Communications Act.). In principle we support harmonised approach, however the regulation shouldn't interfere excessively in the voluntary retention of data retention. In fact we think that excessive control shouldn't be in a direction of ever grater unification, this should principally the responsibility of the Member States themselves.

ANNEX IX

EUROPOL

Retention of electronic communication data:
Problem statement
Europol's contribution to the GENVAL discussion of 3 February 2017

- Law enforcement and judicial authorities face enormous challenges in investigating online criminal activities in the absence of a harmonised legal framework regulating the retention of relevant data. Operational experience strongly argues in favour of such a framework at EU level.

- The data retention related rulings by the European Court of Justice (ECJ) explicitly recognised data retention as a legitimate tool for the prevention and combatting of serious crime and terrorism provided the necessary safeguards are implemented.

The overturning of the Data Retention Directive by the European Court of Justice (ECJ) in its ruling of 8 April 2014 in Digital Rights Ireland [1] has created a scattered legal landscape for law enforcement and prosecutors to obtain relevant data from private parties. The annulment of the Data Retention Directive as such had no immediate effect on the national implementing legal acts. Therefore, in some Member States (MS), there is currently still legislation in place to ensure that telecommunication companies retain such data for law enforcement purposes, whereas in others, the national legislation has been annulled in the wake of the ECJ judgement.

However, it is important to note that the ECJ in its Digital Rights Ireland ruling clearly acknowledged that "(…) the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest. (…) Article 6 of the Charter lays down the right of any person not only to liberty, but also to security. (...) It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data (…) genuinely satisfies an objective of general interest."

Also in 2010 the ECJ ruled that the right to data protection is "(…) not an absolute right, but must be interpreted in relation to its functioning in society".[2]

1 ECLI:EU:C:2014:238 (case C-293/12)
2 ECLI:EU:C:2010:662(case C-92/09 and C-93/09)

Similarly, in its Tele2 Sverige and Watson ruling of 21 December 2016[3] the Court did not go so far as to deem data retention per se unlawful. In interpreting Article 15(1) of the e-privacy Directive the Court highlighted that a MS is not prevented from introducing legislation that would facilitate targeted retention of traffic and location data for the preventive purpose of fighting serious crime. It is also very important to acknowledge that the use of retained communications data may help to clear persons suspected of serious crimes without resorting to other more intrusive means of surveillance such as interception of communications or house searches.

The discrepancies in the legal provisions in MS impede the work of the competent authorities resulting in a loss of investigative leads and ultimately affect the ability to effectively prosecute criminal activity online. Importantly, not only typical cyber investigations are affected: whereas a decade ago, the majority of criminal cases did not have a digital component, nowadays, the situation has changed entirely as almost any criminal activity and act of terrorism has a digital footprint considering the related communication, financing aspects and logistics.

Today, IP addresses often are the starting point of an investigation. Such cases cannot necessarily be solved through “classic police work” or investing more resources. The current situation creates unjust pressure on the investigating authorities to prioritise their activities in accordance with the different data retention frameworks currently in place, rather than focusing on high-value targets.

Those challenges, for instance, concern law enforcement operations targeting online environments extensively exploited for criminal purposes. This could be offences related to child sexual exploitation online, terrorism and the illicit trade of goods and services online, including illegal weapons, drugs or any other commodities related to serious crime or terrorism. This data needs to be analysed, for instance, in order to attribute specific IP addresses to suspected online criminal activities. Moreover, the prioritisation of targets may require a detailed analysis. Taking into account the large volume of data and the technical challenges related to this type of investigations, all of this requires a considerable amount of time and effort which means that by the time Internet Service Providers (ISPs) can be presented with a preservation order, in too many cases the relevant data and potential evidence are no longer available.

[3] ECLI:EU:C:2016:970 (case C-203/15 and C-698/15)

Further complexity is introduced by the fact that IP addresses are often not enough to attribute criminal activity to an individual. The widespread use of Carrier-Grade Network Address Translation (CGN) technologies increases the problem of non-attribution of crime. They allow ISPs to share one single IP address among up to several thousand subscribers at the same time.

The law enforcement community is alarmed by the widespread and growing use of CGN technologies by ISPs. A recent study showed that in 2016, 90% of mobile internet network operators (GSM providers) and 38% of fixed line internet access providers (cable, fibre and ADSL) are using CGN technologies, while 12% are planning to deploy it in the coming months.[4] A study conducted by Europol in the summer of 2016 showed that the scale of the online crime-attribution problems stemming from the use of CGN is significant. 80% of the European cybercrime investigators surveyed had encountered problems in their investigations relating to the use of CGN, causing them to be either delayed or stopped. These cases concern investigations of serious offences, such as online child sexual exploitation, arms trafficking and terrorist propaganda.

This underlines, from an overall perspective, the operational need for a harmonised framework on the retention of electronic communication data.

---

[4] http://www.icir.org/christian/publications/2016-imc-cgnat.pdf, accessed on 20/02/2017.