Council of the European Union
General Secretariat

Brussels, 04 April 2017

WK 3570/2017 INIT

LIMITE

JAI
COPEN
DAPIX
ENFOPOL
CYBER

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	DAPIX (Friends of the Presidency - Data Retention)
Subject:	Europol Study on the data retention regime applying in the EU Member States

Delegations will find attached in the Annex a Study on the data retention regime applying in the EU Member States carried out by Europol, on the initiative of its Data Protection Office. The project was initiated in light of the Judgment of the Court of Justice of the EU of 8 April 2014 Digital rights invalidating the Directive 2006/24/EC.

The Hague, 22/08/2016

EDOC#848769v1

DPO Study on the Data Retention Regime applying in the EU Member States

Contents

1. Introduction

This report is the result of specific and structured research carried out by Europol, on the initiative of its Data Protection Office, regarding the Data Retention regime currently being applied in the Member States of the European Union. The project was initiated in light of the ruling of the European Court of Justice (ECJ)[1] in April 2014 invalidating the Directive 2006/24/EC (DRD), i.e. the European legal framework providing rules and obligations on the retention of non-content data by telecommunications providers. The comparative study hereby undertaken will take into consideration the following sources:

- Europol's survey of the data retention regime being applied in the EU Member States[2]. The survey was carried out with the assistance of participating **Europol National Units** (ENUs) and **Europol Liaison Bureaux**. It built on **feedback** received by national law enforcement and intelligence agencies, answering a **questionnaire** which had been developed for this specific purpose. The present study primarily relies on the information provided by the responding ENUs from the following 20 Member States: Austria, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Germany, Finland, Greece, Hungary, Italy, Lithuania, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

- **Eurojust's analysis** of EU Member States' legal framework and current challenges on data retention[3], a parallel survey on data retention presented in October 2015. Both studies complement each other by reflecting the diverging competences of both agencies.

2. The Data Retention Directive

The DRD was adopted in March 2006 after the London and Madrid bombings to help fight crime and terrorism. Its aim was to harmonise Member States' provisions concerning the obligations of electronic communication providers to retain certain data generated or processed by them (**traffic** and **location** data) in order to ensure that such data are available for the purpose of the investigation, detection and prosecution of serious crime.

The data necessary to identify the subscriber or user had to be retained for a period of no less than **six months** up to a maximum of **two years**. The DRD did not permit the retention of the content of the communication or of information consulted.

It allowed law enforcement to access this data for the purpose of combating **serious crime**. However, the retained traffic data can only be provided to **competent authorities** in specific cases and in accordance with national law.

3. Declaration of invalidity by the ECJ

On the 8th April 2014, the ECJ declared the DRD invalid as it entailed a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary.

It is interesting to note that the ECJ 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

[1] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others

[2] Europol, Data Protection Office. EDOC#791813 (*Study on the Data Retention Regime Applied in the EU Member States*).

[3] Eurojust, 13085/15. (*Eurojust's analysis of EU Member States' Legal Framework and Current Challenges on Data Retention*). Presented on October 26th, 2015.

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."

However, the ECJ was of the opinion that, by adopting the Directive as it stood at that point, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality. Other prominent quotes from the ruling specifically elaborating on data protection and privacy implications include the following:

- "(…) the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"[4].

- "It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications, according to rules of national law, to the obligation of professional secrecy."[5]

- "Moreover, whilst seeking to contribute to the fight against serious crime. Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences".[6]

- "(…) Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued".[7]

[4] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para.37
[5] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para.58
[6] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para.59
[7] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para.62

4. Situation in Member States

A declaration of invalidity does not annul the act in question but means that the DRD is no longer applicable and that this judgment has retroactive effect. National courts cannot continue to apply the directive that is declared invalid. Any other judge or court will have to consider the directive invalid in any other decision. However, it is important to understand that national acts for transposing the directive do not automatically become annulled. They are not directly affected by the judgment and it is up to the national courts concerned to rule themselves on the validity of these national acts. They may maintain, repeal or amend the national law adopted in accordance with the DRD. If maintained, national judges will have to assess whether or not fundamental rights are respected.

The public debate on privacy implications of the DRD, which in fact started even before the legal framework entered into force in 2006, was clearly reinforced by the ECJ ruling in 2014. Citizens and interest groups in many Member States subsequently tackled data retention laws at the national level with the argument that the very basis of these laws, the DRD, was now invalid.

The survey carried out by Europol revealed that in at least **7 Member States** (AT, BG, DE, NL, PL, SI, SK), **valid legislation** on data retention no longer exists. On the other hand, amongst those countries where data retention obligations are **still in force**, at least **3 Member States** (ES, FI, HU), had already examined their legislation or are currently under review of such provisions.

At the same time, the participating Member States unanimously confirm that data retention has a **positive impact** on the prevention, investigation and prosecution of serious crimes and terrorism[8]. However, these types of data are rarely direct evidence of involvement in criminal activities but help to direct the investigation (including the exclusion of individuals for further investigation), check alibis, identify contacts and possible co-conspirators.

Particularly in cases of sexual exploitation of children and grooming[9], murders[10], terrorism[11] or cyber-attacks, participants emphasised the reliance on retained data in order to discern and corroborate other forms of evidence, link suspects to victims or identify the location of a missing person. In the absence of forensic or eye witness evidence, retained data is often the only available tool to initiate an investigation. Additionally, data retention enables the construction of trails of evidence leading up to an offence, as well as supporting the judicial authority in the decision making process.

A number of issues raised in the ECJ ruling deserve closer attention as they have direct implications from a law enforcement perspective.

4.1. Lack of a definition of serious crime

The ECJ found that the DRD ”fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to

[8] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para. 49.

[9] See the case of grooming in Rochdale (UK), which led to several convictions in the context of the “Operation Doublet”, regarding serious sexual abuses taking place between 2005 and 2013.

[10] See the “Soham Murders” case, regarding the homicide of Holly Marie Wells and Jessica Aimee Chapman, two 10-years-old girls killed in August 2002 in the Cambridgeshire

[11] See the Glasgow Airport attacks in 2007

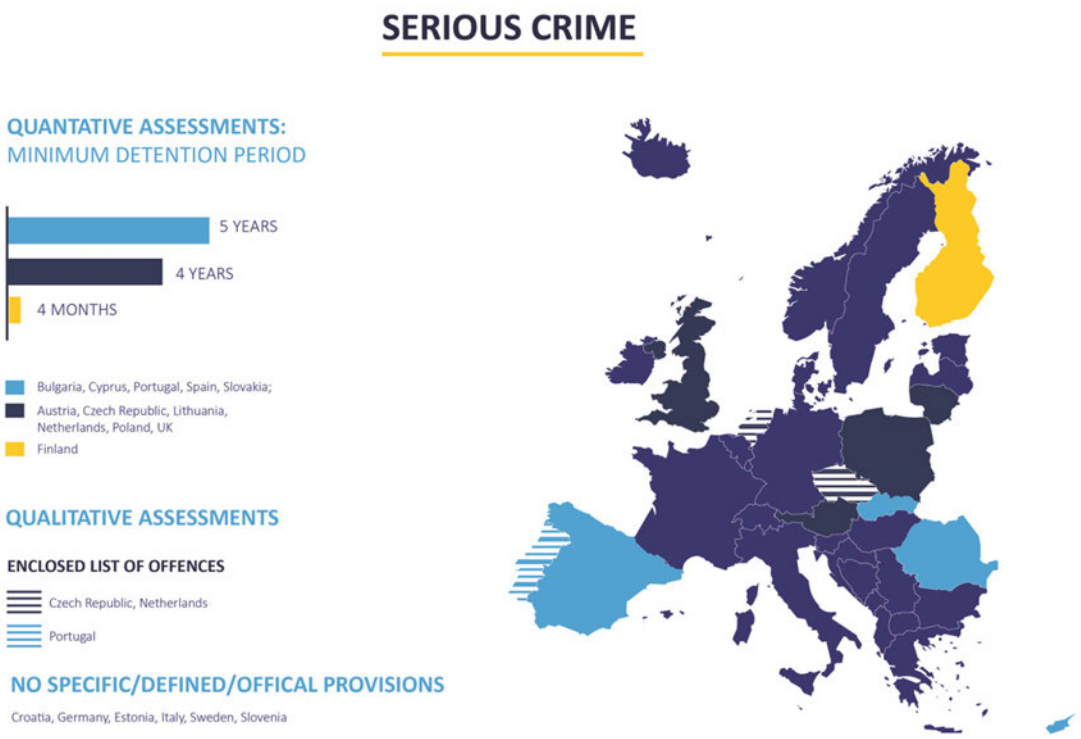
be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law"[12].

The lack of a specific definition of serious crime within the Directive led to a fragmented panorama amongst the participating Member States, as confirmed by the findings of the present survey.

In the majority of Member States, the definition relies on a **quantitative assessment** of the minimum detention period. Specifically, this threshold refers to **five years** of minimum detention period in at least **4 Member States** (BG, CY, ES, PT, SK), and to **four years** for at least **6 Member States** (AT, CZ, LT, NL, PL, UK).

Furthermore, the study revealed that in at least **3 Member States** (CZ, NL, PT), the legislation additionally elaborates on a **qualitative assessment** of serious crimes (i.e., on the characteristics and the typologies of crimes). Specifically, this legislative technique establishes an enclosed list of felonies in which each criminal code considers whether the offence qualifies as a serious crime. However, the analysis of these articles reveals that such lists are not harmonized amongst the aforementioned Member States.

The graphic below highlights the current situation amongst the participating Member States on the definition of serious crime as enshrined by national legislations.



[12] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para. 60.

4.2. Data retention period

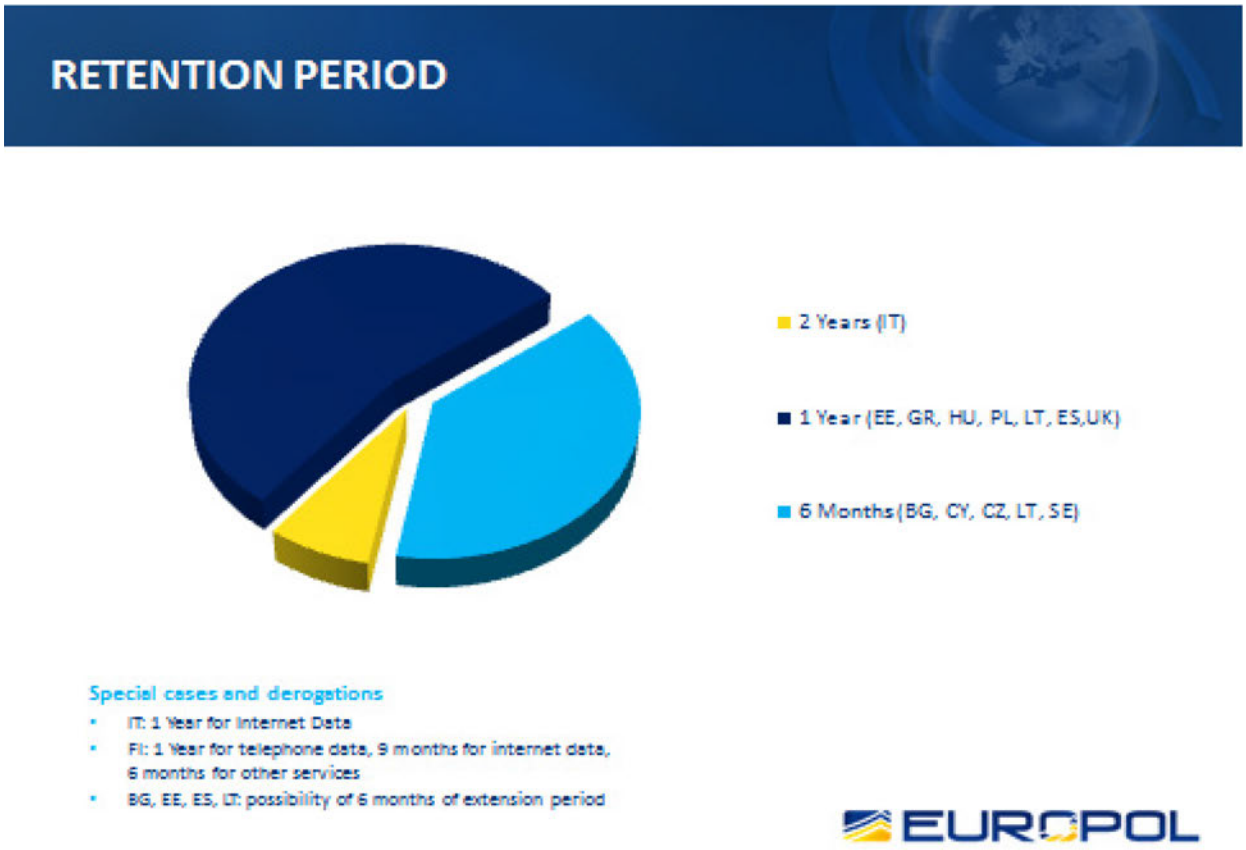
When it comes to the exact length of time for the retaining of data, the DRD set a framework of between 6 and 24 months. In this regard, the ECJ found that "Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned"[13].

Bearing this in mind, the provisions set forth by Art. 6 of the Directive led to a variety of transpositions within the Member States. As confirmed by the present study (see infographic below), the maximum retention period[14] within each national legislation is prescribed for one year in at least **7 Member States** (EE, GR, HU, PL, LT, ES, UK), or six months in at least **5 countries** (BG, CY, CZ, LT, SE). Residually, the maximum retention period allowed by the Directive (**two years**) is prescribed by **one Member State** (Italy).

However, the analysis carried out revealed that some national legislation distinguishes between different retention periods depending on the type of service provided. Specifically:

- Italy (IT) makes a distinction between **fixed telephony** and **mobile telephony** data (**two years**), **internet access**, **internet telephony** and **internet email** (**one year**). Furthermore, the retention period for unsuccessful telephone calls[15] is **one month**, while the prescribed maximum time is **six months** for **invoicing** or **administrative purposes**;
- Finland (FI) differentiates periods of retention according to the typology of the service therein: **telephone service** or **SMS service** (**one year**), **internet access** service (**nine months**), **Internet telephone** service (**six months**).
- In Spain (ES), the retention period is one year. However, after consultation with the operators, the period can be extended or **reduced** for specific data or category of data up to **two years** or a minimum of **six months**, taking into account the cost of storage and data retention as well as the interest for the purpose of investigation of serious crime.
- In Bulgaria (BG), the obligation prescribes a period of six months of retention. However, an **additional six months** extension is allowed under specific request of law enforcement authorities.

[13] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para. 63
[14] Periods are intended to start from the time of the communication
[15] To this end, it is also relevant to highlight that in Hungary (HU), the retention period for unsuccessful call attempts is prescribed for six months instead of the ordinary one-year-timeframe in place.



4.3. The encryption dilemma

Encryption also plays a key role in the data retention debate.

The ECJ in this context stated that "(…) Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data (…)"[16]. The risk of abuse referred by the Court may be limited by the use of appropriate technical measures such as encryption and anonymization, as prescribed by several European data protection legislations[17]. For instance, Recital (60) of the Directive (EU) 2016/680[18] states that "the controller or processor should evaluate the risks inherent in the processing and should implement measures to mitigate those risks, such as encryption".

Additionally, the ECJ further objected the lack of obligations mandating such measures on operators, arguing that the Directive "(…) does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures (…)"[19].

The Europol survey confirmed that amongst the surveyed Member States, the majority have in their respective legal systems an obligation which states that retained data needs to be encrypted for the protection of both integrity and confidentiality of the information therein. Furthermore, in the phase of information sharing, a significant amount of Member States encrypts data before submitting the intelligence (regardless of whether the information is handed in to other national bodies or foreign authorities).

[16] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, para. 66
[17] Inter alia, Art. 6.4(e), Art. 32.1(a), Art. 34.3(a) of the Regulation (EU) 2016/679 (General Data Protection Regulation) and Art.32 and Art.33 of the Regulation (EU) 2016/794 (Europol Regulation)
[18] Directive (EU) 2016/680, *Rec.* (60)
[19] See Case C-293/12 *Digital Rights Ireland Ltd*., judgement of the Court, *Para*. 67

However, encryption not only plays a role when it comes to protecting retained data but at the same time constitutes a challenge in the context of investigating serious crime and terrorism. The polarizing challenges around privacy versus security online, and the need to protect citizens' privacy while giving law enforcement the means to investigate crime, have been discussed in depth during a conference on privacy in the digital age of encryption and anonymity online hosted at Europol Headquarters on 19-20 May.

The conference saw participation from different organisations, public and private, such as the European Data Protection Supervisor, the Europol Joint Supervisory Body, the EU Agency for Network and Information Security -ENISA, Eurojust, Amnesty International, the EastWest Institute and many others from a broad range of professional backgrounds, representing private industry, academia, privacy advocates and law enforcement.

There was general consensus that the availability and use of encryption and anonymity technologies is not only important and legitimate in many circumstances but essential to a secure and safe cyberspace.

One of the main themes at the conference was the dichotomy that encryption and anonymity online present for law enforcement in terms of supporting strong encryption and opposing any technical solution that would weaken security in cyberspace for everyone, and the criminal abuse of these technologies which seriously impedes on law enforcement's ability to protect citizens from criminal and extremist behaviour, and to bring those responsible to justice.

As highlighted by Europol's Director Mr Wainwright, the challenges for law enforcement are very real and lead to a loss of investigative opportunities as a result of the growing misuse of legitimate anonymity and encryption services and tools for illegal purposes. For law enforcement, therefore, the key aspect is to define the modalities of lawful access, within well-defined and regulated boundaries, while fully respecting fundamental rights.

Echoing the need for well-defined and regulated boundaries, ENISA's Executive Director Mr. Helmbrecht advised: "Do not weaken encryption on purpose; do not inhibit the use of tools for data protection and privacy: promote secure IT. Rushed legislation is often inadequate legislation, we need to give time to discuss and invest into R&D" The event provided a unique opportunity to have an open, inclusive and transparent debate among different viewpoints towards finding a way to enhance security online without sacrificing freedom.

At the end of the conference, Mr Helmbrecht and Mr Wainwright issued a joint statement describing the challenges and proposing possible avenues of solutions for lawful criminal investigations that respect 21st century data protection (see Annex).

4.4. Collaboration between law enforcement and intelligence services

Retained data also plays a role when it comes to collaboration between law enforcement and intelligence services. From a data protection perspective, any such collaboration is sensitive because the conditions and requirements to obtain access to data often differ significantly. This, combined with the allegations by Edward Snowden of mass surveillance in 2013, lead the LIBE Committee to hold more than 15 hearings taking into account submissions from EU and US experts, EU institutions and even the legislative branches of the US government.[20]

The Europol survey revealed that, bearing in mind the potential blur between intelligence services and law enforcement bodies, only a few Member States occasionally observed an overlap between their actions, mainly relating to the exchange of best practices or the joined participation within the intelligence cycle. However, with regards to the rules applied therein, the vast majority of the Member States confirms that **specific competencies** and limitations (including those pertaining to retained data), are explicitly

[20] See http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN for details.

organized and applied by means of legislation, interagency agreements and mutual exchange of seconded officers.

It should be noted that, in this context, the JSB has carried out an extraordinary inspection in September 2014 triggered by a call from the European Parliament. The aim of the inspection was to establish whether information and personal data shared with Europol had been lawfully obtained by national authorities, particularly if initially acquired by intelligence services.

This inspection was an important contribution to the necessary debate on how to strike the right balance between freedom and security. In particular, Europol was satisfied to see that the JSB did not find any information indicating that data was obtained in violation of fundamental rights or not in compliance with the national law of the contributing States or international organisations. Furthermore, the JSB confirmed that Europol has well-established procedural measures in place to ensure that incoming data is checked for compliance before inputting it into its systems.[21]

5. Concluding remarks

The study conducted after the initial survey unveils a **non-harmonized panorama** amongst the responding Member States of the European Union, both from a legislative and an applicative perspective. Specifically, this report revealed a fragmented scenario regarding the definition of serious crime and the retention period.

From the point of view of the judicial assessment of data retention laws, national jurisdictions showed a prompter reaction to the Directive than the ECJ, which issued its Decision only in 2014: domestic legislations on data retention started to be challenged in several countries by High Courts or Constitutional Courts already after the adoption of the Directive. As a result of the aforementioned events, the existing situation is that many countries are currently experiencing a **legal *vacuum*** on data retention.

The totality of the surveyed Member States acknowledged the **importance** of data retention for the investigation, prevention and prosecution of serious and/or organized crime and terrorism.

A comprehensive **legislative framework** at the European level is supported by the majority of the interviewed Member States. However, in September 2015, the European Commission stated that "the Commission is not coming forward with any new initiatives on Data Retention. In the absence of EU rules, Member States are free to maintain their current data retention systems or set up new ones, providing of course they comply with basic principles under EU law, such as those contained in the ePrivacy Directive"[22].

A decision is expected to be issued soon by the ECJ, responding to a preliminary ruling from the Swedish Administrative Court of Appeal and to a parallel request from the Court of Appeal of England and Wales. The **joined case**[23], deals with the **interpretation of national data retention legislations** in light of Art. 15 of the **ePrivacy Directive**[24]. As underlined by the opinion of the Advocate General[25], the expected judgement will have to better clarify the relationship between domestic rules on data retention and the

[21] http://www.europoljsb.europa.eu/media/267640/1441%20final%20data%20inspection%20report%20september%202014-%20v07.pdf, accessed on 12/08/16.
[22] European Commission, Statement on National Data Retention Laws. STATEMENT/15/5654 - Brussels, 16 September 2015
[23] ECJ, Joined Cases C-203/15 and C-698/15
[24] Directive 2002/58/EC (ePrivacy Directive), Art.15
[25] Advocate General's Opinion in Joined Cases C-203/15 Tele2 and C-698/15

aforementioned directive, taking into consideration the indications given by the ECJ in its decision on the *Digital Rights Ireland Ltd* case.

An evaluation between the present survey with **Eurojust's report** on data retention reveals that the findings are aligned with each other. It should be underlined that both reports conclude with **complementary results**, especially if attention is paid to the overview of the current fragmented situation, emphasizing the high risk of undermining criminal investigations, prosecutions and judicial cooperation if a comprehensive set of rules are not provided swiftly by means of legislation.

Annex

On lawful criminal investigation that respects 21st Century data protection.

Europol and ENISA Joint Statement, 20 May 2016

1. The communication society

The desire to preserve the secrecy and integrity of a document is as old as written communication, and is deeply inscribed in our modern legislation, touching basic rights such as freedom of expression and the right to privacy. With the move to the information society and the automation of data processing, this need is becoming ever more important. Moreover, these issues go beyond an individual's rights: in a society that is ever more dependent on the correct functioning of electronic communication services, technical protection of these services is mandatory, since criminals will otherwise abuse vulnerable services. From a technical standpoint, both confidentiality and integrity may be fulfilled by the same cryptographic mechanisms. However, while secure communication services have many legitimate purposes, they may also be used to plan and conduct criminal activities. Hence, law enforcement services need tools to investigate cybercrimes as well as cyber-facilitated forms of crimes.

2. The limits of privacy

An individual's rights need to be evaluated carefully in relation to the individual rights of others to find a balance between the individual interests of the persons concerned. Thus, in the face of serious crime, law enforcement may lawfully intrude privacy or break into security mechanisms of electronic communication systems. Legislation must explicitly stipulate the conditions under which law enforcement can operate. Here, we want to stress the importance of ***proportionality*** for the use of intrusive investigative tools. This requires that the intrusive effect of the investigative measure is proportionate to the crime that was committed. It also requires the selection of the least intrusive measure to achieve the investigative objective. The legislation should include the provision of appropriate supervision to ensure that intrusive measures are used in accordance with these principles. Intercepting an encrypted communication or breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information, not on breaking the protection mechanism. The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects. Moreover, forensic methods that make use of physical fingerprints of devices might not help to intercept the communication content itself, but might provide other important clues for the investigator. Even so, there are cases in which there are no such alternatives and access to the concealed content can only be gained by a form of decryption.

3. Considerations on decryption

While no practical encryption mechanism is perfect in its design and implementation, decryption appears to be less and less feasible for law enforcement purposes. This has led to proposals to introduce mandatory backdoors or key escrow to weaken encryption. While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow. The latest generation of encryption tools allow forward secrecy, meaning that the disclosure of a long-term private key does not allow the deciphering of messages from the past.

4 . Resolving the encryption dilemma

Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible. So far, we observe a continued arms race between cryptographers and crypto-analysts. In terms of practical breaks, cryptographers are currently miles ahead, which is good news for all the legitimate users who can benefit from the improving protection of their data. However, there is no doubt that malevolent parties use the same techniques to conceal their criminal activities and identities. For the investigation and disruption of crimes, it is important to use all possible and lawfully permitted means to get access to any relevant information, even if the suspect encrypted it.

To achieve this, it would be worthwhile to collect and share best practices to circumvent encryption already in use in some jurisdictions. Investigators would benefit from more explicit and ideally aligned regulation of the lawful online use of privacy-invasive investigative tools and the conditions under which they can be applied. Moreover, policy makers in consultation with the judiciary could further contribute by issuing clear policy guidance on the proportionality of the online use of such privacy-invasive investigative tools. When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution. For the latter, the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated, is strongly advised. We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests

can be found. In this respect, the deployment of European R&D instruments may drive this collaboration while at the same time EU Agencies can work closely together in establishing best practices.

This Joint Statement is presented as a contribution from ENISA and Europol to the on-going debate on privacy and encryption. It is based on the practical experiences and perspectives of the two organisations and is neither intended as being the formal position of the EU Institutions on this subject, nor as having any prejudice to that.