Council of the European Union

Brussels, 26 October 2015
(OR. en)

13085/15

LIMITE

GENVAL 49
EUROJUST 179
COPEN 273
DROIPEN 119
JAI 760

NOTE

From:	Eurojust
To:	Delegations
No. prev. doc.:	ST 11747/1/15 REV 1 GENVAL 33 COPEN 229 DROIPEN 92 JAI 632
Subject:	Eurojust's analysis of EU Member States' legal framework and current challenges on data retention

Delegations will find in the Annex Eurojust's analysis of EU Member States' legal framework and current challenges on data retention.

Eurojust's analysis of EU Member States' legal framework and current challenges on data retention

26 October 2015

1. Purpose and methodology

Eurojust is carrying out an analysis of the current data retention framework following the 8 April 2014 decision of the Court of Justice of the European Union (CJEU) in the case C-293/12, which culminated in the annulment of the 2006 Data Retention Directive (DRD Judgment). The analytical exercise herewith presented examined the impact of the DRD Judgment on:

- national laws on data retention;
- admissibility and reliability of evidence;
- fight against serious crime and judicial cooperation.

This work is mainly based on: i) research undertaken by Eurojust; ii) information provided by the National Desks, notably via a questionnaire initiated by the National Member for IE (hereinafter, data retention questionnaire) circulated to the twenty-eight National Desks of Eurojust and for which twenty-five replies were received, and; iii) the outcome of the College thematic discussion on data retention (hereinafter, thematic discussion) held on 22 September 2015.

Aware of the importance of data retention in the fight against serious crime and judicial cooperation, Eurojust and the Luxembourgish Presidency decided to make of it the subject of the next Eurojust Workshop as well as to include this subject in the agenda of the upcoming meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions, scheduled to 10-11 December 2015.

2. Background

The Data Retention Directive (DRD) was adopted to harmonize EU efforts in the investigation and prosecution of the most serious crimes. It required operators to retain certain categories of traffic and location data for a period of 6-24 months and to make them available, on request, to law enforcement authorities for the purposes of detecting, investigating, and prosecuting serious crime. However, in 2014, the CJEU declared the DRD invalid in its entirety. It did so on grounds that the retention scheme enshrined therein breached Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights (CFR) because the limits imposed by the principle of proportionality had not been respected. Specifically, he DRD scheme was deemed not compliant with the test of strict necessity for it did not lay down clear and precise rules regarding the scope and justified limitations to the rights to privacy and data protection. The CJEU further held that the DRD lacked sufficient procedural safeguards for the protection of the data. The court came to these conclusions despite acknowledging that the retention of data genuinely satisfied an objective of general interest in the fight against serious crime.

The current fragmented EU legal framework on data retention may negatively impact efforts by national authorities in the prevention, detection, investigation and prosecution of, as well as on cross-border judicial cooperation in, criminal cases, in particular those referring to serious crime, such as migrant smuggling, terrorism, THB and cybercrime.

3. Legal and Practical impact of the DRD Judgment on EU Members States

3.1. National legislation on data retention

The DRD Judgment does not directly or automatically affect the validity of domestic transposing laws of the DRD. Simply, as a consequence thereof, there no longer is an EU obligation to maintain data retention regimes. Member States may certainly decide to legislate on the subject on their own initiative. The question arising is whether the DRD Judgment reflexively bears consequences on national data retention laws.

Already before the DRD Judgment, high courts in BG, RO, DE, CY and CZ struck down national transposing laws of the DRD for their inconsistency with constitutional standards. These decisions focused primarily on the inadmissibility of blanket data retention schemes, lack of sufficient safeguards and a precise purpose, and unsatisfactory terms of access to the data.

Following the DRD Judgment, the situation results as follows:

- **The transposing law of the DRD has been struck down in at least eleven Member States** (AT, BE, BG, DE, LT, NL, PL[1], RO, SI, SK, UK[2]). Amongst these, **nine countries** have had the law **invalidated by the Constitutional Court** (AT, BE, BG, DE, SI, NL, PL, RO, SK)**.**

[1] On 30 July 2014, The Polish Constitutional Court ruled unconstitutional certain provisions of the data retention law, which shall become inoperative on 7 February 2016.

[2] In the UK, the High Court struck down the data retention law but the judgment has been stayed until 31 March 2016.

- **In fourteen Member States** (CZ, DK, EE, ES, FI, FR, HR, HU, IE, LU, LV, MT, PT, SE) the **domestic law on data retention remains in force**. Nonetheless, in DK a part of the legislation has been repealed, while HR amended its Code of Criminal Procedure to enhance procedural safeguards and comply with the standards defined by the CJEU. FI had a legislative proposal on data retention on the pipeline at the time of the issuance of the DRD Judgment and took the opportunity to further align its law with the requirements set forth by the CJEU. In some Member States (EE, ES and IE) the national law has been (reflexively) questioned in criminal cases (see *infra* point 3.2), however the judges dismissed the claim considering *inter alia* that it provided higher safeguards than the DRD and reflected the standards set forth in the DRD Judgment. In SE, the service provider *Tele2* challenged a Stockholm Administrative Court decision that ordered the company to retain data in accordance with the legislation implementing the DRD. This case is now pending before the Administrative Appeal Court who recently requested a preliminary ruling from the CJEU. Another prominent Swedish service provider has recently announced it would not implement data retention obligations as defined in national law.

3.2. Admissibility and reliability of evidence

The post-DRD Judgment framework of data retention in EU Member States may open the way to challenges in the context of criminal proceedings. Specifically, the question arises whether, and if so to what extent, evidence gathered through data retention schemes that essentially replicate the DRD is consistent with the right to a fair trial. Issues relating to the admissibility and reliability of evidence may thus arise.

The outcomes of the data retention questionnaire and thematic discussion provided the following information:

- **Eighteen Member States** (AT, BE, BG, CZ, DK, DE, FI, FR, HR, HU, LT, LU, LV, MT, PT, SE, SI, SK) **have experienced no cases in their respective jurisdictions regarding the effect of the DRD Judgment on the admissibility, in a criminal case, of data retained and retrieved under the invalidated domestic legislation, or no information is available in this regard.** However:

  - Several complaints have been lodged before domestic courts after the decision invalidating the national transposing law of the DRD (BE).

  - The DRD Judgment call for the prior authorisation of an independent authority to access and use the retained data is concerning. The validation by the judge may take considerable time, which may hamper criminal proceedings (IT).

➢ **Five Member States** (BE, EE, ES, IE, NL) **have had case-law in this respect.** Illustratively:

- The *Audiencia Provincial de Pontevedra* decided that traffic data gathered on the basis of the transposing law of the DRD was admissible as evidence. It noted that access to retained (traffic) data always requires the previous authorisation of a judicial authority, through a motivated decision in the light of the specific circumstances. In the case in question, access was granted in relation to a specific date and timeframe, focusing on people suspected of serious criminal behaviour (drug trafficking). The court clarified that content data is excluded from the scope of application of the data retention law. Access to content data in the concerned case was authorised by a judge in line with legislation regarding limitations to the secrecy of communications, which is different from data retention. The mandatory judicial validation to access retained data enables the judge or court to assess the seriousness of the offence, nature of retained data, and thus evaluate the necessity and proportionality of the interference with the rights to privacy and protection of personal data as well as the link with the investigated serious offence (ES).

- In a murder case, the court ruled that the law transposing the DRD could not be considered *prima facie* unconstitutional as it sought to achieve objectives over and above implementing the DRD. Retained data was admitted as evidence and the defendant was convicted on the basis of location and traffic data, which was essential to build up the circumstantial case. The defendant was a completely unsuspicious person until the data was disclosed to investigative authorities. The court's decision is under appeal (IE).

- The Court of Appeal rejected the objection that data retained under the invalidated transposing law of the DRD ought to be qualified as illegally obtained evidence and thus excluded from trial. Rather, it held there had been no irreparable procedural error; consequently, the evidence was admitted. Furthermore, while there no longer is a retention obligation, data stored by the service provider - even if retained under the struck down data retention law and only for business purposes – may be legally obtained and used by the prosecution (NL).

- The court of first instance held that a possible irregularity in the collection of evidence may only lead to its exclusion from trial but not to the inadmissibility of the criminal procedure. It further ruled that the decision of the Constitutional Court by which the transposing law of the DRD was invalidated referred exclusively to metadata. To the contrary, the case at hand dealt with individual data linked to one certain suspect within the framework of a judicial investigation.

The data was requested by an independent investigating judge in line with criminal procedure law, motivated by indicia of guilt and taking into account the principles of subsidiarity and proportionality. The court added that even if the data would be unlawfully collected by the telephone operator, the gathered evidence would not necessarily be null.[3] The evidence was admitted since the court considered that both the right to a fair trial and the rights of the defence had been respected. The case is under appeal regarding one of the defendants (BE).

- Evidence gathered through data retention schemes was challenged by the defence in a case of insurance fraud. The Supreme Court dismissed the claim on grounds that the national law respected the principle of proportionality and fundamental rights (EE).

➡ Amongst the Member States where the national law on data retention has been struck down (AT, BE, BG, DE, LT, NL, PL, RO, SI, SK, UK[4]):

➢ **In four countries** (AT, LT, RO, SI) **illegally obtained evidence is not admissible in court while in three States illegally procured evidence could be, under certain conditions, admitted in court** (BE, NL, SK). Notably:

- Illegally obtained evidence will be inadmissible if: i) its use will be contrary to the principles of fair trial; ii) the irregularity at stake jeopardises the reliability of the evidence; iii) conditions of nullity have been fulfilled (BE).

- Irreparable procedural errors during the preliminary investigation may lead to excluding evidence, though this is considered unlikely by the respondent in the case of information gathered under the annulled data retention law (NL).

- The court may, in exceptional cases, admit illegally obtained evidence. It is worth noting that "*in case the criminal court has decided and accepted the data as evidence on the basis of rules that were subsequently declared contrary to the Constitution, this gives a special reason for re-trial according to* [Slovak] *law*" *(*SK).

---

3 As per Belgian law, the grounds for nullity include, e.g., violation of the right to a fair trial and doubts on reliability. None of the basis was challenged in the proceedings.

4 As per note 1 *supra*, in the UK, the High Court struck down the data retention law but the judgment has been stayed until 31 March 2016.

- **In five countries where the law was struck down by the Constitutional Court, the judgment did not consider the issue of admissibility as evidence of data retained prior to the invalidation of the data retention legislation** (AT, BE, NL, SI, SK). However:

  - As a matter of principle, decisions of the Constitutional Court do not bear retrospective effect; thus, data gathered on the basis of the annulled data retention legislation can be used in criminal proceedings (AT).

  - The Government considers that the decision of the Constitutional Court does not affect the admissibility as evidence of data retained since access by judicial authorities to retained data is sanctioned by the Code of Criminal Instruction, the content of which was not addressed by the Constitutional Court (BE).

  - The transposing law of the DRD was annulled before the DRD Judgment. For the duration of proceedings, the Constitutional Court had issued an interim injunction, with the force of law, altering the existing data retention regime. The Court ordered the destruction of all data retained on the basis of the interim injunction as long as not yet transmitted to law enforcement agencies. It did not decide on the admissibility as evidence of data already transmitted to law-enforcement authorities. The German Federal Court has twice ruled that the interim injunction is an adequate legal basis for the use of data retained and transmitted as well as sound ground for retention and transmission of data (DE).

  - The Public Prosecutor and the police may still have access to retained data (NL, SI, and SK). Specifically: i) they are dependent on the length of time that providers store data for business purposes because storage for investigative purposes is no longer obligatory (NL); ii) the data retention regime is regulated by the Code of Criminal Procedure (SI); iii) access and use of retained data must comply with fundamental rights and the rule of law, with the Constitutional Court advising the Legislator to regulate the matter similarly to the regime in place for interception of communications (SK).

  - ISPs and telecommunications companies are not obliged to delete the retained data, but they no longer have the obligation to collect it following the Constitutional ruling annulling the national law on data retention. This decision prohibited the access of law-enforcement and judicial authorities even to data retained for billing and interconnection purposes. In this regard, it is relevant noting that the provision of the Code of Criminal Procedure that requires judicial authorisation for access to retained data remains inapplicable until a new data retention law is adopted (RO).

➡ Amongst the Member States where the transposing law of the DRD remains in force (CZ, DK, EE, ES, FI, FR, HR, HU, IE, LU, LV, MT, PT, SE):

- **In ten countries** (CZ, DK, EE, ES, FR, HR, LU, LV, PT, and SE) **access to, and use of, retained data requires previous authorisation by a judicial authority.** Specifically:

  - Access to retained data is effected through a disclosure order issued by: i) a court on the basis of specific criteria, such as degree of suspicion, necessity and gravity of the crime (DK); ii) the investigative judge or public prosecutor in charge of the investigation (FR); iii) exclusively the investigative judge (HR, LU, PT); iv) the prosecutor (LV); v) a judicial authority, taken according to the principles of proportionality and necessity and duly motivated, that shall in addition determine what data is to be transferred to the authorised agents (ES).

  - Access to retained data requires authorisation depending on the nature of the data (EE and SE). That is: i) data related to the identification of the final user does not require any authorisation while access to other type of data requires authorisation by the public prosecutor, but, in any event, the request for access must be compliant with the *ultima ratio* principle (EE); ii) access to traffic data is to be decided by a court as opposed to access to IP-number and other subscriber information which is not subject to mandatory prior authorisation (SE).

- **In two countries no mandatory authorisation regarding access to, and use of, retained data exists** (HU and IE). Specifically:

  - The national data protection authority may launch a specific procedure if it is presumed that the illegal processing of personal data concerns a wide number of persons, or significantly harms interests or gives rise to a serious risk of damage; this action may lead to the blocking, deletion or destruction of illegally retained data or prohibiting the retention and or processing of personal data (HU).[5]

  - Access is limited to senior investigative officers, and a High Court judge shall be designated to oversee respect for the applicable provisions and inspect official records (IE).

[5] It should be noted that this regime is applicable to ordinary investigative actions. However, in respect of secret information gathering or covert data gathering the previous authorisation of a judicial authority is necessary in order to have access to and use retained data.

- **In eleven States** (CZ, DK, EE, FI, FR, HR, IE, LU, LV, MT, SE) **it is possible to exclude legally obtained evidence, in particular when fundamental rights and principles of criminal procedure are at stake.** To be precise:

  - Evidence gathered in breach of fundamental rights and related principles (e.g. proportionality, necessity, reasoned decision by a court of law) may lead to the exclusion of evidence (CZ, ES, HR, IE, MT, LV).

  - Evidence obtained in violation of fundamental rights – notably the right to inviolability of private life - shall not be deemed inadmissible in respect of severe forms of criminal offences where the violation of the rights, in terms of its gravity and nature, is significantly lesser than the severity of the criminal offence. In any event, the decision of the court may not be exclusively based on this type of evidence (HR).

  - Evidence obtained in deliberate and conscious violation of the accused constitutional rights will be excluded. However, reliance on a parliamentary act enjoys of a presumption of constitutionality (IE).

  - This possibility invariably depends on the type and nature of the alleged breach, the prejudice suffered by the individual and a careful consideration being made by the court as to whether justice will be served if the said evidence is excluded. Such decision lies with the court, on a case-by-case evaluation, in light of the principle of good administration of justice (MT).

  - Legally procured evidence could be excluded if: i) deemed inconsistent with EU and or international law – *rectior*, higher law – (DK and FR); ii) considered contrary to principles of criminal procedure, e.g. *ultima ration* (EE, HR, and LV); iii) its prejudicial value might overreach its probative value (IE).

  - If the court believes certain data retention provisions breach the Constitution and therefore does not apply them, it shall refer to the Constitutional Court (CZ and EE).

  - The *intime conviction* of the judge and the principle of free evaluation of evidence fully apply (FI, LU and SE). However, reliability, rather than admissibility, is the key concept in evidentiary assessment (SE).

3.3. Judicial cooperation

- **Nineteen Member States** (AT, BE, DK, DE, ES, FI, FR, HR, HU, IE, LT, LU, LV, MT, NL, PT, RO, SI, and SK) **have not experienced** (or are not aware of) **cases whereby the current complex framework on data retention undermined judicial cooperation in criminal proceedings while four Member States** (BG, CZ, EE, and SE) **already had such experience.** It is worth noting that:
  - It is problematic and challenging that national data retention legislations among close cooperation partners differ significantly (DK and EE).
  - Following the recent annulment of data retention legislation, several issues in the field of judicial cooperation in criminal matters are expected. Relevantly, while no legal basis currently exists to proceed to the retention of data, the Prosecutor-General instructed that if a MLA request on data retention is received, it should be sent to the competent judge so that he or she may decide on whether to order seizure actions. (SK).
  - Difficulties in judicial cooperation have already been felt in EU Member States. Specifically:
    - Letters of Request sent to Germany were refused on the basis of the decision of the German Constitutional Court regarding the domestic data retention scheme. Importantly, the data could eventually be shared if the request is given effect within the retention period applicable to service providers in DE, that is seven days. This short timeframe makes it extremely difficult to gather data retained in DE (CZ).
    - MLA requests were rejected due to the expiration of the retention period (BG, EE, SE).

4. <u>Other issues</u>

It should be noted that there are a number of additional practical matters that may pose challenges from the perspective of:

- Admissibility and or reliability of evidence, notably:
  - While both private companies and law enforcement authorities data controllers are required to adopt appropriate measures to protect personal data against accidental or unlawful interference, loss, disclosure and access (principle of data security), were the private company (first data controller) to be aware of a potential breach to the data, it is not required under EU law to inform law enforcement agencies (second data controller) in accordance by the time of

the transfer of the data.[6] Retained data is often a mechanism for constructing evidence trails. Doubts regarding the integrity of the "ancillary base" may put at risk of collapse the entire case.

- Anonymisation services may pose additional difficulties as far as reliability of the evidence is concerned. Indeed, law enforcement agencies may ask service providers information on who was using a certain (anonymised) IP-address at a certain time. Yet, the service provider will look for records within a certain timeframe because it cannot assume that all clocks of all servers creating log records are synchronised.

➢ Judicial cooperation, namely:

- Challenges to the execution of MLA requests on grounds of fundamental rights
- Cooperation with third countries which do not present the same standards of protection of personal data.
-

5. Final remarks

The analysis so far carried out by Eurojust on EU Member States' legal framework on data retention reveals that the fragmented regulation in place undermines criminal investigations and prosecutions as well as judicial cooperation in the fight against serious crime. Indeed, there have been a significant number of challenges to the admissibility of evidence in criminal proceedings in approximately a year from the DRD Judgment. In addition, several States currently have no defined legal data retention framework upon which law-enforcement and judicial authorities may efficiently and rapidly operate. By the same token, some Member States voice the concern that – while not yet judicially challenged – their national laws on data retention may not comply with the requirements enshrined in the DRD Judgment. Certainly, these considerations are without prejudice to the need to respect fundamental rights and ensure the necessary procedural safeguards within data retention schemes.

Accordingly, Eurojust is committed to continue its study on this realm, namely by gathering the views of practitioners during the Workshop and Consultative Forum of December 2015 so as to further detect obstacles felt in investigations and prosecutions, identify best practices in relation thereto and, as feasible and appropriate, voice the recommendations of Prosecutors-General and Directors of Public Prosecutions.

---

[6] Such an obligation was not provided for in the DRD and it is foreseen in neither the proposed Data Protection Regulation nor the proposed Data Protection Directive.