Remarks on Conducting a Data Retention Study

The Belgian consulting company Milieu is currently conducting a study on data retention on behalf of the EU Commission (DG HOME). The study aims to examine the retention of meta data (non-content data) in electronic communications for law enforcement purposes.

The aim of this study is to collect information on the legal framework and current practices for the retention of and access to electronic non-content data for law enforcement purposes in selected Member States (Austria, Estonia, France, Germany, Ireland, Italy, Poland, Portugal, Slovenia, and Spain). Unlike content data (e.g. a conversation during a telephone call, a message in an e-mail), non-content data (also called metadata) contains information on the identity of subscribers or clients of electronic communications service providers (ESPs), traffic, and the location of the user at the time of the communication.

eco, ANGA, BREKO, BUGLAS, IEN and VATM and their members criticise the questionnaire of the study, because we see:

- **the lack of an overall debate about the pros and cons of data retention for society as a whole,**
- **the lack of a comprehensive discussion of its legal basis, especially the jurisdiction of the CJEU,**
- **that necessity of data retention is insinuated without being evidence-based,**
- **the timing of the study as anticipatory without clarification of future aspects,**
- **that mandate is one-sided and not open-ended.**

I. General social debate about data retention

In our opinion, a debate about the pros and cons of data retention for society as a whole is an absolute necessity. The signing associations and their members fully acknowledge the legitimate interests of law enforcement authorities and fulfil their legal obligations in this regard, being well aware of our responsibility for society. It is further very important to consider the facts in the framework of a general societal debate. As a matter of fact, nearly the entire population of those states that implement data retention is affected. For instance, about 55 million people aged between 20 and 66 live in Germany alone. If this group uses the internet (with an assigned IP address) only once a day, and the mobile network for phone calls, also just once a day, around 110,000,000 data sets are generated in a single day. In fact, this group uses these telecommunication services much more often than just once a day, which means the real number of data sets in Germany alone is much higher. The minimum of data sets in which must be retained under German law is more like 520,000,000 on a single day in Germany. This is an estimation by experts of the signing institutions based on figures of the Bundesnetzagentur, the German Federal Network Agency.

This leads to two kinds of infringements. The first affects every single person whose data is stored, see Art. 7 and 8 of the Charter of Fundamental Rights of the European Union (EUCFR). The second concerns the telecommunication providers which are obliged to store the data sets, see Art. 16 EUCFR. The sheer amount of infringements require an open debate about data retention with society as a whole. In addition, the broader effects on society must be discussed.

II. Discussion of legal basis

It is regrettable, but not a surprise, that many member states of the EU took the position that the judgements of the CJEU on data retention (Digital Ireland, C-293/12 and Tele2/Watson, C-203/15) do not bind them, as their rules on data retention were not subject of the proceedings. It is highly doubtful and incomprehensible that most of these states have not even tried to adjust their rules in accordance with the relevant rulings of the CJEU to be conform with EU law.

After Tele2/Watson, the European Commission planned to issue guidelines on how data retention should be formulated to meet the requirements of the CJEU. As far as we know, these guidelines have never been published, although the EU-Commission would have had the opportunity. Instead, it needed the opinion of a General Attorney of the CJEU to outline examples of a general, and unlimited data retention with cause (C-623/17, C-511/18, C-512/18, C-520/18, 15.01.2020). The rulings are expected to be delivered between May and

August this year.

Furthermore, the German rules on data retention are pending at the CJEU in the requests for preliminary rulings (C-793/19 and C-794-19). The case C-793/19 should be paid special attention to, because the Oberverwaltungsgericht Nordrhein-Westfalen (High Administrative Court) has even decided in an preliminary ruling that the German rules of data retention, a parliamentarian law, must not be executed because of inconformity with European law in the light of relevant rulings of the CJEU (Digital Ireland, Tele2/Watson). The Oberverwaltungsgericht stated that the German rules of data retention are materially comparable to the ones of Sweden and UK, which have been found incompatible with Art. 15 (1) in the light of Articles 7, 8, and 11 and Article 52(1) of the EUCFR.

The Bundesverfassungsgericht (Federal Constitutional Court) aims to rule on the German data retention rules. The court questioned the state participants about the conformity of German rules with requirements of the CJEU in Tele 2/Watson. Even the government of the federal state of Bavaria doubts that the requirements of the CJEU to the retention itself are fulfilled by § 113b German Telecommunication Act (TKG), because the meta data is to be stored generally and indiscriminately and without cause in regards to i.e. geographical areas or persons.

A legal basis in conformity with EU law, especially the jurisdiction of the CJEU, would decrease the number of infringements on the fundamental rights of citizens and ISPs because the amount of stored data would be significantly less. Furthermore, such a legal basis would provide legal certainty to telecom operators.

III. Necessity of data retention

Regarding the question whether there are any less infringing means than data retention that are equally effective, it must also be considered that, just in Germany, several hundred million Euros have been sunk into matters of data retention. The obliged providers were forced to invest in provisioning of technical equipment and its maintenance. Furthermore, some of their staff had to be diverted from other tasks, which in opposite would have benefited the provider ‘s return on investment.

The first trial of implementation of German data retention rules was annulled by the Bundesverfassungsgericht in 2010. The second trial, meanwhile, cannot be carried out because of inconformity with European law and is likely to be judged incompatible by the CJEU finally

(C-793/19 a. C-794/19). In consequence, investments for data retention were in vain in 2010 and as well are very likely to be in vain this time.

It must be safeguarded that there will not be sunk costs a third time. Therefore, it is absolutely necessary that all social and legal aspects for a framework have been considered. The member states in favour of data retention have shown close to no efforts for an examination of data retention to create a basis for an evidence based decision making.

We and our members do respect the legitimate interests of law enforcement. Even more importantly, the companies support the law enforcement actively in many cases and in an institutionalised manner. For our member companies, acting in accordance with the law both in handling customer data and in supporting law enforcement authorities is a matter of course. To do so, we expect legal certainty in the sense that necessity has to be proven by evidence.

To create the basis for evidence a study on data retention would have to include many questions, missing in the current study and the corresponding questionnaires. For a fact-based decision, the following questions inter alia should be addressed:

- How many crimes could not be prosecuted due to data retention not being implemented or executed and that is causal for non-prosecution?

- How many crimes could have been prosecuted without data retention, because the conditions for a legal interception were given, but, due to the lack of capacity at criminal courts, state prosecutors, and in law enforcement, the legal interception was not requested?

- How many crimes were prosecuted although no data retention in force?

- Regarding organised crime: How many the offenders, which were later prosecuted used IP addresses, from which their names or location were directly identifiable?

IV. Timing of Study and Mandate

In our opinion, the timing of the study is improper in several ways. It is necessary to clarify the aspects of sections I – III above, before mandating a study like the current one. If alone in Germany 520,000,000 data sets would be created for data retention every day, what is the combined figure for all European member states which favour data retention? Without an overall debate about the pros and cons of data retention for society as a whole there is no

proper justification for data retention.

Lacking serious trials for finding less infringing means with the same level of efficacy puts the necessity of data retention in question, as does a study which does not include trials for finding less infringing means that are equally effective. As a consequence, there was not even an attempt to act proportionately.

V. Conclusion

The signing associations and their members ask for the opening of a broad debate about the pros and cons of data retention for society as a whole. Therefore, the EU Commission and those Member States in favour of data retention should start consultations and dialogues with all stakeholders (society, citizens, non-governmental organisations, and providers of electronic communication as well as the views of law enforcement authorities). This approach would give at least the chance to achieve a consensus of society, industry, and the state and might be suited to properly justify data retention.

We expect a comprehensive discussion on the legal basis for data retention, especially the jurisdiction of the CJEU, both existing and forthcoming (C-623/17, C-511/18, C-512/18, C-520/18, 15.01.2020). This would provide conformity with EU law and legal certainty for telecommunication providers, along with the coming judgements of the CJEU.

In both policy debates and in such studies, we request serious proposals which include less infringing measures than data retention but with the same level of efficacy. The necessity of data retention must not longer be insinuated without supporting evidence.
The mandate of a study has to create an evidence basis, whether data retention is necessary or not and has to explore the views of society, citizens, non-governmental organisations and providers of electronic communication as well as the views of law enforcement authorities.
The mandate of the study must also be open ended. This would bear the opportunity to identify what kind of data law enforcement authorities really require and how that could be provided in less infringing ways than data retention.

18.05.2020

ANGA Der Breitbandverband e. V., Reinhardtstraße 14, 10117 Berlin
Tel.: 030 / 2404 7739-0, Fax: 030 / 2404 7739-9, E-Mail: info@anga.de

BREKO Bundesverband Breitbandkommunikation e. V., Invalidenstraße 91, 10115 Berlin
Tel.: 030 / 58580-415, Fax: 030 / 58580-412, E-Mail: breko@brekoverband.de

BUGLAS Bundesverband Glasfaseranschluss e. V., Eduard-Pflüger-Straße 58, 53113 Bonn
Tel.: 0228 / 909045-0, Fax: 0228 / 909045-88, E-Mail: info@buglas.de

eco Verband der Internetwirtschaft e. V., Französische Straße 48, 10117 Berlin
Tel.: 030 / 2021567-0, Fax: 030 / 2021567-11, E-Mail: berlin@eco.de

IEN Initiative Europäischer Netzbetreiber, Marienstr. 30, 10117 Berlin
Tel: 030 / 32 53 80 -66, Fax: 030 / 32 53 80 -67, E-Mail: info@ien-berlin.com

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V., Alexanderstraße 3, 10117 10178 Berlin
Tel.: 030 / 505615-38, Fax: 030 / 505615-39, E-Mail: vatm@vatm.de