FONDATION ROBERT SCHUMAN

POLICY PAPER

European issues
n°511
16th April 2019

Protecting European citizens in an ultra-connected world

Silvio MASCAGNA
and
Seyda EMEK

On 3rd April the Robert Schuman Foundation organised a conference on the theme of "The Protection of European Citizens in an Ultra-Connected World" in Luxembourg with the Max Planck Institute. We are continuing the publication of the report with the contributions made by two other participants. Silvio Mascagna, a member of the cabinet of Julian King, European Commissioner for Security explains how the Commission is developing the interoperability of databases in the fight to counter terrorism. Seyda Emek, advisor to the European coordinator for the fight to counter terrorism, Gilles de Kerchove, illustrates the need to retain data to facilitate investigations.

1- SILVIO MASCAGNA - Member of the Cabinet of Sir Julian King, European Commissioner for Security Union

When European citizens are interviewed about their greatest concerns, as illustrated by recent surveys undertaken in view of the European elections, security and the fight to counter terrorism are still priority issues.

Despite the defeat of Daesh in Iraq and Syria, the terrorist threat is still high in Europe. Unfortunately, we were witness to this in France with the attack on the Christmas Market of Strasbourg (December 2018). According to the French Centre for the Analysis of Terrorism (CAT), 26 terrorist incidents targeted the EU in 2018, of which four were attacks, one attempted attack and 21 projected attacks. However, the threat has changed in nature with the last incidents being carried out by individuals acting alone, targeting public areas; perpetrators were often radicalised online or within communities.

WORK UNDERTAKEN TO STRENGTHEN SECURITY UNION

For more than two years now the European Commissioner for Security Union has piloted work at European level to guarantee greater security to our fellow citizens.

We have adopted a dual approach:
- On the one hand by trying to deprive terrorists of the means to cause harm as we have limited their access to firearms, financing, as well as restricting their operational capacity via increased protection of the external borders.
- On the other we are developing our resilience to avoid and prevent attacks or improving our response when they do occur. This notably means countering radicalisation in the communities and on the internet, notably withdrawing online terrorist content.

But guaranteeing and strengthening security must necessarily go hand in hand with the respect of fundamental rights.
In a European Union founded on the respect of human dignity, democracy, the rule of law and Human Rights, the protection and promotion of citizens' security and the respect fundamental rights are complementary and must mutually strengthen each other.
I shall return to this issue, which is at centre of our debate, but allow me to provide a rapid overview of the actions undertaken at European level under the Commissioner's mandate.

We have stepped up controls on the external borders: since April 2017 everyone, including European citizens, entering and leaving the Schengen area has been systematically been controlled.
We adopted the PNR directive and now 20 Member States have notified the full transposition of the said directive.

We have also stepped up information exchange at European level. I would like to point to the increase in data resourcing and the use of the Schengen Information System (SIS) since 2015. In December 2017 it contained 76.5 million warnings, and the

Member States consulted it more than 5.2 billion times. We organised the introduction of two new databases: the entry-exit database, which enables the recording of the entry and exit of third country residents. The ETIAS is the equivalent of the American ESTA. These bases will also form part of the new interoperable system.
We have put forward legislation (e-evidence) that facilitates access to electronic proof/evidence, often to be found in another State or on the cloud. This proposal will enable direct (by the judicial authority to the internet platform) access to e-evidence within 10 days, instead of 10 months using legal cooperation. The Council came to an agreement over the text, but unfortunately, we will not be able to finalise it before the elections, because no agreement has been found with the European Parliament. This instrument will be very useful since we know that many requests cannot be completed because e-evidence has not be obtained in time; it is notably even more relevant in terms of terrorism.

I mentioned the internet. Online content has played a role in every attack perpetrated in Europe over the last two years, whether this has been to encourage committing an attack, giving instructions regarding the operational method or to glorify the attack's lethal effects.

The regulation on the prevention of the dissemination of terrorist content online that the Commission adopted in September 2018 will notably force platforms to respond within an hour when police or judicial authorities send them an injunction to remove infringing content.

We are now focusing all our work to achieve an agreement between the Council and the European Parliament before the European elections. But how can we guarantee that the promotion of citizens' security of and the respect of fundamental rights are complementary with one another?
The Commission has progressively developed mechanisms that aim to strengthen the systematic assessment of their impact on fundamental rights over the last ten years. The respect of fundamental rights was also assessed ex post as part of the general assessment of the EU's policies to ensure they were justified and to check their proportionality with the goals sought.

The Court of Justice (ECJ) does not just assess the compatibility of the Union's legislation with fundamental rights and with measures taken at national level by the Member States to comply with European legislation and international agreements like the CETA.

This includes, for example the invalidation of the directive on data retention (directive 2006/24/CE). It is for example the decision whereby the UK and Sweden's legislation which imposes "general and blind" requirements on telecommunications operators to retain traffic and location data is incompatible with the directive on electronic communications (directive 2002/58/CE) in terms of the Charter of Fundamental Rights (the principle of the respect of private and family life and the protection of personal data).

At the same time the Commission ensures that the Member States respect the Charter in the implementation of relevant European legislation.

For specific initiatives, specialist organisations like the European Data Protection Supervisor (EDPS) are involved. The specific expertise of the European Union Agency for Fundamental Rights established in 2007 is also increasingly called upon by the EU's institutions to provide better response to the challenges made to fundamental rights, notably by way of targeted consultations or requests for opinion on issues or specific proposals.
Guarantees specific to fundamental rights are often an important priority in the legislative process involving the European Parliament and the Council. Negotiations between co-legislators are undertaken in several rounds to lend even greater strength to the guarantee of fundamental rights.

DATABASE INTEROPERABILITY

In this regard I would like to mention the legislative initiative on the interoperability of security and migratory databases. This involves the processing of personal data in large scale IT systems.
We have strengthened interoperability, i.e. the way

we communicate between the different security and migratory databases, so that our police services have all the information they need in due time. This will also help in the fight to counter false identities and multiple identities, because several perpetrators of attacks (Marseilles, Berlin) were registered under different identities in several European databases. Hence, it will enable the consultation of all security and migratory databases simultaneously using a search engine, without modifying access rights to these databases (the hit/no hit principle). We hope that this system will be operational by 2023 at the latest. In this proposal we have taken good care to maintain the limits of the goal to be achieved and to protect fundamental rights.

From the very start the drafting of our interoperability proposals was an inclusive, transparent process, together with the European Parliament's LIBE committee and the Member States within the Council and by involving the European Data Protection Supervisor and the Fundamental Rights Agency. Our approach has been to ensure that the protection of data is integrated into the features of interoperability on its conception.

The proposals that we presented in December 2017 are, in our opinion, fully compliant with the Charter of Fundamental Rights, to the general data protection regulation (GDPR) and all relevant European legislation. Any impact on data protection would be proportionate, pursuing a legitimate, balanced goal in relation to other rights.

We think that the results of this inclusive preparation work – including the contributions made by the European Data Protection Supervisor and the Fundamental Rights Agency – are clearly reflected in the result. Their opinions helped co-legislators to further clarify protection and the guarantee surrounding the right to information for example.

Interoperability does not comprise collating new data, nor merging individual systems together. It means using existing information held in our systems in a more targeted, more efficient manner, taking into account the rights of the people concerned. To this end new features will be supported by existing EU information systems which will retain their specific rules regarding the limit on purpose, access and the retention of data. The processing of data will be limited to what is strictly necessary and proportionate, in line with the limits on existing goals. No new types of information will be collated for interoperability ends.

It will be the contrary, relevant guarantees will be integrated into each component and attached to each of the interoperability goals.

Moreover, interoperability does not involve profiling. Interoperability proposals do not provide for the use of profiling tools. We all agree on the goal to counter discrimination based on gender, race or ethnic origin, religion, handicap, age or sexual preference. There is an article in our proposals establishing relevant guarantees. Proposals also guarantee that children benefit from every necessary protection in the processing of their personal data.

Undoubtedly it is a model to follow in terms of how balanced, inclusive policies should be made in the area of security.

Silvio MASCAGNA

2- SEYDA EMEK - Advisor to the European coordinator for the fight to counter terrorism, Gilles de Kerchove

I. WHY IS DATA RETENTION NECESSARY?

Europol has gathered from its members concrete examples of cases affected by the current data retention regime in the EU. The contribution has been shared in 2017 to the Council Working Party on Information Exchange and Data Protection (DAPIX)
The list is not exhaustive, but focuses on typical scenarios law enforcement investigators encounter in their daily work, and the subsequent consequences for those investigations as a result of data retention issues. In essence, the attribution of a criminal activity to the perpetrator is either significantly delayed or made impossible due to the way in which information and data is stored, handled and shared by communication providers and online content providers.

Example 1:

Investigation conducted by the German Public Prosecutor General's office into a network of individuals suspected of supporting of the Islamic State, the examining judge at the Federal Court of Justice requested log files of a chat forum used by the group to communicate.

The judge received a range of different IP addresses without source port numbers (not logged by the hosting provider of the chat forum). A request to identify subscribers using these IP addresses was sent to the relevant German Internet Service Provider.
The ISP could not identify unique subscribers per IP address because of the use of Carrier-Grade Network Address Translation (CGN) and the absence of source port numbers. The public prosecutor was unable to pursue this line of enquiry.[1]
The lack of harmonized data retention obligation across Europe also affects the ability of communication providers and Internet Service Providers (ISPs) to comply with their legal obligations to enable the identification of their subscribers on the basis of an IP address and when served with a court order or a law enforcement request.
This creates a serious online capability gap in judiciary and law enforcement efforts to investigate and attribute crime. This is due to a combination of different factors: It is due first and foremost to the lack of legal obligation for electronic service providers (ESPs) such as social media platforms, webmail services, hosting services to log a piece of information called 'source port number'.
Second, it is also due to the massive adoption by ISPs of a technology called Carrier-Grade Network Address Translation (CGN), which allows ISPs to share one IP address with up to 65.000 subscribers. In the absence of the source port number, ISPs cannot differentiate between subscribers connected to the same ESP with the same shared IPv4 address at a given point in time.

Example 2:

In an investigation related to Islamist terrorism, a joint investigation team searched for contact persons, i.e. possible order-givers and accomplices, of one of the persons charged. Research on social networks led to the identification of relevant social network profiles of possible contact persons.
The social network company was able to provide the IP addresses used to connect to the platform but not the source port number.
According to them, the storage of ports is technically possible, but for data protection reasons (E-privacy directive), the company can only collect and store data which is necessary for the operation of the network and for billing purposes. This is not the case for source port details. Analysis of the IP addresses transmitted by the company indicates that they belong to a German mobile ISP.
However, the ISP was not able to assign the IP addresses to the subscribers because the company allocates the same IP address to several thousand customers at the same time (CGN).
As a result, it was not possible to identify potential further targets by means of the IP addresses.

Example 3:

In relation to the threat of an attack in Paris, competent law enforcement authorities (LEAs) were investigating

1. Internet service providers are increasing their use of CGN technologies. A recent study showed that in 2016, 90% of mobile internet network operators (GSM, 2G, 3G, 4G providers) and 38% of fixed line internet access providers (cable, fibre and ADSL) were using CGN technologies, while 12% were planning to deploy it in the (then) coming months.

an individual behind a social media account.
Logs showed that the individual was connecting with mobile IP addresses provided by a French mobile internet provider.
Due to the use of CGN, the individual could not be identified or located by technical means.

II. WHY WE NEED AN EU INSTRUMENT

1. The current situation is not sustainable. Companies are no longer legally obliged to retain communications traffic data in Member States such as Germany, Sweden and Netherlands after Court rulings.

2. 28 different systems of data retention in the EU have to be avoided. This would be very difficult for companies to handle. The lack of a harmonized approach across the EU may lead to difficulties in law enforcement and judicial cooperation.

3. Targeted retention is not a solution:
-It is impossible from a security perspective, as it cannot be known in advance who will commit serious offenses.
- It would also be discriminatory from a human rights perspective, if for example immigrant or poorer neighbourhoods were designated for data retention, while richer areas were exempted. Criminals could circumvent retention if this was known.
- It is also not enough to retain for a few weeks before or after events.

4. Data kept for business purposes is uneven across companies and not sufficient.

5. Given the increased use by criminals and terrorists of encryption, which makes access to content difficult if not impossible, retention of traffic data is even more crucial to avoid that the competent authorities "go dark".

6. EU data retention instrument is needed that fulfils the needs of law enforcement and other competent authorities as well as the requirements of the ECJ. The EU Counter-Terrorism Coordinator has made suggestions for such a possible legislative EU act in recent discussions in the Council.

III. ECJ JURISPRUDENCE REQUIREMENTS IN TELE2 RULING:

Measure has to be limited to the strictly necessary, be based on objective evidence and needs to set out clear and precise rules.
The ECJ states that retention needs to be restricted in relation to:
a) data pertaining to a particular time period and/or geographical area and/or a group of
persons likely to be involved, in one way or another, in a serious crime,
b) or persons who could, for other reasons, contribute, through their data being retained, to fighting crime.

ECJ jurisprudence does not give hints as to what ECJ-judges would consider as necessary means when it comes to data retention (no positive explanation/ examples what the court would deem as necessary. The court only frames in negative terms what cannot be.

IV. EU COUNTER-TERRORISM COORDINATOR'S SUGGESTION "RESTRICTED ACCESS TO RETAINED DATA"

1.) A different legislative approach possible:

- Restricted access to retained data would be required to fight serious crime and terrorism.
- Higher safeguards with regard to storage, access and use of the data would ensure overall
proportionality.
- The Justice Home affairs Council of 7th December 2017 acknowledged that the concept could eventually serve as basis for developing a data retention framework at EU level and encouraged to facilitate preparatory works for a related data matrix in close collaboration with Member States' technical experts for further discussion in FoP DAPIX that was found for this purpose.
- Europol, together with the Presidency hosted two workshops bringing together specialised investigators and forensic experts from Member States. Council, Commission and Eurojust participated.
- FoP DAPIX convenes regularly in the last 2 years to examine ECJ rulings, national jurisprudence in Member States and legal framework in Member States to find

data retention solutions.
- EU Counter Terrorism Coordinator has made suggestions for possible EU legislation to the Council based on the idea of restricted retention of data.
- Old EU legislation was based on internal market rules. New would ensure protection of fundamental rights, etc

EU instrument would include all the strict access conditions set out by the ECJ in the Tele 2 ruling:

Restricting access solely to the objective of fighting terrorism and serious crime.
Instrument could further consider combining data retention for the purposes of prevention, investigation and prosecution of serious crime with a parallel system of ensuring access to data kept for business purposes by providers (not subject to storage obligations or kept for business purposes although there are also storage obligations, hybrid model).
Such a hybrid model could be instrumental in ensuring the availability of data in emergency or life-threatening situations not necessarily related to criminal activity, e. g. missing persons.
Prescribing clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data.
Access, subject to prior review by a court or an independent administrative authority (exception cases of urgency).
Adoption of e-privacy regulation's structure in light of Tele2-ruling.

Let me explain what I mean with this in a bit more detail.

The EU instrument could assess the current very serious terrorist threat to the EU as well as the increased use of cyber space and communications technology for serious crime, hence the serious threat to public security.
The instrument could include a review clause after several years and require each Member State to assess on a regular basis the threat/risk to public security on its territory which requires data retention and renew the measure following these risk assessments.

-As a first step, to address one of the concerns of the ECJ, there could be an opt-out possibility for persons whose communications are subject, according to the rules of national law, to the obligation of professional secrecy. This means that such users could request that their data is not being accessed and hence consent to the processing of their personal data relevant for operating this exception. Rules for such an opt-out would need to be specified.
- Beyond these exceptions, it is suggested to restrict the retention to the minimum by focusing the necessity test on data categories and providers and only retain data categories that are absolutely and objectively necessary to safeguard public security. It would be important to establish and demonstrate this link.

The necessity test would not focus on groups of persons or specific geographical areas within the territory of a Member State. This would allow to restrict retention while corresponding fully to the law enforcement needs.
There would be a general EU wide approach, the strict parameters and criteria of which would be set out in the instrument, based on strict necessity tests as to which type of data absolutely needs to be retained. Objective evidence with regard to the necessity of the data types could potentially be included in the legal instrument or implementing measures. These measures would have to be regularly renewed after new necessity assessments.
A strict necessity test could and should be carried out for the data categories that are indispensable for retention.
Carrying out these necessity assessments, based on the needs of law enforcement and other competent authorities, requires effort and analysis, but allows to narrow down the scope of the data retained to the minimum necessary for the law enforcement purpose, in line with the ECJ requirements.
If there are strict necessity filters, data retention would not be generalized (only a part of the communications data categories will be retained, even though it might cover a large percentage of the population).
On the other hand, retention would not be targeted to specific time periods, locations or groups of persons

which would not satisfy the needs of law enforcement. The additional exemptions for persons linked to professional secrecy also mean that not the whole population is affected. The population covered by the measures would fall under the category that they "could, for other reasons, contribute, through their data being retained, to fighting crime".

The EU data retention instrument would need to show why retention of certain types of data is absolutely necessary, while also showing that there is a thorough methodology to determine data retention obligations.

To satisfy the ECJ requirements, the possibility of competent authorities to access data stored could be limited to the purposes of counter-terrorism, organized and serious crime, including cyber attacks only.

The six months retention period would be the lower limit of previous EU data retention legislation.

To comply with para 122 of the Tele 2 ruling, it seems that the EU instrument would have to mandate irreversible destruction of the data at the end of the data retention period. However, it would need to be clarified how this relates to data that is retained for business purposes anyhow (where the same data is covered by the retention obligation). Probably it would mean destruction only of the data that otherwise would not have been retained.

Storage in Europe and in encrypted fashion/ pseudonymisation

The ECJ requires " imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse". Therefore, mandating requirements for data security, storing the data in the EU (as the ECJ requires in para 122 of the Tele 2 ruling) and in encrypted fashion would protect against unauthorized access. It would need to be clarified whether encrypted storage is possible with regard to business models and what other privacy by design could be incorporated.

Seyda EMEK

You can read all of our publications on our site :
www.robert-schuman.eu

Publishing Director : Pascale JOANNIN