SAT-LAW

STRATEGIC ASSESSMENT FOR LAW AND POLICE COOPERATION

FACT SHEET – EUROPEAN INVESTIGATION ORDER AND DATA PROTECTION

I. The context

From the initial results of the SAT LAW Living Labs a central topic emerged: the need to strike a fair balance between security, in performing cross-border investigative acts and collecting and sharing digital evidence across different EU Member States, and the fundamental right to the protection of personal information. The sizeable expansion of user-generated content has created a new operational challenge for investigative authorities. While the internet and online social networks have completely changed societal communications (rather positively) and created new economic opportunities, these technological advancements have changed (and continue to change) the very nature of crime, as well as of the evidence that supports law enforcement actions against it. Terrorism and organised crime have been traditional threats to EU Member States. Cybercrime is an emerging one. Each one of them on its own, as well as the combination of these old forms of criminality with the new field of cybercrime, create an unprecedented criminal landscape and a variety of new challenges for law enforcement authorities.

The adoption of Directive 2014/41 on the European Investigative Order (EIO) was an important step towards enhancing the capabilities of law enforcement agencies, but it should not be overlooked that the creation of new and inventive

ways to prevent new forms of criminality need to be based on strong evidence and information. Digital evidence and, most importantly, open-source “big data” could become the basis of the digital overhaul of law enforcement operations, but this shall not come at the cost of fundamental rights, especially at the cost of the fundamental right to the protection of personal information. While Directive 2014/41 on the EIO highlights, in art. 20, the importance of striking a balance between security and data protection, it cannot provide for a comprehensive regime and adequate safeguards to do so. One shall necessarily refer to the specific data protection legislative acquis of the EU, in order to identify the crucial data protection safeguards. Directive 2016/680, in particular, is of great importance, as the generic nature of the GDPR does not (and was not meant) to meet the specific needs and particularities of the investigative activities of law enforcement agencies.

Identifying the relevant legal instrument when it comes to data protection will, nonetheless, only cover part of the problem. The appropriate interpretation of that legal regime within the specific context of an investigative order poses a number of challenges. To begin with, the roles of controller and processor between the cooperating authorities in different Member States might not be straightforward. The exact delimitation of the role of each authority is important, because of the different data protection duties bestowed upon the controller and the processor.

Digital evidence and open-source big data include, quite often, special categories of personal data and, as a consequence, according to Art. 10 of Directive 2016/680, special processing parameters apply (simply put, the processing of special categories of data is possible under stricter terms and extra safeguards).

To strike a fair balance between the rights of the data subject (esp. rectification, restriction of processing, and erasure) and the need to perform investigative operations is a delicate and demanding task. While investigative operations should not be hampered, especially when the crime committed is serious and the evidence strong, at the same time, the data subject must not be unreasonably denied the exercise of his/her rights.

Fairness of processing digital evidence, especially the need for transparency is a key principle (especially due to the fact that digital evidence is available in large volumes, is easily collected, and is prone to processing by automated means, to name a few of the inherent digital risks). Not only must the data subject have fair access to his/her data, but the data controller (i.e. the investigative authorities) must be very open on their processing methods; in particular, they should be diligently keeping records (electronic logs where automated means of processing are employed) so that transparency is facilitated and their accountability is safeguarded.

The purpose limitation principle must be carefully respected, as digital evidence might create incentives to go beyond the initial goal that gave rise to the EIO.

Data minimisation is a major issue. By its very nature, digital evidence is rich in information, easily accessible, and open to a multitude of processing techniques. There must, therefore, be special care to collect, process, and retain only what is absolutely necessary for the specific task. Time limitations in retaining digital evidence are particularly important.

Due to the inherent dangers relating to digital information, privacy by design and by default within the context of an EIO are more necessary than ever. It is equally as important that data security is safeguarded at all stages and by all the institutions involved.

II – Needs identified

- The need to **better train law enforcement officials**, especially in relation to the data protection limitations of digital evidence and open-source big data; it is essential for all practitioners, policy-makers and policing professionals to understand what digital evidence and open-source big data is and what it is not, how it can be used and the data protection limitations or conditions that apply, all the more so considering that safeguarding data protection is not to be understood as an isolated end in itself. On the contrary, safeguarding data protection contributes to the respect and fulfilment of the fair trial guarantees established in art. 6 of the ECHR and 47 of the Charter of the Fundamental Rights of EU citizens;

- The need for **enhanced data security**; digital evidence and open-source big data are sensitive investigative products, in the sense that they are prone to all kinds of manipulation and attacks even when possessed by Member State law enforcement authorities. Evidence produced in the executing Member State and shared with the ordering Member State shall be protected during the entire life span of an EIO operation;

- The need for **enhanced quality of digital evidence and open-source big data**; especially in the case of open-source big data it is not easy to ensure that the information obtained from them is accurate and trustworthy. The sheer size of the data, as well as the uncontrollable nature of the sources that produce digital evidence and open-source big data pose major risks for the quality of information extracted from them.

- The need to **safeguard the purpose limitation and data minimisation principle**s; the fact that digital evidence and open source big data are produced with relative ease and on a mass scale, creates temptations for possible misuses, especially for processing of the personal information included within them for purposes incompatible with the initial EIO request and the retention of the obtained digital evidence and open source big data for periods longer than absolutely necessary for the specific investigative act. Such practices must be avoided and law enforcement authorities should limit themselves to what is absolutely necessary in order to achieve their original goals.

III – Relevants facts and Remedies

Concerning the topic of data protection within the EIO framework, especially when it comes to collecting digital evidence, three relevant issues have been identified :

- Member State variations in data protection standards
- The burden of managing open-source big data
- Digital data transfer hurdles within the framework of an EIO

For further information and training on the EIO, please refer to

https://www.satlawproject.eu/

This project has received funding from the European Commission Directorate-General Justice and Consumers under the Agreement no. 800816.