Council of the European Union

Brussels, 7 November 2019
(OR. en)

13510/19

LIMITE

COSI 221
DAPIX 320
ENFOPOL 470
JAI 1140

NOTE

From:	Presidency
To:	Delegations
Subject:	EU Information Management - Automation, access to, sharing of, and analysis of information

EU Information Management[1] – automation, access to, exchange of, and analysis of information

Law enforcement work is inherently an information-based activity. Information is gathered, processed and acted upon in order to prevent, detect and investigate crime. For law enforcement to be effective, processing large quantities of information or data from a variety of sources is often required. In the era of digital data, relevant authorities have to cope with further increasing volumes of information, which needs to be collected, integrated and analysed and furthermore compiled into a comprehensive overview of a specific situation, both at operational and strategic level.

[1] Information management is defined in line with the DAPIX IE discussions on automation of information exchange in a strategic context1 as pertaining to the processing of data or sets of data, whether or not operated by automated means, such as collecting, consulting, exchanging, storing, deleting etc., or profiling. When data is processed, organized, structured or presented in a given context to make it meaningful, it is called information. In the law enforcement context, the management of the above processes can focus either on dealing with an individual case (operational information management) or on establishing and developing the framework for executing these processes more efficiently and effectively (strategic information management).

The need to ensure that law enforcement authorities are in a position to exploit digital data and large volumes of information and to boost the effectiveness of crime analysis was underlined at the Council in June. This discussion paper concentrates on three aspects of information management: access to and analysis of information, as well as automation of information exchange.

Access to information: challenges of new technologies

Law enforcement authorities continue to face technical difficulties and challenges in accessing information held by private parties that they are lawfully entitled to obtain and that they need for their everyday work especially in the online context.[2] Anonymisation techniques make it increasingly difficult to identify the creator, sender or receiver of data. Introduction of 5G networks can mean that law enforcement authorities are no longer able to locate or identify specific mobile devices and that the authorities are thus unable to assign a device to a specific person. The existence of network slicing leads to potential challenges as information is fragmented, and may either not be available or accessible from a technical point of view for law enforcement. This will challenge law enforcement and may make lawful interception virtually impossible.[3]

Once the data has been identified, law enforcement authorities need to be able to access it. Changes in the way data is retained[4] may mean that the data required is no longer available at this point. End-to-end encryption could mean that the data that is finally obtained might not be in a readable format.

Member States should ensure that the needs of law enforcement authorities are known and taken into consideration when developing new technologies that influence their work. Law enforcement authorities themselves should take an active position at the forefront to highlight their needs and to develop solutions that address their concerns. As agreed upon by the Council in October, an innovation laboratory should be established at Europol where, among other tasks, an active role of law enforcement in relation to technological solutions sought should be addressed.

---

2 Part of these problems have been elaborated in discussions on Europol's cooperation with private parties in Law Enforcement Working Party.

3 Cf. documents 8268/19 and 8983/19.

4 Document 14319/18.

Analysis of information

In the era of digital data, law enforcement authorities have access to more data and information than they can currently use. The need to ensure that law enforcement authorities are in a position to use digital data and large volumes of information and to boost the effectiveness of crime analysis was underlined at the Council in June[5].

Criminal analysis remains at the core of law enforcement. Analysis provides the added value to raw data that makes it into actionable information that can be used nationally as well as in cross-border operations. However, a clear vision of EU level standards for crime analysis work is missing. Successfully enhancing analysis activities across the Union requires a better understanding of national law enforcement proceedings and of the various information processes involved, including those of criminal investigation and criminal intelligence gathering. It will also put more emphasis on the quality of information that is used as the raw material of analysis.

To this effect, Member States' authorities should intensify their cooperation with Europol as well as with eu-LISA and CEPOL. Member States should also invest more efforts to develop best practices on how to integrate criminal analysis into law enforcement operations - both at national and at Union level. Both should support each other. To that end, Member States should assess the ways which are most suited for an increasingly efficient cooperation between these levels. The criminal intelligence analysis and data analytics portal CONAN established at Europol subsequent to the Novel Actionable Information initiative, which was forwarded by the previous Presidency is a good example of such common work that advocates connecting experts, tools, initiatives and services in the area of digital data.[6]

Automation of information management

The ultimate goal of information management from a business perspective is to ensure that end-users have a fast, streamlined and systematic access to all the information they need and which they are legally entitled to obtain to perform their tasks: the right information to the right person at the right time and place.

---

5 Council Conclusions 9720/19.
6 Council Conclusions 9720/19.

Automation of information serves to release budgetary and human resources from labor- and time-consuming routines. Provided, that common standards for information are agreed upon and high data quality is ensured, automation enables competent authorities to better cope with the ever growing amount of data to be processed in law enforcement.

Fundamental rights and freedoms of natural persons, and the requirements stemming from EU data protection legislation set limits to the use of automation in law enforcement. For instance, decisions which are only based on automated processing, including profiling, and which produce an adverse legal effect on the data subject are, in principle, prohibited unless authorised by Union or national law.[7] Such legislation must provide appropriate safeguards for the rights and freedoms of the subject, at least the right to obtain human intervention on the part of the competent authority involved.

It is of prime importance for EU internal security that law enforcement authorities make effective use of information technologies and keep pace with both rapidly evolving technologies. Cross-border law enforcement is based on the shared purpose of fighting cross-border crime in a spirit of cooperation and mutual support between the competent national authorities and supporting EU agencies. It relies, furthermore, essentially on information exchange. In their fight against crime and terrorism, law enforcement authorities and supporting Union agencies need a framework, which, in particular, enables smooth information exchange.

Any strategic planning of the future of EU internal security has to take account of these key elements of cross-border law enforcement information exchange. However, particular attention should be paid to the perspective of the end-user. Simplicity should be the key here: the end-users should gain access to the information they need and can lawfully obtain with as little effort as possible and avoid multiple queries based on the same search attributes. Both dealing with an individual case (operational information management) and establishing and developing the framework for executing these processes more efficiently and effectively (strategic information management) need to focus on the prioritized operational needs.

[7] Directive (EU) 2016/680, Art. 11.

The Regulations on the Interoperability of information systems[8] involve the interoperability between certain large scale EU information systems (EES, ETIAS, ECRIS-TCN, SIS, VIS and Eurodac) that allow those systems to supplement each other and facilitate searches through a single entry by streamlining access to the underlying information systems, to Europol and Interpol data. These reforms are to a large extent based on the strengths of automation, and when implemented thoroughly will substantiate the fight against crime in Europe even further and make it more difficult for criminals to misuse the gaps between information systems and the way in which data is searched and cross-matched at borders or during police checks.

Implementing and applying interoperability requires aligning legal frameworks, information management tools, policies and, finally, working processes in order to avoid redundancies and inconsistencies. Setting up an interoperability framework also requires taking into account the requirements of data protection and data security as well as respect fundamental rights.[9]

The interoperability Regulations refer to centralised information systems. A significant part, however, of law enforcement information in the Member States[10] lies completely outside of the scope of any kind of automation or interoperability. Most biographic data is exchanged through traditional request-answer information exchange. This creates a major part of the workload of law enforcement officers handling cases with cross-border dimensions.

As far as further development of EU information systems and interoperability solutions are concerned, there is a need for an assessment of current practices and obstacles from operational, legislative and political perspectives, as well as including the possibilities for improving information exchange through existing channels and information systems such as the 'Prüm Decisions' and the Europol Information System.

There is also a need for an assessment of developing automation and interoperability solutions further: from operational business needs', legal, political and data protection perspectives, as well the possibilities for improving information exchange through existing channels and information systems such as the 'Prüm Decisions' and the Europol information systems.

---

8 Regulations (EU) 2019/817 and (EU) 2019/818

9 11535/19

10 The national fact sheets annexed to the manual on law enforcement information exchange (9346/19 ADD 1 REV 1) set out the scope of information made available by Member States across borders.

Based on the above, COSI is invited to address the following questions:

- Which changes (legal, policy, implementation, best practices) do you consider necessary in order to enhance law enforcement authorities' smooth and more efficient access to information?

- How can we strengthen the link between the national and EU levels when it comes to (criminal) analysis? How can the EU level, especially the EU agencies, best support the Member States in this respect?

- From a strategic viewpoint, how could the automated availability of information across borders be further developed? How should the interoperability of decentralised databases be addressed in the future?