INNOVATIONS IN DATA EXCHANGE FOR LAW ENFORCEMENT TASKS

Ērika Krutova
Dr.iur., Docent of Department of Police Law of State Police College,
e-mail: erika.krutova@koledza.vp.gov.lv, Rīga, Latvia

Abstract. *Information systems are becoming increasingly important in the functioning of law enforcement authorities. In addition to border control in the area, the exchange of information between national competent services is of particular importance. This process is ensured in the European Union through a number of tools, some of which the Schengen Information System, Passenger Name Record, the Europol's Secure Information Exchange Network Application are.*
Legal instruments such as the Prüm Decisions and the Swedish Initiative have been adopted to reduce legal barriers and accelerate the exchange of information between national competent services. However, criminal threats force to reassessment of the effectiveness of existing cooperation and for even more targeted action. Although existing resources and technological capabilities allow information to be searched online, to perform cross-checks for match detection and rapid data exchange, modern options have not been fully implemented yet. The aim of this article is to analyse the existing instruments for information exchange and to assess the novelties of the Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA.
Empirical research methods were used in the study. The author of the study comes to the conclusion that the implementation of the Directive requires significant improvements in national regulation.

Keywords: *information exchange, police cooperation, Schengen information system, Swedish Framework Decision.*

Introduction

In assessing the development of police cooperation, it should be noted that it is still relatively new and has not reached maturity. This is not the case to be accepted where 70% of organised crime groups operate in more than three Member States (Eiropols, 2021).

One of the key elements of law enforcement cooperation is the exchange of information. The European Union Security Union Strategy states that important legal, practical and support instruments and tools have already been introduced, but that they both need to be strengthened and better implemented. Significant progress has been made to improve information exchange and intelligence cooperation with Member States and to close the area where terrorists and criminals operate (Brisele, 2020).

https://doi.org/10.17770/bsm.v4i9.7043

The aim of this article is to analyse the existing instruments for information exchange and to assess the novelties of the Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA. The object of research is the legal regulation of information exchange. The subject of the research is legal innovations in cross-border information exchange in Latvia. To achieve the aim set, the author gives an insight into the current instruments and tools in the field of information exchange, evaluates the existing achievements and provides proposals for the improvement of the legal framework at the national level. Empirical and theoretical research methods are used in the research. Analysis of legal documents, observation, as empirical methods. Axiom method of evaluating, analysing, improving informative material; aperception method, forming a personal judgment based on knowledge, as theoretical research methods.

The study has been carried out since the publication of the European Commission proposal for a Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA. The practical contribution of the article can also apparent in the fact that law enforcement officials will have access to material supporting the development of a common understanding in the field of information exchange.

Information Exchange Tools

The information exchange process covers three important areas: legal basis, information systems/databases, and communication channels.

Information is data or compilations of data, in any technically possible form of fixation, storage or transfer (Informācijas atklātības likums, 1998).

In the context of cross-border cooperation, information at the disposal of one country is relevant in another. National and international law provides a general framework for how such information is to be accessed and for what purposes. This is one of the reasons hindering equal access to information in the same way in the fight against crime.

Looking back at history, the data was initially structured manually, creating files that were replaced by the databases. A structured set of information is called a database. National authorities, in accordance with their competences and functions, establish information sets where data are processed for a specific purpose. The Schengen Information System (hereinafter – the SIS) was set up in the Schengen area, which provides for the free movement of more than 420 million people.

The Schengen Information System is an information system established in accordance with the legislation of the European Union in order to strengthen public order and security in the territory of Member States, ensuring the availability of reports to the competent authorities and institutions of Member States. The SIS is one of the main complementary measures contributing to the maintenance of a high level of security in the area of freedom, security and justice of the Union by supporting operational cooperation of competent national authorities, in particular border guards, police, customs, immigration authorities and authorities responsible for crime prevention, investigation or prosecution of them, or the execution of criminal penalties. The legal framework governing the operation of the SIS and the information exchange processes has been continuously developed through travel from the Convention to the Regulation.

At the national level, the Law on Operation of the Schengen Information System entered into force in 2007, which specifies the procedures for the maintenance and use of the SIS and SIRENE information system in Latvia, institutions and authorities responsible for ensuring of the operation thereof, as well as the functions of these institutions and authorities.

One of the major innovations in the SIS legal framework (Regulation 2018/1861/EU, 2018) provides that Europol will be entitled to access the SIS data and process them. On the other hand, the Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA will not affect the provisions applicable to specific systems, such as the SIS.

At the national level, the police shall cooperate with the police (militia) of other countries, international organisations, unions or communities, and shall also participate in international missions and operations in accordance with international agreements which are binding on the Republic of Latvia (Likums "Par policiju", 1991). On the other hand, cooperation mechanisms and capabilities are not defined together in either this or any other law. It is clear that the situation is similar in other countries, because international rules do not regulate these issues together. Legislation is adopted at different times, regulates the defined scope and differs in legal force. In order to strengthen cooperation, the European Union will adopt the Police Cooperation Code in the near future, one of the key aspects of which is to modernise information exchange processes.

Accession to the European Union and to the Schengen area imposed a number of obligations on each Member State, but these are being met unequally.

The Stockholm Programme provided that the European Union Security Information Management Strategy would be based on development based on

professional law enforcement needs; a strict data protection regime in line with the data protection strategy; targeted data collection to protect citizens' fundamental rights and to avoid over-information to competent authorities; basic principles for information exchange policy with third countries for law enforcement purposes; interoperability and overall coherence of information technology systems (Stokholmas programma, 2010). On the basis of this programme, the structuring of the information exchange model has started, developing the legal framework and adapting the technical possibilities. On the basis of this programme, the structuring of the information exchange model has been launched, developing the legal framework and adapting the technical possibilities. In this respect, it must be agreed that "the creation of formal EU mechanisms for law-enforcement cooperation, however, has not changed the fact that policing within the EU is essentially a national function and that accountability for the conduct of law enforcement is primarily to national governments, legislatures and courts" (McCartney et al., 2011).

Analysing the decisions taken in the European Union, one can conclude that, in most cases, they are based on the principle of availability of information. Law enforcement officials in one Member State of the European Union may, in the performance of their duties, obtain information from another Member State in order to achieve an objective specified. However, Directive of the European Parliament and the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA specifies a number of principles for information exchange:

- principle of availability;
- principle of equivalent access;
- principle of confidentiality (Padomes Pamatlēmums 2006/960/TI, 2006).

The inclusion of new principles in the Directive highlights the problems in the area of the information exchange between Member States.

In 2019 the European Parliament and the Council adopted Regulation 2019/818 establishing a framework for interoperability between the Entry/Exit System, the Visa Information System, the European Travel Information and Authorisation System (ETIAS), EURODAC, the Schengen Information System and the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN) (Regulation 2019/818/EU, 2019).

The need for this Regulation was determined by the need to improve the Union's data management architecture in order to address structural weaknesses that hamper the work of national authorities and to ensure that law enforcement authorities have the necessary information at their disposal. This Regulation introduces new data processing activities aimed at

the correct identification of the persons concerned. These issues will not be addressed in this publication.

The structuring of data management was clearly influenced by the support of the Prüm decisions among Member States. The data exchange under the Prüm Decisions provides for the right of the competent services of the Member States to make requests for information online and to cooperate in the information exchange with their counterparts in other countries.

Back in 2011, studies and researches suggested that forensic DNA profiling and databasing have become increasingly significant resources for criminal investigations in many jurisdictions (McCartney et al., 2011).

The Prüm Decisions aim to promote law enforcement cooperation in the fight against terrorism and cross-border crime. The Prüm decisions introduced the automated information exchange with DNA profiles, dactyloscopic data, vehicle registration data; information exchange on major/significant events; information exchange to prevent terrorist activities, etc. However, in accordance with the procedures laid down at the national level, it is also necessary to draw up separate documents in the execution of these tasks and these arrangements are not uniform in the Member States. The data exchange system operates in a decentralized manner through the national contact points and the conditions for data protection are governed by national laws and regulations. Unfortunately, it has to be noted that there is also a mixed attitude towards automated data processing, with more negativity. This issue cannot be clearly assessed. The public security and the rights of the individual must be assessed. A democratic society plays a role in the public interest. At the international level, the issue of data security in the performance of police tasks is addressed on a hit/no hit basis.

Given that automated access to data is based on a hit/no hit principle or compliance/non-compliance system, it is necessary to ensure and establish procedures at the national level for the competent authorities of the Member States to obtain and exchange part of the coded information. The exchange of such information is intended for the investigation of criminal offences and is necessary for the identification of a natural person. Unfortunately, these facts show that police officers are faced with a dilemma: to carry out or not to carry out an inspection. This is at odds with all the European Union's legal efforts to strengthen police cooperation.

The Prüm system operates on the principle that the requesting country receives an automatic notification for the matching reference and is followed by cooperation on the Swedish Initiative to obtain personal data or other data related to the matching profile. (Padomes Lēmums 2008/615/TI, 2008).

Requesting DNA profiles and dactyloscopic data differs in that the DNA profile cannot be requested to prevent a criminal offence. Dactyloscopic data may also be required for this purpose, as unidentified fingerprints may be found at the scene or a person may need to be identified. Each country has contact points for DNA profile searches, which cannot impose stricter requirements for cooperation with other countries than at the national level.

At the national level, Cabinet Regulation No 620 provides for the procedures by which biological material is collected for the inclusion thereof in the National DNA Database. The information stored in the DNA National Database of the Forensic Service Department can be used to detect criminal offences, search for missing persons and identify unidentified corpses (corpse material).

The DNA profiles and data to be included in the National DNA Database are limited availability information and must be requested by the competent authorities with the consent of the public prosecutor.

On the basis of Cabinet Regulation No 698, investigative institutions have the right to receive information from the National DNA database by applying to the Forensic Service Department with a request approved by the Prosecution Office. The data processing procedure stipulates that requests shall be registered and stored at the Forensic Service Department for five years, as well as a copy of the reply provided shall be kept.

The Prüm Decisions clearly influenced the development of the Biometric Data Processing System (hereinafter – BDPS) at the national level. The Biometric Data Processing Law defines "biometric data" as a set of physical properties of a natural person (digitalized picture of a face, finger (palm) trails or prints). On the other hand, a slightly more detailed definition is provided in another law: "biometric data is personal data after specific technical processing which apply to the physical, physiological or behavioural characteristics of a natural person and allow or confirm the unique identification of that natural person." (Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā, 2019).

It follows that BDPS is a technological platform that provides the operation of several information systems, i.e. Biometric Data Processing System, Fingerprint Information System of Asylum Seekers and the State Border Guard Automatic Fingerprint Identification System.

Internal Regulations No 41 of the State Police of October 30, 2014, "Procedures for Collection and Inclusion of Biometric Data in the Biometric Data Processing System" of the State Police stipulate that the official who collects them shall be responsible for the authenticity and quality of biometric data. The collection of biometric data takes place during an operational action or an investigative action. The dactyloscopic card is sent to the Forensic Service Department that includes the data in the BDPS.

Some amount of vehicle registration data is available for automated online searches. The Information Centre of the Ministry of the Interior has been designated as the contact point for the exchange of vehicle registration data and the Road Traffic Safety Directorate has been established as the co-responsible authority for resolving technical issues.

Member States have agreed to establish and maintain a common system for the exchange of vehicle and driving licence data, known as the "European Vehicle and Driving Licence Information System" (hereinafter – "EUCARIS"). The purpose of EUCARIS is to ensure that the central registers of vehicles and driving licences of the Parties are accurate and secure; to assist in the prevention and investigation of violations and the prosecution of violations of national laws relating to the field of driving licences, vehicle registration and other vehicle-related counterfeiting and criminal offences; to ensure the rapid information exchange in order to increase the effectiveness of the administrative measures taken by the institutions in accordance with the legal and administrative procedures of the Parties. (Par Līgumu par Eiropas transportlīdzekļu un vadītāja apliecību informācijas sistēmu (EUCARIS), 2002).

Unlike EUCARIS, data on vehicle owners, keepers and vehicle insurance are also available under the Prüm Decisions.

…Prüm offers clear benefits for cross-border policing, it continues to present challenges of a technical and scientific nature as well as legal, ethical and socioeconomic concerns (Sallavaci, 2018).

Another system in which air passenger data is stored is the Passenger Name Record. Terrorist threats introduced innovations in the processing of passenger data on international flights, obliging airlines to transfer passenger data to the competent authority for processing. Passenger Name Record (hereinafter – PNR) was established to track terrorist financing programmes by controlling the flow of suspicious financial transactions. Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime provides for the processing of passenger data on external flights for the purpose of prevention, detection, investigation and prosecution of terrorist offences and serious crime and holding criminally liable for them.

The Directive provides for the establishment of a passenger information unit (PIU) in each Member State, which is responsible for collecting, storing and processing data and transmitting the relevant data to the competent authorities, and for exchanging data with other EU countries and Europol. In addition, each Member State shall adopt a list of competent authorities that are entitled to request or receive from the PIU PNR data or the results of the processing of that data in order to further verify that information or to take

appropriate action to prevent, detect, investigate and prosecute terrorist offences or serious crime and to hold criminally liable for them.

At the national level a written request must be made to the court for the location of the authority in order to obtain data from the register.

Finally, it is necessary to describe the contribution of the Swedish Initiative or Framework Decision 2006/960/JHA in the field of information exchange. The aim of the Swedish initiative was to develop rules for the efficient and expeditious exchange of information and intelligence data between law enforcement authorities of Member States in the investigation of criminal offences or collection intelligence data on them. The information and intelligence data shall be provided at the request of the competent law enforcement authority conducting the criminal investigation or collecting the intelligence on a criminal offence in accordance with the powers conferred by national law. Basis for a request of information is detection, prevention, investigation of a criminal offence, if there are factual reasons to believe that the relevant information and intelligence is available in another Member State. The request shall state the actual reasons and explain the purpose for which the information is requested, as well as the link between that purpose and the person who is the subject of the information or intelligence.

At the national level, Council Framework Decision 2006/960/JHA was implemented in 2009 by the Law on the Exchange of Information for the Prevention, Detection and Investigation of Criminal Offences (hereinafter – the Law on the Exchange of Information) (Noziedzīgo nodarījumu novēršanas, atklāšanas un izmeklēšanas ziņu apmaiņas likums, 2009), which lays down the procedures for requesting and providing information to a competent authority. The purpose of the law is to ensure the rapid information exchange between law enforcement authorities of Latvia and other Member States that investigate criminal offences. Cabinet Regulation No 886 of August 1, 2009, "Regulations on the Contents and Layout of Forms for the Provision of Information for the Prevention, Detection and Investigation of Criminal Offences" is subordinated to the Law on the Exchange of Information.

The Framework Decision provides that Member States may not impose stricter conditions than those existing at the national level. Member States must reply within seven days if they have information on the offences subject to the European Arrest Warrant. On the other hand, in urgent cases one must reply within eight hours. In other cases, a response must be provided within 14 days. In cases where it is not possible to reply within the time limit, the reasons for preventing it from being complied with must be stated. Member States should provide information spontaneously if there are grounds for believing that it will assist in the investigation or prevention of criminal

offences which have occurred or may occur in another country.

Evaluations, including evaluations carried out in accordance with Council Regulation (EU) No 1053/2013 (Regulation 1053/2013/EU, 2013), show that Framework Decision 2006/960/JHA is not sufficiently clear and does not ensure a proper and rapid exchange of relevant information between Member States. The evaluations also show that the Framework Decision is of little use in practice, partly because in practice there is no clear distinction between the scope of the Convention implementing the Schengen Agreement and the scope of the Framework Decision (Directive 2006/960 /JHA, 2021)

The Framework Decision provided that any of the existing channels could be used for the information exchange, but there was a request to inform Europol or Eurojust if the information concerned the competence of those institutions.

When exchanging information in response to the Swedish initiative, Member States are not obliged to take any coercive measures to obtain information. Information obtained without the consent of the state may not be used as evidence in criminal proceedings. Information received from a third country may not be shared without its consent.

Conclusions

The assessment that Framework Decision 2006/960/JHA is not sufficiently clear and does not ensure a proper and rapid exchange of relevant information between Member States confirms the need for a change of legal nature.

Framework Decision 2006/960/JHA limits the use of information as evidence in judicial proceedings and this restriction remains also in the Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA.

Directive of the European Parliament and the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA specifies a number of principles for information exchange:

- principle of availability;
- principle of equivalent access;
- principle of confidentiality.

The inclusion of new principles in the Directive highlights the problems in the area of the information exchange between Member States.

The information exchange process covers three important areas: legal basis, information systems/databases, and communication channels.

Member States shall ensure that their single point of contact, as well as any of their law enforcement authorities that may be involved in the information exchange of information under the Directive, are directly connected to SIENA. However, the use of a single channel for all types of information exchange was also not supported by the Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA.

The general presumption in the Directive that the Directive does not apply to the information exchange between law enforcement authorities of Member States for the prevention, detection or investigation of criminal offences specifically governed by other Union laws and regulations is critical. (…) It allows avoiding uncertainty and specification in the information exchange.

On a positive note, Member States shall establish and regularly update a list of one or more official languages of the Union in which their single point of contact may provide information upon request or on its own initiative.

References

1. Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. Official Journal of the European Union. L 210/1, 06.08.2008.
2. Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen. Official Journal of the European Union. L 295, 6.11.2013.
3. EU SOCTA. Europol (2021). From https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf
4. Informācijas atklātības likums. Latvijas Vēstnesis, 334/335, 06.11.1998.
5. Likums "Par Līgumu par Eiropas transportlīdzekļu un vadītāja apliecību informācijas sistēmu (EUCARIS)". Latvijas Vēstnesis Nr.62, 24.04.2002.
6. Likums "Par policiju". Latvijas Republikas Augstākās Padomes un Valdības Ziņotājs, 31/32, 15.08.1991.
7. MCCARTNEY, C.I., WILSON, T.J. & WILLIAMS, R. (2011). *Transnational Exchange of Forensic DNA: Viability, Legitimacy, and Acceptability.* Eur J Crim Policy Res 17, p 305–322. From https://doi.org/10.1007/s10610-011-9154-y
8. Ministru kabineta 2005.gada 13.septembra noteikumi Nr.698 "Noteikumi par DNS nacionālajā datu bāzē iekļautās informācijas sniegšanu". Latvijas Vēstnesis, 147, 15.09.2005.
9. Ministru kabineta 2005.gada 23.augusta noteikumi Nr.620 "DNS nacionālajā datu bāzē iekļaujamo ziņu sniegšanas, kā arī bioloģiskā materiāla un bioloģiskās izcelsmes pēdu izņemšanas kārtība". Latvijas Vēstnesis, 135, 26.08.2005.
10. Noziedzīgo nodarījumu novēršanas, atklāšanas un izmeklēšanas ziņu apmaiņas likums. Latvijas Vēstnesis Nr.51 (4037), 01.04.2009.

11. Padomes Pamatlēmums 2006/960/TI par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu. Oficiālais Vēstnesis L 386/89, 29.12.2006.
12. Par fizisko personu datu apstrādi krimināprocesā un administratīvā pārkāpuma procesā. Latvijas Vēstnesis 147, 22.07.2019.
13. Proposal for a Directive of the European Parliament and of the Council of 8 December 2021 on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA. 08.12.2021, COM(2021) 782 final, 2021/0411(COD).
14. REGULATION (EU) 2019/818 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816. Official Journal of the European Union, L135, 22.05.2019.
15. SALLAVACI, O. (2018). *Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange.* Eur J Crim Policy Res 24, 219–235. From https://doi.org/10.1007/s10610-017-9355-0
16. Stokholmas programma. Oficiālais Vēstnesis C, 115/1, 04.05.2010.
17. Šengenas informācijas sistēmas darbības likums. Latvijas Vēstnesis, 102, 27.06.2007.