DOI: 10.38146/BSZ-AJIA.2024.v72.i9.pp1715-1726

The big law enforcement information exchange challenge

Nikolett Ujfalussy
deputy director, deputy chairperson
Hungarian National Police,
International Training Centre
Management Board of CEPOL
ujfalussy.nikolett@nokitc.hu

Abstract

Aim: The paper attempts to take stock and present the most significant dilemmas and challenges of cross border criminal data and intelligence exchange between law enforcement authorities of EU Member States that can be experienced by police personnel in the field at the moment.

Methodology: In addition to the relevant legislation, recommendations and best practices, the paper – based on personal experience as a police professional, supplemented by insights of the members of the EU law enforcement community – describes and illustrates the various challenges of today's international police cooperation landscape.

Findings: The EU law enforcement information exchange scene is in the midst of its transformation due to globalisation and the progressive information and communication technology advancement. The evolution of the institutionalised cross border criminal data and intelligence exchange has to keep up with the world of crime and reflect the challenges which arise from the sensitive nature of the policy area itself, where any substantial development can only be reached by innovation and capacity building of the law enforcement sector.

Value: This snapshot is to give a structured overview and to draw more attention to the complexity and the controversies of the international law enforcement information exchange landscape, which policy-makers and police professionals have to face nowadays in order to successfully prevent, detect or investigate cross border criminal offences.

The manuscript was submitted in English. Received: 30 May 2024. Revised: 18 July 2024.
Accepted: 23 July 2024

Keywords: Europol, cross border information exchange, capacity building, innovation

Introduction

Before the entry into force of the Lisbon Treaty,[1] police officers involved in the cross border exchange of criminal information felt like members of a small club, ready to cooperate in the spirit of camaraderie and mutual trust. Their standard toolkit consisted of Interpol notices and the alerts of the Schengen Information System (SIS); Europol was their trusted wingman, using 'Swedish Initiative'[2] as an ultimate information exchange guide for police officers.

International information exchange was more of an opportunity than a must, and the privilege of the chosen ones compared to today's reality, where great number of info exchange practitioners feel more like they are on the information superhighway in rush hours.

Then, with the Treaty of Lisbon, the regulatory climate changed and the level of ambition of the EU Justice and Home Affairs (JHA) policy area – hand in hand with the emergence of new types of threats and criminal challenges – significantly increased. The evolution of crime turned international police cooperation into a routine and part of the core business of the central criminal units of the EU Member States.

Europol, with its new legal basis,[3] became a genuine EU information hub playing fundamental role in the fight against cross border serious and organised crime, providing indispensable tools and services and the league of third countries whom it has operational cooperation agreements with. Europol also operates the European Secure Information Exchange Network Application (SIENA), which is more and more often referred to as the 'default channel', as in the new EU Directive on Information Exchange[4] and in the Prüm II Regulation.

Europol has also greatly contributed to the progression of EMPACT[5] into an EU flagship instrument, becoming a multidisciplinary and multiagency operational cooperation tool to fight organised crime at EU level. This integrated approach, which the EMPACT framework provides, including information

1 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007).
2 Council Framework Decision 2006/960/JHA of 18 December 2006.
3 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016.
4 Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023.
5 European Multidisciplinary Platform Against Criminal Threats.

management, innovation and training for EU internal security, enables Member States to carry out their tasks effectively by working together and making the greatest possible use of legal, technical, and educational resources by gaining advantage from both operational and strategic support (Vetter, 2023).

The European Union Strategy to Tackle Organised Crime 2021–2025[6] recognises EMPACT as one of the key tools to tackle organised crime and identifies 'smooth exchange of and timely access to information', 'advanced cooperation frameworks', and 'international cooperation' as priorities.

With its key actions (access to encrypted information, full interoperability, modernisation of the Prüm framework,[7] Revision of the Europol Regulation, including the amendments to the SIS Regulation) it concentrates on the development of the law enforcement information management architecture itself. In conclusion it declares that 'The Union and its Member States need to stay ahead of criminal organisations'.

Based on the pillars of the European Security Union Strategy, by the development of EU information systems (existing and future ones[8]) and by embracing the concept of interoperability[9] of the systems established to use for law enforcement, border management, migration and asylum purposes, the European Union has become a police information superpower by virtue of its databases and other tools, techniques and activities, and a strategic figure of the globalised world of law enforcement (De Buysscher, 2023).

Changing the face of law enforcement information exchange

Law enforcement information and intelligence exchange plays a crucial role in fighting against serious organised crime, particularly in today's interconnected world, where criminal activities can easily cross geographical borders and jurisdictions.

Given the increasing complexity and sophistication of organised crime, there is a clear need for a more refined international response, and for the modernisation of the global intelligence sharing structure and information management

6 Communication on the EU Strategy to tackle Organised Crime 2021-2025 (COM/2021/170 final) is the first EU Strategy dedicated to organised crime since the entry into force of the Lisbon Treaty.

7 Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA, OJ L 210, 6.8.2008.

8 European Search Portal, European Entry/Exit System, European Travel Information and Authorisation System.

9 Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862.

architecture. Technology shapes the law enforcement sector, which changes our approach to international police cooperation (De Bolle, 2023).

EU policy making reacts quickly and constantly to the new policy demands with action plans, legislative proposals and other significant products of the policy process. However, the idea that simply creating a policy – which is itself a challenge – can resolve a crucial issue or address a threat is an illusion. The second act of the challenge starts with policy implementation 'in 3D' where the last resort is the impact assessment and the ultimate enemy is the implementation deadline and the five-year evaluation. The solution is to have a fully-fledged and effectively running product in place that proves to be a well-functioning and unchallengeable tool of cross border law enforcement cooperation.

Generally, it is important to act with moderation, common sense and some degree of fairness when trying to give a policy response to a problem. However, as technology evolves and global connectivity expands, the pace and level of ambition have had to be increased over recent years. The catchphrases of policy making became innovative, dynamic and multidisciplinary.

Hence EU law enforcement nowadays faces a wide range of challenges in exchanging information effectively and securely. These challenges, among others, include ensuring interoperability and data accuracy, guaranteeing timely access to digital evidence, addressing resource constraints, navigating legal and ethical complexities also by outlining reasonable approaches to data retention questions and ECJ rulings, and last but not least, safeguarding privacy and civil liberties, and dealing with increasing cybersecurity threats.

These challenges, which by nature appear in every working silo of the law enforcement sector, need to be mapped and examined in a comprehensive and collaborative way, assessing their potential impact on law enforcement information exchange to exploit possible synergies and share the burden of addressing them.

Snapshot of possible challenges in implementation

1. Privacy and civil liberties

Protecting privacy and civil liberties is a duty and a fundamental challenge for law enforcement, as authorities and EU agencies handle large volumes of personal and sensitive data, processed in cross-border dimension (both at European and international level). Public trust in law enforcement depends on the responsible use of this information, and any breaches of privacy can erode confidence in the system.

By prioritising privacy and civil liberties, the EU is a very attractive and reliable partner to cooperate with when it comes to personal data processing, which is crucial for establishing and maintaining meaningful partnerships and for fostering greater cooperation in preventing and combating crime.

EU law enforcement authorities and agencies implement robust data protection measures to safeguard personal information and prevent abuse. This includes, among others, transparency in data collection, sharing, and usage, data anonymisation, encryption, and access controls to limit who can view and use sensitive data.

The EU's and the MS's independent supervisory authorities and oversight mechanisms supervise the lawfulness of personal data processing and monitor information exchange practices.

Due to the flow of incoming data, new types of processing operations have to be established and approved, and potential privacy concerns have to be addressed real-time in close association with law enforcement specialists. When reinforcing safeguards and monitoring of compliance with data protection standards, it is necessary to reflect the new challenges for law enforcement.

2. Legal complexities

One major challenge lies in navigating legal and ethical complexities that arise from the diverse legal frameworks and data protection laws across different jurisdictions. As crime becomes increasingly transnational, cooperation between law enforcement agencies from various countries becomes essential. However, this cooperation is often hindered by differences in legal standards, data privacy laws, and evidence collection procedures.

For instance, some jurisdictions may have stricter data protection regulations that limit the sharing of personal information, while others may have more lenient laws that allow for broader information exchange. These differences can lead to delays and challenges in sharing crucial information for investigations.

Moreover, legal dilemmas arise when balancing the need for effective crime prevention with the protection of individual rights and with single market interests. A textbook example of this challenge is the question of communications data retention[10] schemes in the EU.

Law enforcement authorities and agencies must ensure that their information exchange practices are in compliance with legal and ethical standards, while

10 Data retention constitutes a limitation of the right to private life and the protection of personal data which are fundamental rights in the EU.

respecting privacy and civil liberties. To address these complexities in practice, clear guidelines and protocols for day-to-day information sharing need to be established to align legal standards and data protection measures.

3. Interoperability and data accuracy

Data accuracy and interoperability are critical components of effective law enforcement information exchange. Inaccurate or inconsistent data can lead to flawed investigations, wrongful arrests, and miscarriages of justice.

Ensuring data accuracy requires robust data validation and verification processes to confirm the reliability of information before it is shared or used in investigations. To enhance data quality and interoperability, law enforcement policy area invested in the past (e.g. SIS) and should invest in the future (e.g. ETIAS[11]) in standardised data formats and protocols (e.g. UMF[12]) as a part of the newly developed interoperable systems.

Although working in silos for interoperability is one of many contradictions big systems suffer from, it also delays or hinders reaching the goal of establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration.

Moreover the 'big data' itself brings its very own set of challenges, frequently referred to as the '4 Vs' for Volume, Velocity, Variety and Veracity (referring to the quality and reliability of the data). The volume of big data itself represents significant challenges for organisations, as large amounts of data need to be stored, processed and analysed. Handling such large amounts of data requires new storage (distributed computing systems and cloud-based storage solutions) and processing solutions, however ensuring data quality, governance and security remain key issues in realising the value of big data.

At the very moment when the interoperability and synergies between European databases in the area of Justice and Home Affairs will become not just a legal but a practical reality the big data problem will be turning from a hypothetical into an everyday challenge of the law enforcement community which can only be solved by the highest possible level of automation.

4. Cybersecurity threats

As technology advances, cybersecurity threats pose significant risks to law enforcement, and additional risks to international information exchange. Criminal

11 European Travel Information and Authorisation System.
12 Universal Messaging Format.

organisations and malicious actors may target law enforcement systems to steal data, disrupt operations, or gain unauthorised access to sensitive information. Cyberattacks such as ransomware, phishing, and data breaches can compromise the integrity of information exchange potentially discrediting the authorities and agencies involved.

Developing effective cybersecurity strategies, including early warning and crisis communication plans, is essential for maintaining the integrity of information exchange and avoiding data breaches, cyberattacks, and other forms of digital crime hand in hand with robust security measures, such as implementing firewalls, intrusion detection systems, and encryption to protect data and systems from cyber threats.

Information about suitable or new means of tackling harmful content is important not only for the specialists in the field, but for practically every end-user so that they can do their best to respond appropriately and as effectively as possible to new dangers.

Additionally, from a MS point of view, it seems necessary to collaborate with technology providers to conduct regular security audits and vulnerability assessments to identify and address potential weaknesses. Cybersecurity experts and private sector partners can also play a crucial role in staying ahead of emerging threats and in developing effective defence protocols and strategies. An improperly managed cybersecurity incident can and will impede effective information exchange for a long time.

5. Resource constraints

Resource constraints can limit the ability of law enforcement agencies to adapt to emerging challenges in information exchange. Adequate funding, training, and technological infrastructure are essential for MS authorities and EU agencies to leverage advanced tools and techniques for effective information sharing, and to stay ahead of criminal networks instead of more and more often having the minimum viable infrastructure in mind.

Budget limitations may hinder the adoption of new technologies and the recruitment of skilled personnel to manage information exchange processes. Additionally, lack of training can also block the effective use of advanced systems and tools.

To overcome resource constraints, law enforcement agencies should explore opportunities for collaboration and resource sharing with other agencies and organisations. This may include joint training programs, shared technology infrastructure, and cooperative funding initiatives.

Moreover, agencies should advocate for increased funding and resources to support their information exchange efforts and enable them to meet the challenges of an evolving crime landscape.

For that reason, it is extremely important for the European Commission and other EU institutions to gear policy-making far more strongly towards the operational reality of law enforcement professionals, and to demonstrate that the European Union is taking account and accurately planning and providing the resources needed for fulfilling their mission.

Combined with globalisation, fast technological change has a great impact on societies and extreme implications for Justice and Home Affairs policy area. The technological white whale pushes policing to raise Europe's research performance and keep the European Information Communication Technology (ICT) sector at the forefront of technology development. Advanced ICT use requires that the Justice and Home Affairs policy area continues to keep up to date with technological progress.

It is essential to prioritise the financing of investments to benefit from technological development across various thematic areas corresponding to major fields of knowledge and technology progress, where research must be supported and strengthened to address European law enforcement challenges.

For the law enforcement sector, the silver linings in the field of innovation, are the Europol hosted entities, such as the EU Innovation Hub for Internal Security, the Europol Innovation Lab and the related initiatives enhancing EU Community engagement with them.

Europol hosts the EU Innovation Hub for Internal Security, which is a collaborative network of European innovation labs aimed at ensuring coordination and possible collaboration between EU actors (e.g. law enforcement, justice, fundamental rights, border management, migration, customs) in the field of innovation on internal security.

The EU law enforcement community itself is supported by the Europol Innovation Lab in the area of innovation. It provides a structure and a set of services to law enforcement authorities to avoid redundancies, duplication of work. It also creates synergies and pools of resources to support innovative solutions aiming at improving operational investigative and analyst work.

The purpose of the related initiatives newly formed in November 2020 is to facilitate the involvement of the Member States and the Schengen associated countries in the work of the Europol Innovation Lab, by creating working groups on operational level, in order to promote cooperation in research, innovation and development issues. Its mandate to ensure that law enforcement agencies are adequately prepared to face the latest technological challenges, trends and threats to conduct criminal investigations, is more than ambitious.

Training systems need to be tuned real-time to the rapidly changing needs of the field, the technological development and new approaches to the organisation of work.

Conclusion

The exchange and analysis of information function, along with its organisational, technical and operational environment and characteristics, has changed a lot in the recent decades and currently is in the midst of transformation, which presents complex challenges to EU and MS regulators, policy makers and, last but not least, law enforcement practitioners. By investing in standardised data formats, interoperable systems, robust security measures, and adequate training, law enforcement authorities and agencies are predestined to enhance their information exchange capabilities.

Although the fact that the principles and the methodology of the new EU Directive on Information Exchange, which has to be transposed into national law by 12 December 2024, closely resembles the spirit and the aim of the Swedish Framework Decision, shows that the EU law enforcement sector has something of a track record in adopting ambitious targets, which have so far proved difficult to achieve and long-standing accumulated obligations to fully and correctly implement existing instruments on which they once agreed.

While it seems indisputable that due to globalisation and to the progressive advancement of information and communication technology, further transformation is needed and expected, the question is how the European Union and the Member States themselves provide the necessary means of resources for the EU agencies and the national authorities to race against the clock with acquiring appropriate new technology and taking on the necessary modifications on the information management architecture and on the daily routine of the international law enforcement cooperation.

Ultimately, overcoming these challenges requires a comprehensive and collaborative approach that prioritises addressing the resource constraints of the law enforcement field both on EU and national level to strengthen the ability of law enforcement authorities and agencies to effectively combat crime, protect public safety and maintain trust in the justice system.

And this is not impossible, the Digital Services Act[13] might serve as a shining example of the right way forward to exchanging and sharing data between

13 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

private parties (Very Large Online Platforms – VLOPs, Very Large Online Search Engines – VLOSEs) and law enforcement authorities and agencies.

This instrument encapsulates the ambition but also the operational possibility to swiftly react to imminent threats and dangers while fundamental rights of all users of the different services are protected.

References

Vetter, D. (2023). Az EMPACT szerepe a kiberbűncselekmények elleni küzdelemben [Role of the EMPACT in the fight against cybercrime]. *Belügyi Szemle, 71*(8), 1331–1346. https://doi.org/10.38146/BSZ.2023.8.1

De Buysscher, P. (2023). 100 Years of INTERPOL: its Position and Role within the European Union. *Belügyi Szemle, 71*(SI3), 7–80. https://doi.org/10.38146/BSZ.2023.11.6

De Bolle, C. (2023). A Glimpse at International Police Cooperation. *Belügyi Szemle, 71*(SI3), 21–28. https://doi.org/10.38146/BSZ.SPEC.2023.3.2

Laws and regulations

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025 COM/2021/170 final

Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Members States of the European Union

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU

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

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community

Reference of the article according to APA regulation

Ujfalussy, N. (2024). The big law enforcement information exchange challenge. *Belügyi Szemle*, *72*(9), 1715–1726. https://doi.org/10.38146/BSZ-AJIA.2024.v72.i9.pp1715-1726

Statements

Conflict of interest

The author has declared no conflict of interest.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Ethics

No dataset is associated with this article.

Corresponding author

The corresponding author of this article is Nikolett Ujfalussy, who can be contacted at ujfalussy.nikolett@nokitc.hu.