Council of the European Union

Brussels, 13 April 2023
(OR. en)

8281/23

LIMITE

COSI 58
ENFOPOL 167
IXIM 86
CATS 21
COPEN 113
CYBER 83

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	WK 4651/23
Subject:	Scoping paper for the High-Level Expert Group on access to data for effective law enforcement

Delegations will find in the Annex the scoping paper for the High-Level Expert Group on access to data for effective law enforcement. The document takes into account the discussions at the informal COSI meeting on 30 March 2023 and the written comments received from delegations after the meeting. Additions to the previous version (WK 4651/23) are marked in **bold underlined,** deleted text is marked in ~~strikethrough~~**.**

HIGH-LEVEL EXPERT GROUP

ON ACCESS TO DATA FOR EFFECTIVE LAW ENFORCEMENT

SCOPING PAPER

1. INTRODUCTION

In today's digital age, almost every criminal investigation has a digital component. Technologies and tools, including those that are necessary to guarantee our society's need for cybersecurity, data protection, privacy, and other fundamental rights, such as freedom of speech, association and to conduct business are also abused for criminal purposes.

This development makes it increasingly challenging to maintain effective law enforcement[1] across the EU to safeguard public security and to prevent, detect, investigate, and prosecute crime, and to meet victims' legitimate expectations of justice and compensation. If not properly addressed, there is a real risk that this current trend will enable criminals to go 'dark', by creating online safe havens of impunity, where anonymity of criminals is guaranteed at the expense of victims and potential victims of crime. This is a serious threat to individuals' and society's security and can ultimately impede on the positive obligation of the state to continue ensuring the rule of law and a democratic society.

Significant efforts, including legislation as well as capacity building and innovation initiatives, have already been undertaken at the EU and at national level to address these challenges. However, the necessary access by law enforcement to data to perform their tasks remains significantly hampered by both legal and technical challenges, such as a patchwork of different jurisdictions and rules, end-to-end encrypted communication, anonymisation techniques and the dark web. More should be done to build up a stronger common understanding between key actors across various sectors of the need to ensure all the necessary conditions and safeguards to uphold the rule of law and give justice in the digital age, including cybersecurity, privacy, and internal security due considerations as part of a comprehensive approach.

[1] Law enforcement is understood as a public function in broad sense including all public authorities in the criminal justice system.

To contribute to the further consolidation of an effective Security Union, the European Commission, associating the Presidency of the Council of the European Union, will set up a High-Level Expert Group (HLEG) on access to data for effective law enforcement, based on and guided by the inputs from the EU Member States, as submitted through the Standing Committee on Operational Cooperation on Internal Security (COSI).

2. OBJECTIVES, PRINCIPLES AND EXPECTED OUTCOMES

The High-Level Expert Group will be tasked to explore the problems that law enforcement **practitioners** face in their daily work, and to define potential solutions to overcome them, with the aim of ensuring the availability of effective law enforcement tools to fight crime and enhance security in the digital age. Specific focus will be on the need for law enforcement practitioners to have adequate access to data.

The objectives of the High-Level Expert Group will be to:

- Establish a **collaborative and inclusive platform** for stakeholders from all relevant sectors, including law enforcement, data protection experts, private sector operators, NGOs, and academia, to overcome silos and work towards commonly accepted solutions.

- Formulate a **strategic forward-looking vision** on how to address current and anticipated challenges against the background of technological developments, enabling a comprehensive EU approach to ensure access to data for effective law enforcement.

- Propose **recommendations** for the further **development of Union policies and legislation** to enhance and improve access to data for the purpose of effective law enforcement. In this context: contribute to integrating a law enforcement perspective, including privacy and data protection requirements, in all relevant EU policies and actions (‘security by design’).

The HLEG's objective of enhancing security in the digital age shall be pursued **in full compliance with fundamental rights**. This is not only a legal requirement but also an opportunity to produce better operational outcomes. The objective of ensuring public security, can only be attained in full respect of the EU Charter for Fundamental Rights, and fundamental rights proscribed therein. The HLEG will demonstrate that security can be effectively strengthened whilst being in full compliance with the highest data protection and justice standards and safeguards. The concept of 'security by design' *i.e.*, combining access by design and privacy by design is important in this context and will be explored to the full.

The HLEG will **build on existing work** and benefit from synergies with existing structures and fora related to access to data, such as the work done by the Council preparatory bodies, the Joint Research Centre (JRC), the EU Internet Forum, the EU Innovation Hub for Internal Security, FRA's research, ENISA's work on cybersecurity and the Commission's work on the way forward on encryption. The High-Level Expert Group will not only map the current situation and identify possible needs and solutions but also explore ways to better support the implementation of existing and proposed measures, building on the recent achievements made at EU and national level.

In its overall approach, the HLEG will systematically address the following questions:

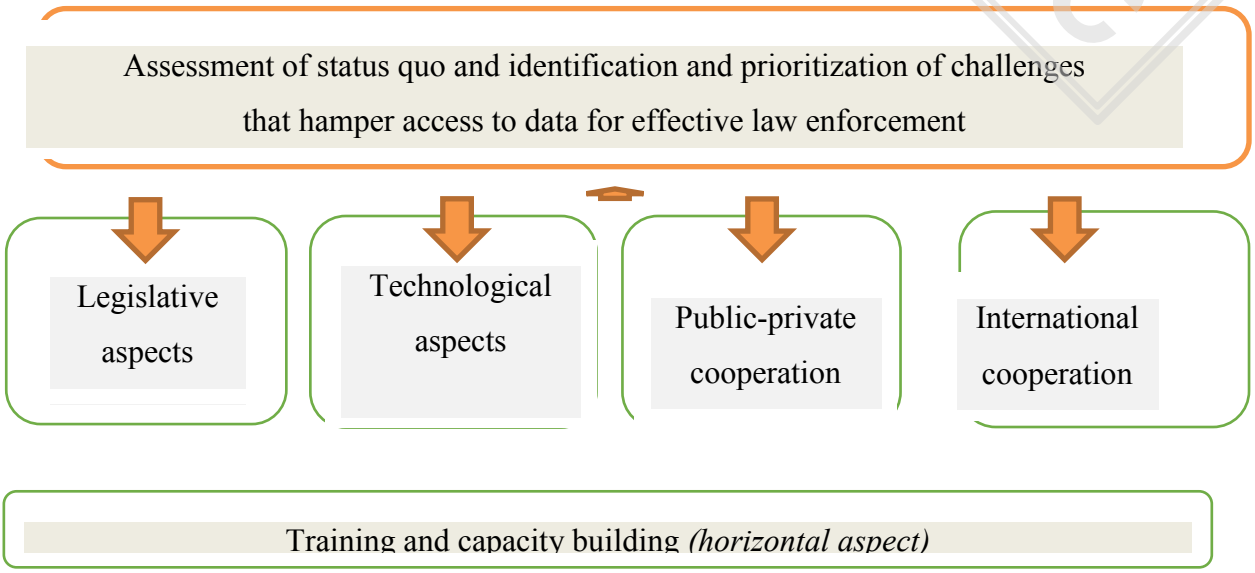
1. *What is the current situation?* The HLEG will take stock of what exists, what works and what does not work. It will invite law enforcement practitioners to present their success stories, but also their failures to overcome certain obstacles and challenges.

2. *What are the main problems that need to be addressed?* The HLEG will examine the key issues and critical challenges that require a consolidated response at EU level.

3. *What solutions should be considered / proposed?* The HLEG will identify a possible way ahead, including further measures at the operational, technical, political and/or legal level.

3. WORK STREAMS

The High-Level Expert Group will map, assess, and prioritize the relevant issues that will be examined through various work streams. It will identify, in a comprehensive manner, the **legal, technical, and operational challenges,** both current and potential future ones, and assess the practical impact of the lack of access to data on law enforcement's ability to perform their function. It will also look at the selected issues from the angle of cooperation, both between public and private stakeholders, and between countries.



During the preparatory discussions amongst Member States, the following challenges were identified as most pressing ones.

- Encryption (access, *en clair,* to stored content and digital communication data);
- Data retention;
- Localisation data and roaming data;
- Anonymisation, including VPN and Darknets

More challenges may be identified throughout the above process.

a) Legislative aspects

The HLEG will assess the legal framework currently available to law enforcement at the EU level, and the EU *acquis* as it currently stands, as well as the need for common EU solutions for access to data, legislative or otherwise.

Furthermore, the High-Level Expert Group will assess the appropriateness and the interplay between past and ongoing EU legislative proposals that have a bearing on the law enforcement's ability to perform their functions in a digitalised society, including their legal basis.

Respect for and protection of fundamental rights as enshrined in Article 2 of the Treaty of the European Union are unconditional and essential components of effective law enforcement. The protection of both individual and collective security touches upon several fundamental rights and freedoms, including, but not limited to the right to life, physical integrity, liberty and security, respect for private and family life and protection of personal data, and freedom of expression and association.

The High-Level Expert Group will assess the interaction between the various fundamental rights at play that set up the safeguard framework for law enforcement access to data in the performance of their duties. The High-Level Expert Group will address the issue from the perspective of the victims of crime and the protection of potential victims.

b) Technological aspects

Technology shapes security challenges and responses in the EU. Law enforcement must engage in foresight activities to understand emerging challenges, formulate innovative countermeasures and, where necessary, challenge established business models and embrace organisational change to keep pace with technological developments. As foreseen by Europol in its report on new technologies and future threats,[2] emerging technologies such as Artificial Intelligence (AI), quantum computing, 5G, the Internet of things and cryptocurrencies have already proven to have a major impact on the capacity of law enforcement to investigate crime in the digital realm.

Several structures and initiatives have been set up to develop foresight capabilities and to mobilise EU funds to cover research gaps and a better uptake of innovation[3]. However, a lot remains to be done to anticipate the impact of new technologies on law enforcement.

In particular, the High-Level Expert Group will explore how security by design could be a standard requirement in the development of new technologies. This would notably imply reflecting on an increased participation of law enforcement representatives in relevant international standardisation bodies such as CEN/CENELEC, ETSI or 3GPP.

c) Public-private cooperation

Consumer behaviour regarding communication services is changing, leading to an increased use of non-traditional communication services. Digital data held by private parties is essential to nearly all criminal investigations into any crime area. User data that is not publicly available, such as connection logs, IP addresses, contact details or payment data, may be key elements for competent authorities to investigate and prosecute criminal offences or save lives in imminent danger. Cooperation with private parties is therefore the key to effective investigations.

Considering that non-traditional communication providers increasingly hold large amounts of information vital to law enforcement, the High-Level Expert Group will assess how to strengthen effective public-private cooperation with necessary safeguards in place.

---

[2] https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf

[3] Such as the EU Innovation Hub for Internal Security, the Innovation Lab of Europol supported by the EU Clearing Board as well as specialised networks of practitioners including Cyclopes in the area of digital investigations, EACTDA for the development of tools or ECTEG for the development of trainings contribute significantly to address the gaps.

The High-Level Expert Group will also assess the availability and appropriateness of the legal framework in view of the changing nature of service providers in the area of electronic communications.

d) International cooperation

Given the global and borderless nature of the Internet, requesting data from service providers often requires engaging with legal entities based abroad. Efforts to improve cross-border access to electronic evidence for criminal investigations are undertaken around the globe, at national, at European Union[4] and at international level[5], namely by introducing alternative mechanisms to the existing international cooperation and mutual legal assistance tools, in the form of direct cooperation with the service providers.

The High-Level Expert Group will assess the current framework and operational practices when it comes to multi-jurisdictional investigations. The High-Level Expert Group will also assess their interplay and the resulting regulatory landscape.

***

In addition to the challenges already described, law enforcement authorities are not sufficiently equipped in tackling the current scale of cybercrime as a mass phenomenon. To keep pace with fast developing technologies used by criminals, there is a clear need to step up **coordination in developing tools and training**, among Member States and across sectors, in areas such as digital forensics, open-source intelligence, cryptocurrencies, and dark web investigations.

4 Such as the internal EU e-evidence package.

5 Such as the Second Additional Protocol to the Budapest Convention, EU-US agreement on e-evidence and the discussions in the UN ad hoc committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

Moreover, there is a pressing need to step up the capacity of non-specialised law enforcement services. Today, every law enforcement officer and prosecutor need to know the basics of how to investigate crime online, because close to every crime today has an online component. Yet law enforcement struggles to cope with the number of devices seized for analysis, with investigating cases and providing assistance to victims of online crime. This contributes to a pervasive sense of impunity for online crime, which erodes the trust of citizens in the ability of authorities to enforce the law in cyberspace.

4. ORGANISATIONAL ASPECTS

The working method of the High-Level Expert Group will aim at synergizing all relevant experiences and assessments, which in the past were often developed and discussed in silos. To this end, the High-Level Expert Group will be composed of high-level representatives of the EU Member States and the European Commission, relevant EU bodies and agencies (including Europol, Eurojust, ENISA, the EU Agency for Fundamental Rights and CEPOL), the Joint Research Centre of the Commission, and the EU Counter Terrorism Coordinator.

The European Parliament and the European Data Protection Supervisor will be invited as permanent observers to advise and support the work of the High-Level Expert Group.

The General Secretariat of the Council will also be invited to attend the meetings of the group as a permanent observer.

Non-institutional stakeholders, such as representatives of academia, non-governmental organisations, and industry (*e.g.*, cybersecurity, telecommunication operators and service providers) will be invited to take part in the work of the group on an *ad hoc* basis and contribute with specific expertise to the overall objectives of the High-Level Expert Group.

The High-Level Expert Group will be co-chaired by the European Commission (Deputy Director General for Security in DG HOME) and the Member State holding the rotating presidency of the Council of the European Union, supported by a Secretariat in DG HOME.

The High-Level Expert Group will draw on existing expertise. It will take account of relevant findings from research, the work of EU law enforcement expert networks and previous discussions in relevant Council configurations and the European Parliament. Where necessary, to complete its picture of the current situation, the group may also conduct its own analysis (e.g., through questionnaires to Member States' practitioners)

The work of the High-Level Expert Group will be carried out at two levels: (1) the High-Level Expert Group itself, meeting in plenary sessions, which will be tasked to provide the overall policy vision and define and agree on conclusions and recommendations; and (2) dedicated working groups to examine specific questions identified by the High-Level Expert Group.

The working groups will enable deeper discussions on specific topics in a more restricted format (tentatively around ten Member States experts per working group, supplemented by representatives of relevant EU agencies, other EU stakeholders, and other experts). Participants in these working groups will be nominated/selected based on proven expertise and experience, with an appropriate balance between the various stakeholders. The working groups will receive guidance from the High-Level Expert Group and will report to the High-Level Expert Group.

To feed and facilitate discussions of the High-Level Expert Group, the Secretariat will prepare, in cooperation with the Presidency, discussion papers and/or background documents for each of the meetings. The co-chairs may also invite other members of the High-Level Expert Group to contribute in writing to the proceedings of the group.

All meetings will in principle take place in person. Online or hybrid meetings are not envisaged.

5. TIMING

The lifespan of the High-Level Expert Group is envisaged to be one year with the possibility of extension, from June 2023 to mid-2024.

The tentative timing of plenary meetings is as follows:

June 2023 – **plenary meeting 1** – inauguration of the process, presentation, and discussion of the challenges, agreeing on priorities to be addressed by the various working groups, potential solutions and expected outcomes.[6]

October/November 2023 – **plenary meeting 2** – taking stock of the first round of reports from the working groups, identifying possible connections or overlaps, and adjusting or confirming the way forward.

February/March 2024 – **plenary meeting 3** – taking stock of the second round of reports from the working groups, drawing connections between work strands and topics, and providing guidance on additional work required to facilitate conclusions.

June~~/September~~ 2024 **(or possibly later in 2024) – plenary meeting 4** – closure of the process, agreement on the conclusions, recommendations and way forward.

Following the last meeting of the High-Level Expert Group, the Commission will prepare a report to the Council and the European Parliament. The report will present the main findings of the High-Level Expert Group and propose concrete actions for follow-up.

The High-Level Expert Group will regularly inform COSI, CATS and other relevant working formats of the Council, and the LIBE Committee of the European Parliament of the progress of its work.

---

[6] The key issues and critical challenges for law enforcement in the digital age that require a consolidated response at EU level will be prepared ahead of the first plenary meeting by COSI/Presidency with the purpose of ensuring a shared understanding of the problem.