High Level Group Recommendations on Law Enforcement Data Access

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

On 15 November 2024, the High-Level Group on access to data for effective law enforcement (HLEG) published its concluding report. The concluding report outlines possible solutions on how law enforcement authorities (LEAs) can overcome challenges in their daily work in connection with the access to data to prevent and fight crimes and to enhance public security in the digital age. The HLEG was established in 2023 in order to support the Commission and the Council in defining the future EU policy and legislation regarding adequate law enforcement access to data (→ eucrim news of 12 March 2024).

Basis: the recommendations of spring 2024

The concluding report builds on 42 recommendations that the HLEG presented in spring 2024. The recommendations addressed current and anticipated challenges in view of technological developments, such as problems for LEAs in accessing data in a readable format for criminal investigations. The recommendations aimed at enabling a comprehensive EU approach to ensure effective criminal investigations and prosecutions and were clustered in three blocks:

- Capacity building;
- Cooperation with industry and standardisation;
- Legislative measures.

The main points in the concluding report

The concluding report seeks to give more impetus on how the recommendations could be operationalized, and to provide a clear and concise narrative on access to data for law enforcement. The report summarises the key challenges for lawful data access in the context of criminal investigations and prosecutions. In addition, it describes the main issues of and possible solutions for the three workstreams that guided the HLEGs mandate:

- Digital forensics;
- Data retention;
- Lawful interception.

Digital forensics refers to the collection, analysis and preservation of digital evidence (both communication metadata and content data) stored in any digital form on an electronic device, including information from computer hard drives, mobile phones, smart appliances, vehicle navigation systems, electronic door locks,

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2024, Vol. 19(4) eucrim pp 270 – 271
ISSN: 1862-6947
https://eucrim.eu

data stored in the cloud and other digital devices. As far as digital forensics are concerned, the HLEG points out that LEAs must boost their resources, skills and technical solutions with regard to accessing encrypted data. In this context, there is a need for more effective cross-border cooperation by sharing expertise, developing standardised tools and procedures, and pooling resources. Next to such capacity building measures, LEAs must be enabled to have access to data in a readable format under clearly regulated circumstances, which would be a more sustainable long-term solution.

Looking at data retention, i.e. the collection of potential evidence stored by communication providers in the form of metadata, the HLEG advocates a harmonised and consistent legislation "which complies fully with fundamental rights". Given the rapid advancement of technologies, law enforcement's timely access to relevant data stored by providers is becoming "increasingly valuable". The report outlines in particular that access to said metadata is essential for identifying suspects and understanding their activities.

With regard to lawful interception, which relates to the access to the content of a communication, a major issue is, according to the HLEG, the shift from traditional communication providers to "over-the-top (OTT) services" and the fact that criminals are increasingly moving to end-to-end encrypted platforms. Therefore, lawful access to communications in real time requires an assessment of the need for clear rules for cooperation between LEAs and technological companies. In addition, enhanced cooperation at EU level in order to facilitate cross-border requests is needed.

Reactions by the Council

On 13 June 2024, the Home Affairs Ministers of the EU Member States held an exchange of views on the HLEG's 42 recommendations at the JHA Council meeting. They welcomed the recommendations and identified the following three priority areas of work that should be addressed during the next legislative term: (1) a harmonised EU legal framework for data retention, (2) the establishment of rules for access to data pertaining to interpersonal electronic communication, and (3) legally and technically sound solutions to access encrypted electronic communication in individual cases and subject to a judicial order for the purpose of preventing, investigating, and prosecuting serious and organised crime as well as terrorism.

At the Council meeting of 12 December 2024, the Home Affairs Ministers discussed the next steps after the HLEG finalised its work by the concluding report. In its conclusions on access to data for effective law enforcement, the Council called on the Commission to present, by the first half of 2025, a roadmap for the implementation of concrete measures to guarantee access to data for effective law enforcement, "taking into account the relevant case law of the Court of Justice of the EU and with full respect for fundamental rights." The Ministers stressed that the matters raised by the HLEG should be treated with urgency and the needs of law enforcement to ensure public security should be explained "through a common communication narrative". The committees COSI and CATS are tasked with coordinating, discussing and monitoring the implementation of the envisaged roadmap prepared by the Commission.

Reaction by data protection experts

On 4 November 2024, the European Data Protection Board (EDPB) issued a statement on the HLEG's 42 recommendations. The EDPB casted doubts whether all measures suggested by the HLEG would be compliant with the Charter of Fundamental Rights of the EU, especially the right to data protection and the respect for private and family life, given their potential serious intrusiveness. The EDPB criticised, for instance, the fact that the recommendations are not complemented and supported by objective evidence, including, where relevant, statistics, which makes it difficult to assess the necessity and proportionality of certain proposed measures. The EDPB also raised specific concerns over the HLEG's position on data retention. With regard to data security and encryption, the EDPB emphasised that "preventing the use of encryption or weakening the

effectivity of the protection it provides, would have a severe impact on the respect for private life and confidentiality of users, on their freedom of expression as well as on innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide."

Reaction by civil society

On 11 December 2024, 55 associations and organisations from civil society voiced concerns over the HLEG's recommendations and concluding report in an open letter to the Justice and Home Affairs Council. In light of the HLEG's overall aim to grant law enforcement authorities maximal access possible to personal data, the associations/organisations identify important risks of mass surveillance as well as substantial security and privacy threats, if these recommendations were taken as a basis for future EU policies and legislation. Among other things, the associations/organisations recommend the following to policy makers:

- Discarding any measure that may bypass the protections afforded by encryption or weaken them, as it would create security and privacy threats to millions of people, public institutions and inevitably damage the broader digital information ecosystem;
- Giving up the plan to extend the data retention obligation, because this would generate in people's mind the feeling that their private life is the subject of constant surveillance and cannot be considered compliant with the legal requirements;
- Guaranteeing that any measure respects professional secrecy;
- Not accepting "backdoor mechanisms" for law enforcement, which can always be exploited by other actors, as numerous examples have shown.

Lastly, the open letter criticised the HLEG's outline of the enforcement framework, including harsh sanctions to deter and punish non-compliance with EU obligations and law enforcement orders (administrative sanctions, commercial ban, imprisonment). This would risk either driving reliable operators offering secure services out of the EU market or out of business if they are small or not-for-profit, or preventing them from developing secure solutions if established in the EU. In addition, such approach would be highly detrimental to the EU's cybersecurity initiatives and ambitions. In sum, the civil society associations/organisations are of the opinion that the law enforcement objectives of general interest can be met with less intrusive measures than mass surveillance and systemic weakening of essential security guarantees.

The critical voices show that the Commission is now in a delicate position. On the one hand, it has to implement the Council's mandate to lay down concrete proposals on "adequate" law enforcement access to data, while on the other, there are still many questions regarding the protection of fundamental rights, in particular the right to privacy and data protection. With the presentation of the roadmap envisaged for the second quarter of 2025, the discussion will pick up speed again.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union