EUROPEAN
COMMISSION

Brussels, 24.6.2025
COM(2025) 349 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Roadmap for lawful and effective access to data for law enforcement

Introduction

As set out in the European Internal Security Strategy ('ProtectEU')[1], **security is the bedrock on which all our freedoms are built**. Democracy, the rule of law, fundamental rights, the well-being of Europeans, competitiveness and prosperity – these all hinge on our ability to provide a guarantee of basic security.

The EU and Member States have a duty to ensure that citizens can enjoy a **high level of security in their daily life**. For that purpose, law enforcement and judicial authorities need to have the necessary tools to track illicit activities, identify perpetrators, dismantle criminal networks and protect victims, ultimately ensuring criminal justice, in full respect of fundamental rights.

Terrorism, organised crime, online fraud, drug trafficking, child sexual abuse, online sexual extortion, ransomware and many other crimes have something in common: they leave **digital traces**. As Europol observes in its Serious and Organised Crime Threat Assessment (SOCTA) for 2025, nearly all forms of serious and organised crime have a digital footprint[2]. **Today, around 85% of criminal investigations rely on electronic evidence**[3]. Requests for data addressed to service providers have tripled between 2017 and 2022, and the need for these data is only increasing[4].

While we have recently seen remarkable examples of law enforcement and judicial authorities successfully cracking down on dedicated criminal communications networks[5], many more investigations are **delayed or unsuccessful due to a lack of timely access to digital evidence[6].** Law enforcement and the judiciary have been losing ground to criminals over the past decade as criminals use tools and products from service providers that have put in place measures preventing cooperation with lawful requests[7].

Critical criminal evidence remains inaccessible because it[8]:

- **is deleted** by service providers within days, in line with their obligations for the protection of personal data and privacy or their business needs;
- **cannot be obtained** due to conflicts of laws between jurisdictions, as different countries have varying laws and regulations regarding data access, making it difficult to obtain data stored abroad;
- **cannot be retrieved from devices seized in criminal investigations** because **digital forensics** is difficult if not entirely impracticable;
- **cannot be read** because the data are encrypted;

---

[1] EUR-Lex - 52025DC0148 - EN - EUR-Lex

[2] European Union Serious and Organised Crime Threat Assessment 2025 EU-SOCTA-2025.pdf.

[3] Commission Impact Assessment on the Proposals for an e-evidence Regulation and an e-evidence Directive (17 April 2018) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:EN:PDF.

[4] 2023 SIRIUS Report, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, p. 69.

[5] Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized | Europol joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf / Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe | Europol.

[6] Reported by the High-Level Group (HLG) on access to data for effective law enforcement - European Commission.

[7] Concluding report of the High-Level Group on access to data for effective law enforcement (15 November 2024).

[8] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust.

- **cannot be effectively and lawfully analysed** because of the lack of suitable technologies or sufficient human resources to effectively filter and analyse large quantities of seized data without impinging on the EU and Member States' legal frameworks.

In response to these challenges, a **High-Level Group on Access to Data for Law Enforcement** (High-Level Group) was set up in 2023, delivering a set of 42 recommendations in May and November 2024. The **EU Justice and Home Affairs Council** endorsed the recommendations of the High-Level Group[9] on 13 June 2024, and later, in December 2024, adopted conclusions calling on the Commission to draw up a roadmap. The roadmap was to be based on the work of the High-Level Group and its recommendations for putting in place measures to ensure lawful and effective access to data for law enforcement[10]. This Communication responds to that call.

As digitalisation becomes more pervasive and provides criminals with an ever-growing source of new tools, a framework for **lawful access to data** is essential to ensure criminals are brought to justice. The 'lawful access' to which this roadmap refers is the access, in conformity with the law, to the digital information that law enforcement authorities need for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

To be lawful, access to data needs to be **necessary and proportionate and respect fundamental rights**, ensuring that privacy and personal data are adequately protected; it must be based on **clear, precise and accessible rules set out in law**, subject to independent **oversight mechanisms**, and with **effective remedies** available to the individuals who may be affected by the access to their data. Ensuring that digital systems remain **cybersecure** from unauthorised access is equally important to protect against cybersecurity threats.

I. Ensuring the availability of digital evidence: data retention[11]

In Spain, a criminal investigation into the disappearance of a young woman was solved in 2019 thanks to location data stored by a communication service provider in line with a national legal obligation. These data enabled investigators to locate the missing woman, determine that the suspect of the kidnapping was also in that area, and rule out other suspects[12]. Non-content communication data (e.g. subscriber information, location data and the date, time, duration, sender and receiver, and size of the communication) are critical in most criminal investigations and prosecutions. These data can be decisive in identifying and locating victims, suspects and accused individuals, shedding light on a committed offence, including helping rule out suspects.

In line with EU privacy and data protection laws, electronic communications service providers may only store non-content communication data that are going through their systems for as

[9] Recommendations of the High-Level Group on access to data for effective law enforcement.

[10] Council conclusions on access to data for effective law enforcement (12 December 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/en/pdf; Council conclusions on future priorities for strengthening the joint counterterrorism efforts of the European Union and its Member States (12 December 2024) https://data.consilium.europa.eu/doc/document/ST-16820-2024-INIT/en/pdf.

[11] Data retention refers to service providers keeping certain non-content data processed in the context of the communication services that they provide for a given period, to enable access under appropriate safeguards by competent authorities in criminal investigations and to ensure criminal justice.

[12] La cobertura del móvil de Diana Quer desmonta la versión del Chicle: no la abordó donde él dijo que estaba robando gasolina | España.

long as it is necessary for specified, explicit and legitimate business purposes. However, legal obligations can require them to keep (or 'retain') this data for other purposes, e.g. if they are needed for the prevention, investigation, detection and prosecution of criminal offences.

Since the EU Data Retention Directive[13] was invalidated in 2014[14], the EU legislative landscape on obliging service providers to store data has become fragmented and uneven. Member States' data retention frameworks diverge on the types of electronic communications that service providers have to retain, the categories of data they cover, and the required retention periods[15]. Moreover, some Member States do not have any data retention laws. Law enforcement and judicial authorities face legal and operational obstacles in conducting their work. Electronic communication providers, especially smaller providers, also face additional costs and obstacles when providing their services across the EU because they are required to comply with different legal requirements in different Member States.

The High-Level Group therefore recommended setting up **a harmonised EU framework for data retention** to ensure that the digital evidence required to investigate and prosecute crimes is available. A harmonised EU regime would aim at limiting fragmentation between Member States as regards the rules on retention and the safeguards pertaining to fundamental rights, in particular, privacy and data protection and the rights of defence, including the right to a fair trial. Such a legal framework would thereby also ensure legal certainty for the competent authorities, on one hand, and service providers on the other[16].

Key action

- **In 2025, the Commission will prepare an impact assessment with a view to updating EU rules on data retention as appropriate.**

The High-Level Group identified a need to **strengthen the synergies between law enforcement practitioners and service providers**[17].

To do so, **the European Union Agency for Law Enforcement Cooperation (Europol) and the European Union Agency for Criminal Justice Cooperation (Eurojust)** are invited to continue and expand their efforts **to facilitate cooperation, the exchange of information and best practices between practitioners and service providers** through the **SIRIUS project**[18], with the continued support of the Commission. The SIRIUS project has become the most important source of information **to support law enforcement practitioners and judicial authorities in the EU and beyond in accessing electronic evidence stored by online service providers** based in third countries. The SIRIUS Platform has over 8 000 members from the law enforcement and judicial communities, representing 47 countries worldwide, and has directly supported almost 70 police operations.

---

[13] https://eur-lex.europa.eu/eli/dir/2006/24/oj.
[14] Judgment of the Court (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others.
[15] For an overview see The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU | Eurojust | European Union Agency for Criminal Justice Cooperation and European Commission Study on the retention of electronic communications non-content data for law enforcement purposes.
[16] Recommendation Cluster 6, Concluding Report of the High-Level Group.
[17] Recommendation Cluster 5, Concluding Report of the High-Level Group.
[18] SIRIUS Project | Europol.

With the same aim, Europol and Eurojust should use the SIRIUS project to develop, in cooperation with the **private sector, a catalogue of the data that electronic communications services legitimately process for their business purposes**. This will help competent authorities to identify what data may be available for their lawful access requests, identify relevant service providers and better target lawful access requests, therefore saving time and costs for both public authorities and service providers.

Key actions

- **With the continued support of the Commission, Europol and Eurojust are urged to build on the SIRIUS project to streamline cooperation with electronic communications service providers.**

- **Europol and Eurojust are urged to develop, in cooperation with the private sector, a catalogue of data that electronic communications providers process for their business purposes (to start in Q4 2025).**

II. Obtaining evidence across systems and jurisdictions: lawful interception

Lawful access to communication data in real time is essential to fight criminals online and offline. In 2020, a French and Dutch joint investigation team dismantled EncroChat, an encrypted phone network widely used by organised crime groups. This joint investigation involved intercepting millions of messages in real time between criminals planning to execute serious crimes, sharing these messages with other authorities and analysing them. Thanks to the information obtained, law enforcement authorities all around Europe and other parts of the world have disrupted criminal activities, including violent attacks, corruption, attempted murders and large-scale drug trafficking. Certain messages indicated plans to commit imminent violent crimes and enabled law enforcement authorities to prevent them[19]. The European Investigation Order (EIO) facilitated sharing this evidence efficiently[20].

The EncroChat case demonstrates that real-time access to content data of communications is an essential tool in the effective investigation and prosecution of organised crime groups. However, this case remains one of the few success stories: the High-Level Group noted that the effectiveness of lawful interception[21] has drastically decreased as communication has moved from traditional phone calls and SMS to 'over the top' (OTT) messaging services provided through apps. Currently, around 97% of all mobile messages are sent through messaging apps, while traditional SMS and MMS messaging accounts for only about 3% of messages[22]. The High-Level Group also noted that, since 2020, following the disruption of some of the major criminal communications networks, many criminal groups have decided to move back to regular end-to-end encrypted OTT messaging services[23].

[19] Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe | Europol; Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée.

[20] European Investigation Order | Eurojust | European Union Agency for Criminal Justice Cooperation.

[21] In the context of this Communication, lawful interception technologies that are implemented to get real-time access to communication data in judicial investigations by a communication operator as well as technologies that can be deployed autonomously by law enforcement authorities.

[22] Concluding Report of the High-Level Group, p. 38.

[23] Internet Organised Crime Threat Assessment IOCTA 2024.

National rules imposing obligations for lawful interception are fragmented in the EU[24]. The High-Level Group noted that although some Member States impose similar obligations for all types of electronic communication services, including OTTs, others exclude them. In addition, service providers are often not established in the Member State of the requesting authority, which can result in complex jurisdictional issues, conflicts of laws and challenges to enforcement[25]. As a result, the content of such messaging services is practically inaccessible.

The EIO and other cooperation instruments can help overcome the challenge of cross-border interception in parts of the EU. However, Member State authorities still face difficulties when using them: these instruments cannot support interception where the service is provided either from Member States that do not participate in the instrument concerned, or from a third country. The High-Level Group therefore recommended a number of measures to ensure that a broad range of providers, including OTT providers, respond to lawful interception requests[26].

In response, the **Commission will propose how to improve measures to enhance cross-border cooperation on interception** both among authorities and between authorities and services providers. Following the High-Level Group's recommendations, the Commission will primarily work on improving existing instruments, in particular the EIO, and voluntary cooperation (where there are no conflicts of laws with third countries or these have been lifted). Ultimately, Member States should be able to enforce lawful interception obligations on all communication providers proposing services domestically, as provided for in national laws, regardless of whether they are traditional telecommunication services or internet-based and regardless of their location.

Furthermore, some Member States do not have the required network capacities for data sharing in cross-border cooperation. Therefore, the **Commission will identify Member States' needs** and support the deployment of secured networks with sufficient bandwidth among relevant Member States, enabling the transfer of large amounts of data in real time. This initiative could be funded from EU programmes.

Key actions

The Commission will:

- **propose measures to improve the efficiency of cross-border requests for lawful interception through existing instruments, including assessing the need to further strengthen the European Investigation Order (by 2027);**
- **explore measures to create a level-playing field for all types of communication providers in the enforcement of lawful interception obligations;**
- **determine the most efficient approach to tackle non-cooperative communication providers;**
- **support the deployment of secured information sharing capacities between Member States, Europol and other security agencies (from 2026 to 2028).**

[24] See the EU White Paper on Digital Infrastructure, p. 14; Letta Report on the Internal Market, p. 59, and the Draghi Report on EU competitiveness, pp. 70, 74, 76.
[25] Concluding Report of the High-Level Group, p. 41.
[26] Recommendation Cluster 8, Concluding Report of the High-Level Group.

Member States are encouraged to implement cross-border lawful interception measures, building on existing mechanisms such as the European Investigation Order and bilateral and multilateral agreements.

III. Retrieving evidence from devices seized in investigations: digital forensics

To conduct criminal investigations, law enforcement and judicial authorities need to be able to access, collect, analyse and preserve digital evidence stored on electronic devices. This digital evidence can, for example, help identify members of organised crime groups or rule out people as suspects[27].

The High-Level Group discussed a number of challenges that impede access to this digital evidence. National authorities suffer from a severe lack of resources and capabilities to conduct digital forensics. They struggle to keep up with the need to continuously develop new skills and tools to keep pace with new technologies (e.g. new types of devices and operating systems, the Internet of Things and cloud computing). Cross-border cooperation among Member States is undermined by the lack of comparable capacities and by the absence of mechanisms for recognising digital forensics experts' skills and expertise. Existing commercial solutions quickly become obsolete, are unaffordable and are often developed outside the EU. They may also be poorly suited to the needs of Member States' authorities or may not meet EU digital forensics' accountability standards or other legal requirements.

As a result, to strengthen the ability of European law enforcement authorities to perform digital forensics on seized devices, the High-Level Group recommended providing targeted funding for projects, both for the research and development of digital forensics tools and for their uptake. The High-Level Group welcomed the ongoing efforts of the Commission to support these through funding under certain EU instruments (Horizon Europe, the Digital Europe programme and the Internal Security Fund) and corresponding instruments under the EU's next long-term budget (Multiannual Financial Framework).

In response to these recommendations[28], the **Commission, with the support of Europol, will coordinate a gap and needs analysis of research, development, deployment maintenance and uptake of common technical solutions for digital forensics.**

The use of resources must be maximised by building synergies among digital forensic projects, including by integrating those funded under Member States' programmes in existing mechanisms or networks. This should include funding public-private partnerships to deliver fully tested and ready-to-use software tools with no licencing costs[29].

Within OLAF's mandate to perform administrative investigations, the Office has developed significant experience in digital forensic processes and tools and can assist Members States authorities in reinforcing their capacities through the Union Anti-fraud Programme.

[27] A case discussed in the High-Level Group related to the analysis of a device that was instrumental in proving that a suspect was not involved in a murder. Concluding Report of the High-Level Group, p. 12.
[28] Recommendation Cluster 1, Concluding Report of the High-Level Group.
[29] For example, the European Anti-Cybercrime Technology Development Association (EACTDA) (www.eactda.eu) delivers fully tested and operationally ready-to-use software tools with no licence costs and access to the source code for EU law enforcement agencies. On top of eight tools finalised to date, the EACTDA is developing 16 more digital investigations tools, to be delivered by mid-2025.

The **Europol Tool Repository** is a secure online platform, exclusively available to law enforcement authorities, for sharing free, non-commercial software developed by Europol, European law enforcement agencies and academia. National investigative authorities have widely used the repository's tools to support related to serious and organised crime areas including trafficking in human beings, cybercrime and online child sexual abuse. This repository should remain the privileged distribution channel for digital investigative tools developed by EU projects, and Member States, who will be encouraged to share open-source digital forensics tools developed at national level within existing mechanisms or networks. **Europol can further develop and promote its Tool Repository** to make trusted, secure, free-of-charge, easy-to-install and scalable investigative tools available to EU law enforcement authorities.

The Commission will also **support the uptake of innovative solutions by Member States' law enforcement authorities through existing mechanisms, such as EMPACT[30], and through dedicated Internal Security Fund calls**.

The High-Level Group underlined that **licences for digital forensics tools** are costly and sometimes unaffordable for some law enforcement authorities. Digital forensic tools may provide data in formats that are not compatible with systems used for further processing. In addition, trust is fundamental for digital forensics activities, which should not rely on 'black box' tools (i.e. tools that process data without trusted authorities being able to verify how they work). Sharing digital forensics tools should be supported by evaluation schemes and, where relevant, certification of commercial tools at EU level to ensure they meet trustworthiness and forensic standards without imposing undue burdens. Support should also be given through common procurement schemes, ensuring cooperation between operational units and the contact points in procurement authorities[31].

Therefore, **the Commission will support Member States' operational units and their procurement authorities to put in place joint purchases of licences for digital forensics tools, starting with a pilot phase.**

Key actions

The Commission, with the support of Europol, will:

- **coordinate a gap and needs analysis of research, development, deployment maintenance and uptake of common technical solutions for digital forensics before Q2-2026;**
- **continue to support the development of technical solutions for digital forensics through appropriate funding and coordination mechanisms;**
- **support Member States and procurement authorities in putting in place joint purchases of licences for digital forensics tools (before Q2-2027), starting with a pilot phase.**

[30] EMPACT (European Multidisciplinary Platform Against Criminal Threats) is a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime.
[31] Building on the iProcureNet Project (www.iprocurenet.eu/), which, funded under the EU Horizon Europe Programme for research and innovation, has built a methodology for joint procurement in the area of security, as well as a network of procurement authorities in Member States.

Europol is invited to further develop and promote its Tool Repository to enable law enforcement authorities' access to non-commercial digital tools (starting in Q3-2025).

Member States are invited to participate, support and steer the development, validation and uptake of digital forensic tools.

The EU Agency for Law Enforcement Training (CEPOL) delivers training to digital forensic investigators, including on mobile forensics and live data forensics. Following the High-Level Group's recommendation[32], the **Commission should continue supporting the creation of training materials and resources** through existing mechanisms involving practitioners and academia[33]. In addition, CEPOL and Member States should **prioritise delivering digital forensics training.**

The High-Level Group also underlined that a certification scheme could be created at EU level for digital forensics experts. Such a scheme would ensure the quality of digital forensics work, contribute to more transparent judicial proceedings and increase trust between law enforcement authorities across borders.

In line with the High-Level Group's recommendations[34], CEPOL **could support practitioners and academia, making full use of existing networks and mechanisms[35], in creating a certification scheme at EU level for digital forensics experts**.

Key actions

The Commission will:

- **continue supporting the creation of training materials and resources.**

CEPOL and Member States are encouraged to:

- **prioritise delivering digital forensics training (from Q3-2025);**
- **support the development and implementation of a certification scheme at EU level for digital forensic experts (to be prepared between Q1-2026 and Q4-2028).**

The High-Level Group made recommendations on facilitating the sharing of solutions and digital forensics tools among Member States in an environment of trust[36]. In response, **Europol should further develop its role as the EU law enforcement centre of excellence for digital operational expertise in the field of digital forensics**. This could include setting up a project similar to SIRIUS[37] to facilitate the sharing of knowledge, expertise, technical solutions, digital forensics tools and best practices in an environment of trust. Europol should also step up its coordination role in creating knowledge in digital forensics at EU level, building on the

[32] Recommendation Cluster 3, Concluding Report of the High-Level Group.
[33] For example, the European Cybercrime Training and Education ECTEG (www.ecteg.eu) is an association working in close cooperation with Europol and CEPOL, with the aim to deliver free training resources to law enforcement authorities in the area of digital investigation. It is currently funded by the EU Internal Security Fund.
[34] Recommendation Cluster 3, Concluding Report of the High-Level Group.
[35] In particular ECTEG.
[36] Recommendation Cluster 1, Concluding Report of the High-Level Group.
[37] The SIRIUS project, led by Europol and Eurojust, supports EU law enforcement and judicial authorities by facilitating efficient cross-border access to electronic evidence stored by online service providers. It provides practical tools, training and resources for over 9 000 practitioners, fosters cooperation among online service providers, and promotes knowledge-sharing through international events and partnerships.

mechanisms created in recent years[38]. Europol can begin some of these actions under its current mandate. However, Europol will need a reinforced mandate and additional resources to fully develop these actions and effectively meet Member States' operational needs.

Following up on the commitment set out in the Political Guidelines for the 2024−2029 European Commission and as announced in the European Internal Security Strategy, **the Commission will propose an ambitious overhaul of Europol's mandate**. To prepare this, in close cooperation with Member States, the Commission will explore how to bolster Europol's technological expertise and capacity to support national law enforcement authorities in the digital space. Boosting Europol's digital forensics capabilities, based on a reinforced mandate and with additional resources, will be crucial in this effort.

The High-Level Group recommended improving access to knowledge for experts through dedicated mechanisms and for experts to work with producers and developers of digital forensics tools[39]. As of 2026, **Europol, using its own resources, should foster cooperation among relevant national authorities and experts to facilitate public-private cooperation on digital forensics**. It should support Member States in developing digital tools and common procedures, including setting common data formats for digital forensics purposes[40].

Key actions

Europol is called upon to:

- **develop into a centre of excellence for operational expertise in digital forensics and step up its role in coordinating the creation of knowledge in this area at EU level (from 2026 onwards);**

- **facilitate cooperation between law enforcement authorities and private parties, including service providers, on digital forensics and help set common data formats for digital forensic purposes (from 2026 onwards).**

IV. Ensuring that evidence can be read: decrypting data

Encryption and other cybersecurity measures play an important role in protecting information systems from espionage and disruption and securing communications, privacy and personal data. Between 60% and 80% of messaging applications are end-to-end encrypted, including mainstream providers such as WhatsApp, Messenger, Signal and iMessage, while the use of SMS and traditional phone calls is drastically decreasing worldwide[41].

The High-Level Group emphasised that these developments impact the ability of law enforcement and judicial authorities to gather evidence in criminal investigations and prosecutions as most lawful interception of communications become unusable. The High-Level Group underlined that Member States have limited expertise and capabilities to decrypt data at

[38] Dedicated communities on the Europol Platform for Experts (https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts); the Forensic Experts Forum (https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference); Europol Industry and Research Days (https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025).

[39] Recommendation Cluster 1, Concluding Report of the High-Level Group.

[40] These efforts should be supported by the appropriate EU funding source (programmes for research or development, depending on the level of maturity of the envisaged systems).

[41] The percentage referred to relates to end-to-end encryption during transmission.

rest, with significant differences in success rates, ranging from 15-20% in some Member States to more than 66%in others.

Decryption equipment is expensive and highly specialised, and the hardware consumes a lot of resources. Most law enforcement digital forensics departments rely on commercial solutions to access data on devices. These solutions struggle to keep pace with technological developments and quickly become obsolete; the high cost of licences significantly reduces the number of authorised users; and these solutions are often developed outside the EU and may therefore not meet the needs of EU authorities or digital forensic standards. As a result, they are only used successfully in a very small number of investigations.

In addition, relying on these tools has other downsides. In their investigations, authorities often exploit vulnerabilities to gain access to decryption keys on devices, which could in some cases create tension with the policy objective of ensuring cybersecurity by default. Furthermore, accessing encrypted data is becoming increasingly complex. The High-Level Group noted that data stored on certain types of modern devices, protected by crypto chips or strong encryption algorithms and complex passwords, cannot be accessed by authorities, even using the most powerful decryption platforms.

The development and roll-out of **quantum safe cryptography** is a necessity to protect data from future quantum computer attacks that would render sensitive communications, financial transactions and state secrets vulnerable to decryption and exploitation. As set out in the Commission Recommendation on a Coordinated Implementation Roadmap for the transition to **post-quantum cryptography (PQC)**[42] and in the European Internal Security Strategy (ProtectEU), deploying PQC solutions and developing quantum key distribution will be crucial to safeguarding data in the new quantum era. However, as highlighted by Europol, this will make lawful access to digital evidence more difficult in the years to come, and law enforcement agencies need to invest in keeping pace with rapid technological development[43].

The High-Level Group[44] recommended developing a technology roadmap to implement targeted lawful access by design when appropriate, while ensuring strong security and cybersecurity and fully respecting legal obligations on lawful access. In response, **the Commission is tasking an expert group to provide support in preparing a technology roadmap on encryption.** The group will identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, while safeguarding cybersecurity and fundamental rights. The group will include experts in law enforcement, cybersecurity, encryption, communication technologies, standardisation and fundamental rights. Technological studies and proof of concepts will support that work. The purpose of this work is to identify:

- **tools that law enforcement authorities currently need and will need in the future** to lawfully find, retrieve and analyse encrypted data; such tools must facilitate digital forensics, decryption, remote data collection and crime analysis activities;
- **technologies that ensure that future information and communication technologies**, such as the sixth generation of cellular networks (6G) and quantum resistant encryption,

[42] Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography.
[43] The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement | Europol.
[44] Recommendation Cluster 10, Concluding Report of the High-Level Group.

do not harm law enforcement authorities' ability to access data lawfully, while ensuring compliance with fundamental rights and cybersecurity.

Where no tools currently exist, the technology roadmap is expected to provide recommendations on their development and on how to both ensure compatibility with the EU legal framework and guarantee cybersecurity. The outcome of the technology roadmap may also inform specific actions to foster a coordinated approach to standardisation

The Europol decryption platform has proven instrumental in supporting major criminal cases, including those coming from the Sky ECC[45] and EncroChat cases. Enhanced decryption capabilities, also driven by further investments in artificial intelligence (AI) and high-performance computing, are needed to ensure that law enforcement has the capacity to decrypt increasingly complex algorithms.

The High-Level Group made a recommendation[46] to increase funding to support innovation on access to data. In response, **the Commission will support the research and development of new decryption capacities** to ensure that Europol is well equipped after 2030 to support Member States, in light of new technological developments and the most advanced research in the field. This initiative could involve increasing funding to support decryption research, as well as the development and implementation of tools by Member States. Member States will be closely involved to share their specific requirements, aiming to level up their capacities, skills and technical resources, building on technologies designed at EU level and possibly exploring joint procurement.

Key actions

The Commission will:

- **deliver a technology roadmap on encryption (in Q2-2026);**
- **support the research and development of new decryption capacities to equip Europol with next-generation decryption capabilities (from 2030).**

V. Reconciling technology and lawful access: standardisation

Standards are essential in digital communications. Developed by a vast array of actors, mostly by industry, they provide for interoperability between systems and devices developed by technology providers and facilitate technologies' compliance with legal obligations, including on lawful access for law enforcement purposes. The European Telecommunications Standards Institute (ETSI) has developed several standards in the area of lawful interception and lawful disclosure. However, gaps exist, such as with the fifth generation of cellular networks (5G), where the lack of appropriate consideration for lawful access in its development has hindered law enforcement and judicial authorities' ability to access the necessary evidence to identify and bring criminals to court[47].

The High-Level Group recommended taking a cautious approach to designing solutions for lawful access to systems, whereby industry should not be asked to integrate systems that are

[45] New major interventions to block encrypted communications of criminal networks | Europol
[46] Recommendation Cluster 10, Concluding Report of the High-Level Group.
[47] See First report on Encryption from the EU Innovation Hub on Internal Security, 11 June 2024.

likely to weaken encryption in a generalised or systemic way for all users of a service. Lawful access to data must remain targeted and limited to specific communications on a case-by-case basis.

As a general rule, any solutions should be implemented based on clear standards that are developed with input from all stakeholders, including industry representatives, data protection, privacy and cybersecurity experts, and law enforcement practitioners. However, caution is warranted when dealing with encryption, as underlined by the High-Level Group. Based on solutions identified in the technology roadmap, specific measures to foster a coordinated approach to standardisation will be envisaged.

Any standardisation should reflect the applicable legal requirements and be based on evaluated solutions. It must ensure that lawful access does not conflict with applicable cybersecurity standards, such as those developed under the Cyber Resilience Act, or standards supporting the implementation of the NIS2 Directive nor otherwise impair the security of products and services.

Regarding the High-Level Group recommendations[48], **the Commission will develop and streamline an EU approach to standardisation for internal security, with a focus on digital forensics, lawful disclosure and lawful interception.** This approach will be based on continuous landscape analysis conducted by law enforcement practitioners, in particular through the European Working Group on Standardisation on Internal Security, led by Europol. This action will also increase the resources and scope of the Working Group and entail further collaborating with other initiatives in standardisation, particularly on AI and digital forensics. The goal is to ensure that security concerns are integrated into standardisation policy. In addition, this initiative will include developing and organising training on standardisation in the area of security and providing financial support through the Internal Security Fund to experts participating in relevant standardisation forums. It will also incorporate relevant governance mechanisms.

Key actions

- **The Commission, in close cooperation with Europol, will develop and streamline standardisation activities for lawful access, supported by suitable governance mechanisms (from Q2-2025 to Q2-2027).**

- **Member States are encouraged to devote sufficient resources to ensure that security practitioners participate in relevant standardisation forums on lawful access.**

VI. Analysing evidence effectively and lawfully: AI

Europol and Eurojust recently noted that an increasing number of investigations contain very large amounts of data[49]. In a standard child sexual abuse case, investigations often require analysing between 1 to 3 terabytes of data, which can include 1 to 10 million images and thousands of hours of video footage[50]. In 2023, 1 553 822 large files were exchanged via

[48] Recommendation Cluster 10, Concluding Report of the High-Level Group.
[49] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust.
[50] Europol IOCTA.

Europol's large file exchange (LFE)[51]. In the EncroChat case, over 115 million conversations among organised crime suspects were intercepted. In the following months, through advanced analytical techniques and means, such as machine learning, Europol and law enforcement agencies were able to identify patterns, connections and hotspots, leading to the arrest of 6 558 suspects. Dutch and French authorities shared this information with their counterparts in EU Member States and third countries, leading to more than 200 murder plots being foiled in the UK alone[52].

The continuous increase of data handled in the course of investigations is making it difficult to store, manage and effectively analyse data without significant expertise, computational resources and specialised tools. Europol and Eurojust confirmed that the data volume can be overwhelming for investigators and lead to higher processing times and storage capacity issues. Member States also often lack the mechanisms and infrastructure required to handle the transfer of large amounts of data to other Member States and Europol.

Therefore, using AI is essential for law enforcement authorities to prevent, detect and investigate crime and therefore protect our societies in the digital age. AI-based solutions can perform simple tasks, such as machine translation or converting speech to text, or more complex tasks, such as data filtering, correlating evidence from massive amounts of data, or fighting against the malicious use of AI. AI-powered tools for law enforcement authorities need to be accurate, transparent and fully compliant with the EU legal framework for AI, data protection and privacy to ensure trustworthy and ethical data-driven investigations. AI and high-performance computing are of paramount importance in getting access to encrypted data and supporting investigations and forensic analysis.

Following the High-Level Group recommendations to increase funding for the research and development of tools for AI-based data analysis and set out clear deliverables[53], **the Commission will foster the development and uptake of AI solutions.** This includes targeted investments in developing key capabilities, such as solutions to identify investigative leads from very large amounts of data in full compliance with data protection and privacy principles or improvements to tracing crypto-currency transactions. It could also be possible to leverage opportunities for training, testing and evaluating AI tools in an AI regulatory sandbox, as provided for in the AI Act[54], with support and guidance of competent supervisory authorities. Furthermore, AI factories and future gigafactories could support the development of AI-based tools and services for law enforcement. The Commission should facilitate these efforts, based on an analysis of the needs with stakeholders, including Europol's Innovation Lab and the EU Justice and Home Affairs agencies' Innovation Hub for internal security.

Member States can have access to relevant capabilities at little or no cost, ensuring compatibility with the AI Act's requirements. A comprehensive approach to AI is crucial, including creating standardised data formats for any exchanges and drawing up guidelines on the use of such systems in line with the AI Act and applicable EU data protection laws. This action could be supported by funding from the Internal Security Fund, the Digital Europe programme and Horizon Europe. It will involve supporting Europol and the EMPACT

[51] Europol consolidated annual activity report 2023.
[52] Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée; Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized | Europol. EncroChat.
[53] Recommendation 4, High Level Group Recommendations.
[54] See Article 57 of the AI Act.

community to ensure a proper match with operational needs and to promote uptake and mainstreaming by practitioners.

Key actions

The <u>Commission</u> will:

- **Foster the creation and uptake of new AI solutions and improve existing ones for filtering and analysing digital evidence, including through the full use of AI regulatory sandboxes for their development, testing and evaluation, in line with the AI Act (from 2025 to 2028);**

- **engage in a dialogue with law enforcement and other stakeholders to identify their needs, building on the work of Europol's Innovation Hub and the EU Justice and Home Affairs agencies' Lab;**

- **support the creation of clear guidelines for the use of AI in law enforcement;**

- **support pilot projects aimed at developing and training legally and technically sound AI solutions for digital forensics, data analysis and other investigative tools for law enforcement use.**