Ref. Ares(2023)7888883 - 20/11/2023

Background document

Operational Challenges Faced by Law Enforcement Related to Access to Data

Input to the second plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement

21 November 2023

1. **Introduction**

The European Union constitutes an area of freedom, security, and justice with respect for fundamental rights and the different legal systems and traditions of the Member States.[1] It endeavours to ensure a high level of security and privacy through measures to prevent and combat crime, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities.[2]

Law enforcement authorities need to carry out their tasks effectively and lawfully and in full respect of fundamental rights to prevent, detect, investigate, and ensure the prosecution of crimes, to provide justice to victims, and to safeguard public security. In recent years, the European Council, the Council,[3] the European Parliament,[4] the Court of Justice of the European Union, and EU agencies have on several occasions discussed and formulated conclusions on various legal and policy aspects of access to electronic communications data, including technical traffic and location data (metadata), and more generally, to electronic evidence. In its conclusions of 22–23 June 2017,[5] the European Council called for "addressing the challenges posed by systems that allow terrorists to communicate in ways that competent agencies cannot access, including end-to-end encryption, while safeguarding the benefits these systems bring for the protection of privacy, data and communication" and highlighted that "effective access to electronic evidence is essential to combating serious crime".

The EU Strategy to tackle Organised Crime 2021–2025 stresses the importance of access to electronic communications data to tackle organised crime and making law enforcement and the judiciary fit for the digital age.[6] Access to data is also of key importance for all EMPACT priorities in the fight against serious and organised crime for 2022–2025,[7] and the EU Security Union Strategy has stated that the Commission will explore measures to enhance law enforcement capacity in digital investigations.[8] This is further supported by the assertion in the EU Drugs Action Plan 2021-2025 that the Union will endeavour to improve possibilities to tackle encryption.[9] In 2023 the Swedish Council Presidency presented the document 'Law Enforcement – Operational Needs for Lawful Access to Communications (LEON)' which sets out a comprehensive list of operational needs of law enforcement authorities with respect to communications networks and services.[10]

---

[1] *The Treaty on The Functioning of the European Union* (TFEU), Article 67, para 1.
[2] *Ibid.*, para 3.
[3] Doc. no. 8289/1/16, *Council conclusions on improving criminal justice in cyberspace.*
[4] OJ 2018/C 346/29, Eur*opean Parliament resolution of 3 October 2017 on the fight against cybercrime.*
[5] Doc. EUCO 8/17.
[6] *Communication from the Commission on the EU Strategy to tackle Organised Crime 2021–2025,* COM/2021/170 final of 14 April 2021.
[7] Doc.no. 8665/21.
[8] *Communication from the Commission on the EU Security Union Strategy,* COM/2020/605 final of 24 July 2020
[9] *EU Drugs Action Plan 2021-2025,* Official Journal of the European Union C 272/2 of 8 July 2021
[10] *Communication from the Council Presidency on Law Enforcement Operational Needs for Lawful Access to Communications (LEON),* 6050/23 of 16 February 2023

Digitally generated, processed, or stored communication data (both metadata and content data) is an increasingly important component of modern criminal investigations. However, law enforcement authorities face increasing operational challenges when seeking to lawfully access data digitally generated or stored in a readable format, be it (i) data at rest in a user's device, (ii) data at rest in a provider's system, or (iii) data in transit.

Access to this data is understood as access granted to law enforcement subject to judicial authorisation when required, in the context of criminal investigations and on a case-by-case basis. As a rule, in the cases where such judicial authorisation is necessary due to the sensitive nature of the data in question, it represents an integral part of the applicable legal and operational framework for facilitating access to this data by law enforcement. Access to data on behalf of law enforcement authorities must be achieved in full respect of data protection, privacy, and cybersecurity legislation, as well as the Court of Justice of the European Union (CJEU) case-law on these matters and applicable standards on procedural safeguards.

At the first Plenary Meeting of 19 June 2023, the High-Level Group on Access to Data for Effective Law Enforcement (HLG) confirmed the establishment of three separate Working Groups to explore the above cases in further detail.

The first meetings of the three Working Groups took place on 19 July, 6 September, and 4 October of 2023, respectively. The experts participating were tasked with taking stock of the current situation for each of their allocated data categories and focusing on identifying and prioritising the main challenges encountered by law enforcement, and the drivers that underpin them, and subsequently reporting back to the second plenary meeting of the HLG.

This present background document provides a summary of the challenges identified across the three Working Groups to facilitate discussions at the second Plenary Meeting of the HLG.

2. **Problem Definition**

Each of the individual Working Groups were tasked with identifying the issues that law enforcement face in regard to access to, respectively, (i) data at rest in a user's device, (ii) data at rest in a provider's system, or (iii) data in transit.

Alongside Working Group-specific problems, cross-sectional concerns were identified. Despite requests to this end, it appears unfeasible for law enforcement authorities to classify the criminal case types that are more or less reliant on access to data to be solved, as well as the categories of data which are necessary to investigate and prosecute criminal offences. National experts highlighted the difficulties faced in providing statistics which could quantify the importance of lawful access to data for successfully investigating and prosecuting crime, regardless of the type of offence suspected or the type of data required. Furthermore, the current state of the public discourse concerning privacy and security, which are at times erroneously contrasted, was proposed as a factor which might have

negatively affected the development of legislation to develop lawful pathways for law enforcement authorities to access data.

2.1. **Working Group 1 - Data at rest in a user's device**

2.1.1. What are the problems?

Working Group 1 was given the mandate of exploring issues that national law enforcement authorities face in lawfully accessing data at rest in a user's device. This has been flagged at the first Plenary Meeting of the HLG as a challenge that manifests itself in almost all investigations due to the overwhelming use of digital communication devices in our modern society. For access to data at rest in a user's device, the key problems for law enforcement authorities are gaining lawful access to a user's device and, if access is possible, decrypting the data and metadata available to extract readable information that can be of use to investigations or be presented as admissible evidence in court.

Though encryption is a necessary means for protecting fundamental rights and the digital security of governments, industry, and society,[11] law enforcement authorities asserted that its increasing role as an industry standard for electronic communications has impacted their ability to carry out their mandates by hampering evidence gathering and slowing down or stalling investigations. The pace of technological developments related to encryption is rapid to the point that decryption is proving more difficult, and progressively the techniques and tools that are commonly available to law enforcement authorities are solely effective for use in lower-level criminal cases. For cases where the concerned suspect or organised crime group is aware of how to maintain a more 'access-proof' device even such techniques and tools often do not suffice, and the capacity of individual national law enforcement authorities to develop more sophisticated or custom-designed decryption tools is limited. The time required to decrypt devices is also a significant issue faced, where in some instances this was reported as taking up to 24 months. The degree of difficulty involved in decrypting custom mobile encryption devices that have been designed and marketed for criminal purposes is even higher and presents further challenges to digital forensics departments across the Member States.

However, technical solutions to enable authorities to use their investigative powers must preserve all the advantages of encryption[12] for data protection and national security reasons. To uphold this principle of 'security through encryption and security despite encryption', any technical solutions or tools that are developed must not result in the weakening, banning, circumvention, or impediment of encryption. [13]

[11] Council Resolution 13084/1/20 on Encryption of 24 November 2020.
[12] *Ibid.*
[13] Presidency of the Council of Ministers, "Security Through Encryption and Security Despite Encryption" (Council of Ministers 2020) 10728/20

2.1.2. What are the problem drivers and legal constraints?

The first problem driver, that law enforcement authorities face at the outset of any investigation involving users' devices, pertains to suspects that refuse to cooperate with requests to unlock these devices. There are different national legal frameworks across the Union concerning the lack of suspect cooperation. However, applying lawful coercive measures to unlock the device in question was reported to be ineffective even in those Member States where the suspect is obliged by law to cooperate. As a rule, the legal principle of *nemo tenetur*, or the right not to incriminate oneself, applies to all legal systems of the Member States. This fundamental right is recognised by the ECtHR as an implicit part of Article 6 (2) ECHR[14] and is enshrined in Article 48 of the Charter of Fundamental Rights of the EU as well as in Directive (EU) 2016/343 on the presumption of innocence.[15] This adds to the issues that prosecutors can face in court with regards to the admission of evidence obtained through lawful but coercive access to users' end devices, specifically in Member States that do not oblige suspects to hand over their access keys. An additional driver is the lack of clarity about the use of Open-Source Intelligence (OSINT) to access users' devices.[16]

The second key problem driver for accessing data at rest in users' devices is that due to the increasing robustness of encryption with keys stored in secured chips, alongside the prevalence of encryption by default,[17] advanced digital forensic tools available to law enforcement have become less effective. This creates situations where law enforcement authorities are unable to access and retrieve data from lawfully seized devices in a readable format. Commercial solutions for decrypting data on which law enforcement authorities have traditionally relied are costly and are being outpaced by encryption developments as the industry acts to find countermeasures in response to decryption techniques. A further issue with commercially available digital forensic solutions is that the large majority of these are developed outside the EU and may therefore neither

[14] Mickonytė, A. (2018). "Chapter 7 Duty of Cooperation: Compliance with Nemo Tenetur under Article 6(2) echr". In *Presumption of Innocence in EU Anti-Cartel Enforcement*. Leiden, The Netherlands: Brill | Nijhoff. Available at: https://doi.org/10.1163/9789004384651_008

[15] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, p. 1–11.

[16] Open-Source Intelligence is the collection and analysis of publicly available data. If a password found online as part of a password leak is found to be the access code required to gain entry to a device belonging to a suspect under investigation it can be considered both stolen data and OSINT – the former would disqualify data accessed using this password in court as this access would be based on a stolen code, whilst the latter would qualify the evidence as submissible as OSINT can be used in court cases. The lack of clarity creates operational uncertainty for law enforcement authorities.

[17] Encryption by default is often a feature of the operating system. Devices running on various versions of MacOS, Windows, IOS or Android include this feature.

comply with data protection and privacy requirements, nor digital forensic standards maintained within the Union.

The third key driver is the lack of cross-border law enforcement cooperation concerning the sharing of digital forensic tools as Member States often have distinct solutions for similar technical problems. Despite Europol hosting an in-house repository for tools developed that can be accessed and used by national law enforcement authorities, Member States likely have access to further tools and bespoke decryption software. However, they reportedly refrain from sharing these, either due to a lack of trust and communication between the relevant digital forensic departments and the prevalence of a *quid pro quo* approach to sharing such tools, or because they are not allowed to do so by law, often due to national security concerns.

A fourth driver of the problem faced when attempting to decrypt data in users' devices is the decline in communication between law enforcement authorities and providers and suppliers of hardware and software. Whereas previously lines of communication between traditional service providers and governments were generally established, the pace at which new technologies and developers are entering the communications market has led to a significant decline in bilateral communication. These new private entities are not engaging in a dialogue with governments to the same extent as the traditional telecom service providers. This is suggested as a reason as to why fewer protocols to establish lawful access for law enforcement authorities through users' devices are being established.

2.2. **Working Group 2 - Data at rest in a provider's system**

2.2.1. What are the problems?

Working group 2 was tasked with taking stock of the current situation that law enforcement authorities across the Union face when attempting to lawfully access data at rest in a provider's system. A growing number of crimes occur solely online, and some form of access to data for law enforcement is important to many criminal investigations, including those focusing on offline crime. Many types of data can provide relevant leads – emails and messages, the identity of a subscriber, or the technical traffic and location data on when a message was sent, from which device, and where the device was located at the time. The group focused in particular on metadata generated in the context of telecommunications, whose retention by providers has been the subject of a number of judgments by the CJEU.

During the discussions, some participants referred to the March 2023 *Lisbon Declaration*[18], where the European Police Chiefs expressed their particular concern

[18] *Joint Declaration of the European Police Chiefs (Lisbon Declaration)*, March 2023; available at: Joint-Declaration-of-the-European-Police-Chiefs-Lisbon-Declaration.pdf (policiajudiciaria.pt).

about the national and international impact of the lack of clarity regarding data retention at the EU level for traffic and location data. This affected not only the accomplishment of their missions but the whole of society, bringing into question the impact on citizens' rights, freedoms and guarantees and, consequently, on the democratic rule of law since some types of crimes could only be prevented and investigated if meaningful non-content data retention was allowed.

Regarding accessing data at rest in a service provider's system, the first key issue that law enforcement authorities confront revolves around the divergent legality of both retaining data within providers' systems and the duration of such retention across the EU, as the regulatory and institutional framework for data retention across Member States is fragmented. The absence of harmonized EU-wide data retention legislation thus leads to the undesired consequence of lengthening or complicating investigations with a cross-border component. The law enforcement authorities' frequent need to resort to more intrusive methods of investigation (e.g., interception, DNA analysis), to compensate for shortcomings in data retention and access to data, can also be prejudicial to the rights of the persons subject to the measures concerned.

Secondly, law enforcement authorities also face difficulties relating to the metadata types retained by service providers. Where legal obligations exist, they at times leave flexibility as to the types of metadata that telecommunications service providers should retain, resulting in a variety of available data with different degrees of usefulness as investigative leads. Also, the inclusion of so-called 'Over-the-Top' service providers (OTTs) in the scope of national legal obligations is at times unclear or at least contested by some of those service providers.

The third issue, faced in practice by national legislators yet brought up as a challenge by law enforcement, is how to design lawful pathways through which law enforcement authorities can exercise their investigative powers, in line with the applicable data protection framework, including the CJUE case-law and applicable judicial procedural safeguards.

2.2.2. What are the problem drivers and legal constraints?

The first driver is that the current CJEU criteria limiting general and indiscriminate retention of traffic and location data under specific circumstances to fighting serious threats to national security and allowing targeted retention of such data for fighting serious crime only[19] do not establish a clear framework within which law enforcement authorities in the Member States can act in proportionate fashion when attempting to

[19] CJEU. (20 September 2022) *Judgment of the Court in Joined Cases C-793/19 | SpaceNet and C-794/19 | Telekom Deutschland,* [Press Release]. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220156en.pdf

access data retained on service providers' systems. Specifically, the concept of targeted data retention is proving very difficult for Member States to implement, and a lack of clarity concerning what types of data can be accessed for non-serious offences persists.

The shift to the use of services provided by OTTs has been a key driver of the difficulties that law enforcement face when attempting to access data stored on service providers' systems. OTTs have been brought into the scope of relevant EU legislation with the European Electronic Communications Code (EECC[20]); however, absent a comparable licensing system and – for many of them – local establishments, their obligations when it comes to data retention are at times unclear and some OTTs have contested or ignored such obligations. Additionally, certain OTTs sometimes retain no data whatsoever.

While a standard developed under the auspices of the European Telecommunications Standards Institute (ETSI) exists for traditional telecommunications metadata, it is far from universally applied across the Member States even with telecommunications providers, and there is no agreement on a standardised format for data transmissions from OTTs to law enforcement authorities. This adds complexity to the data analysis where data can be provided at all.

A further driver stems from the fact that many providers are based outside the EU. Within the context of Working Group 2, some practitioners reported that attempts, through mutual legal assistance treaties (MLAT), to access data that they have retained can take between 18 to 24 months in certain cases. The e-evidence package will increase the effectiveness of investigations significantly by allowing law enforcement and judicial authorities to request information from relevant third-country based providers offering their services in the EU and obtain a reply within 10 days. However, if the data has not been retained pursuant to national legislation or the retention period is very short, no matter what tool is used to address the provider, it may not be possible to obtain it. Given the wide diversity of obligations on service providers across the EU to retain data for a specific period of time, law enforcement and judicial authorities may also have difficulties to find out, before issuing a production or preservation order, if the data is still available.

[20] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

2.3. **Working Group 3 - Real time access to data in transit**

2.3.1. What are the problems?

Criminals frequently take advantage of opportunities offered by broadband communications systems to plan among themselves and to commit offences while seeking to avoid detection. In that context, real time access to data in transit remains an essential tool for the fight against serious online crime and organised crime as well as counter-terrorism.

Most Member States have dedicated national regulatory frameworks in place for real time collection of communication data. From a legal perspective, Member States can set obligations on communication service operators for real time access to data in transit, within the boundaries set by EU Law, notably the EU Charter of fundamental right, CJEU case law, GDPR and the ePrivacy Directive[21]. The latter allows for proportionate exemptions from the rule of confidentiality of communications, notably for the purposes of prevention, investigation, detection, and prosecution of criminal offences. Moreover, the 2018 European Electronic Communications Code (EECC[22]) allows Member States to impose obligations on operators of communication networks and services in compliance with the ePrivacy Directive and the GDPR.

The most pressing challenges for law enforcement authorities in this area are lawful real time access to data in transit from non-traditional service providers and access to data in readable format. In addition, operations conducted on networks specifically designed to provide anonymity and to be used for illicit purposes, such as Encrochat or Sky ECC, are a significant issue as traditional methods for obtaining access to real time communication data and metadata are not applicable.

2.3.2. What are the problem drivers and legal constraints?

The first driver is that regarding OTTs, Member States have difficulties enforcing obligations concerning the facilitation of real time access to communication data. While several Member States have established regulations which oblige OTTs to respond to lawful requests for such access, their successful application has been hindered. Like for access to data at rest, it has been reported that there is an uneven implementation between communication service providers (CSP) and OTTs of their national legal obligations on real time access to data, with some OTTs not implementing such obligations fully owing to legal and technical reasons. This results in a frequent lack of access to data in transit that has been processed by OTTs. However, challenges that law

[21] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[22] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

enforcement authorities face are not solely limited to OTTs. The increased use of rich communication services (RCS) to exchange SMS' in an end-to-end encrypted manner, increased 5G communication for inbound roamers and initiatives such as Apple Private relay, which cut CSP from the most relevant information[23], impact the ability of law enforcement to access real time data in transit effectively and lawfully.

The second driver is that, beyond technical problems, there is also legal uncertainty stemming from different requirements across national legal frameworks concerning interception. The EIO provides an effective tool for requesting interception by another Member State, as well as the exchange of evidence collected through interception. Nevertheless, like other similar instruments, the EIO does not regulate the admissibility of such information and leaves that to national law. This issue has been recently brought before the CJEU.[24] International cooperation with third countries on communication intercepts provides challenges as implementing such a measure through MLA, where it is available, can be very time consuming and may keep investigations from proceedings at the desired pace. challenges as implementing such a measure through MLA, where it is available, can be very time consuming and may keep investigations from proceedings at the desired pace.

A third driver is that differences in the legal frameworks of EU Member States on interception of metadata or content data creates challenges for law enforcement in cases with cross-border elements. For instance, it may be difficult for law enforcement authorities to intercept in real-time communications between two citizens in their country where the communication service these citizens use is hosted in another EU Member State and that Member State has different procedural requirements for live interception that are difficult to meet. This is especially the case where that Member State does not participate in the EIO Directive or where the service provider is based in a third country. Cases like Encrochat or Sky ECC, where the interception targets broadly users of a criminal communication networks that are subject to different jurisdictions, bring another level of complexity into this debate.

[23] For example, Apple Private Relay is designed to ensure that technical attribution (linking an online activity with a user) is not feasible (see https://support.apple.com/en-us/102602)

[24] In the case C-670/22 | Staatsanwaltschaft Berlin (EncroChat) that the CJEU is examining, a German Court asked the CJEU if the European Investigation Orders issued to obtain data originally obtained in another EU Member State through interception measures were in breach of the European Investigation Order (EIO) Directive. In a recent Opinion of 26 October 2023, the Advocate General recalled that an EIO may only be issued if the investigative measure it entails could have been ordered under the same conditions in a similar domestic case. In the case at hand, a similar domestic case is one where evidence is transferred from one criminal procedure to another within Germany. The Advocate General thus concluded that the German Public Prosecutor was entitled to issue the EIOs at issue. The Advocate General found that because the interception of telecommunications was authorised by French courts, the German authorities should attribute to that procedural step the same value as they would domestically. The Advocate General indicated that the admissibility of evidence received potentially in breach of EU law is not a matter of EU, but of national law, subject to compliance with fundamental rights guaranteed by the EU legal order.

2.4. **Problem Categories and Drivers**

The following table presents **the main problem categories and underlying drivers as well as legal constraints** identified across the three Working Groups.

Problem Categories	Problem Drivers and Legal Constraints
Gaining lawful access to user devices	• Law enforcement authorities across the union are subject to differing national legal frameworks concerning lack of suspect cooperation. Some frameworks are more permissive whilst others are more restrictive. Many of the more restrictive frameworks are considered inadequate by the respective affected law enforcement authorities. • Rules on and methods employed for accessing communications data must comply with the principle of *nemo tenetur* to ensure the admissibility of evidence in court. • There is a lack of regulatory clarity regarding the use of OSINT to gain access to user devices.
Decrypting content data and metadata available on user devices	• Ongoing technological developments in encryption are making commercial decryption tools less effective. • Commercial decryption tools are expensive and are often developed outside the EU so may not comply with accountability and forensic standards within the Union. • Sharing of bespoke decryption tools is hampered, either by a lack of communication and trust between law enforcement authorities, or prohibitions on the decryption tools being shared. • Communication between law enforcement authorities and providers of hardware and software has declined, leading to fewer protocols for lawful access to user devices being established.
Enabling the lawful retention of data in the systems of service providers	• Rules on data retention across the EU are not harmonised. • Law enforcement authorities and service providers face difficulties in making use of the possibilities targeted retention for location and traffic data. • Member States are finding it more difficult to implement data retention obligations on OTTs than on traditional telecommunication companies. • Certain OTTs do not retain any data at all.
Accessing data that has been lawfully retained by service providers	• There exists no agreed standardised format for data transmissions from OTTs to law enforcement authorities.

	• OTTs are often based outside the EU, and requests by law enforcement authorities for access to data retained can be subject to long waiting times or obstacles.[25]
Coordinating lawful access to data in transit with service providers	• Member States struggle to enforce legally mandated obligations on real time access to communication on OTTs, partially due to blocking statutes of third countries in which these companies are based. • The pace at which international cooperation requests via MLA concerning communication interceptions are processed, and the inability for some third countries to respond to such requests, affects the speed at which investigations can proceed.
Decrypting and utilising lawfully intercepted data in transit in real time	• End-to-end encryption as an industry standard has impacted law enforcement authorities' ability to make intercepted data readable. • Different legal requirements across national legislatures may result in legal uncertainty on the applicable procedures to obtain evidence from other EU Member States and its admissibility and probative value in judicial proceedings.

3. Questions

With the above table setting out the key problem categories and drivers, alongside the legal constraints governing access to data that transpired from the discussions in the three Working Groups in mind, the following questions have been prepared for discussion during the Plenary.

1. *Does the Plenary agree with the problem categories and drivers as well as the legal constraints and principles governing access to data that have been mentioned in the table? Are there any further categories or drivers that should be addressed within this table.*

2. *With the problem categories, their drivers, and relevant legal constraints set out, what are the possible solutions for these issues that the respective Working Groups should explore in their second meetings? Within this context, please consider the legal, technological, pubic-private, and international dimensions of any proposed solutions.*

[25] These obstacles can be the voluntary nature of cooperation by service providers in some cases, delays in the MLA process, or blocking statutes in third countries.

ANNEX 1

Definition of the 4 Workstreams based on Council Scoping Paper 8281/23 for the High-Level Expert Group on access to data for effective law enforcement

WORK STREAMS

The High-Level Expert Group has been tasked with mapping, assessing, and prioritising the relevant issues that were examined and identified across the various Working Groups. It seeks to look at solutions for the selected issues from 4 angles:

a) The Legislative aspect
b) The Technological aspect
c) The Public-Private cooperation angle
d) The International Cooperation angle

Legislative aspects

The HLEG has assessed 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.

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 also 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.

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,[26] 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.

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

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[27]. 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 seek to discuss technological solutions for improving law enforcement authorities' ability to lawfully access data. One of these oughts to be 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.

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 important 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.

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.

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[28] and at international level[29], 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 seek to discuss solutions related to 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.

[27] 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.

[28] Such as the internal EU e-evidence package.

[29] 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.