Council of the European Union

Brussels, 8 May 2020
(OR. en)

7675/20

LIMITE

CT 24
COSI 66
CATS 27
ENFOPOL 101
TELECOM 56
CYBER 63
IXIM 48
JAI 326

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Law enforcement and judicial aspects of encryption

Introduction

Some emerging trends in encryption[1] have gained a lot of attention lately. Several recent changes to the encryption practices of service providers [online service providers (OSPs) and telecommunication providers], including many more planned to be implemented in the coming months, have been in the international news and prompted public responses from governments, particularly among partner countries such as the US[2].

1 Strong encryption was recognized by the Commission's 2017 Cybersecurity strategy as "the basis for secure digital identification systems that play a key role in effective cybersecurity; it also keeps people's intellectual property secure and enables protecting fundamental rights such as freedom of expression and the protection of personal data, and ensures safe online commerce" JOIN(2017) 450 final; Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defense: Building strong cybersecurity for the EU; 13.9.2017, which likewise recognizes the vital importance of encryption in protecting the private data of EU citizens and of ensuring a robust security infrastructure in cyberspace.

2 In July 2019 US Attorney General, William Barr publicly raised the serious problems caused by increasing trends of encryption for law enforcement and urged technology companies to address law enforcement concerns (https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber), which was subsequently supported in comments made by the EU CTC (https://www.consilium.europa.eu/en/policies/fight-against-

This paper aims to present the state of play of the evolving issues in the field of encryption that are disrupting the ability of Member States and EU Agencies to carry out their vital **law enforcement and judicial roles** through limiting the possibility for **lawful access to data** (in transit - lawful interception - or at rest, including in clouds) **that they currently have at their disposal**[3]. The technical addendum includes more detail on the various forms of encryption.

The note also intends to stimulate a discussion of the proposed recommendations in COSI, on steps the EU and its Member states can take to address the situation, notably **legislative solutions**, but also by **proactively engaging at technical level with service providers**. It thereby hopes to contribute to continue to develop effective responses towards the evolving trends of encryption at the European level, to position the EU and its Member States not only as the protectors of their citizens' personal data[4], but also of their security, including victim's rights and to ensure that law enforcement does not lose valuable tools because of technological developments. Impunity for serious crimes must be avoided.

---

terrorism/counter-terrorism-coordinator/). A joint open letter by the UK Home Secretary, US Attorney General and Secretary of Homeland Security and Australian Minister for Home Affairs was published in October 2019 in response to Facebook's 'Privacy first" proposals, and urged that "Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes. This puts our citizens and societies at risk by severely eroding a company's ability to detect and respond to illegal content and activity".

3 European Union's Agency for Fundamental Rights (FRA) 2017 Fundamental Rights Report; p. 159.

4 As stipulated in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) and in 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 (Directive on privacy and electronic communications).

The hitherto unmatched pace of the roll-out of these encryption practices and their ability to create *de facto* standards across the next generation of technology in an industry-driven and focused approach, which excludes many stakeholders most notably law enforcement and the judiciary, represents a massive challenge. The forthcoming expansion of the Internet-of-Things and 5G[5] will only make the problem more serious and require an inclusive and comprehensive dialogue. The window of opportunity to respond to these challenges regarding lawful access, including interceptions is rapidly closing. In addition to criminal abuse of encryption, law enforcement agencies face other challenges such as criminal abuse of crypto currencies, privacy-enhancing and anonymity technologies (e.g. TOR) in combination with legal challenges such as data retention, which are beyond the scope of this paper but taken together increase the urgency to act to preserve law enforcement and judicial capabilities and avoid impunity.

There is, therefore, an **urgent** need to take stock of these rapidly evolving trends, and form a robust response to unfettered encryption by service providers and the standards bodies that regulate them to preserve lawful access of law enforcement and the judiciary and avoid impunity.

1. EU Action on encryption so far

Encryption in itself should be regarded as **a common good** and yields important benefits in terms of strengthening cybersecurity and reinforcing privacy. EU institutions have repeatedly expressed support for strong encryption along with the need for a **balanced approach** between citizen's privacy protection and law enforcement's need for access to data[6].

---

5 See 8983/19; Law Enforcement and judicial aspects related to 5G; 06.05.2019. Within the 3rd generation partnership project (3GPP) which develops standards for the 5G technology, one technical specification group is in charge of norms on service and systems aspects (SA) and has a working group specifically tasked with security (SA3). The sub-WG SA3-LI provides the requirements and specifications for lawful interception in 3GPP systems. It is critical to ensure adequate representation in those fora to ensure that standards are defined and implemented in a manner that meets the requirements of law enforcement.

6 Regulation 2016/679 (GDPR) Art. 32 considers encryption as one of the "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" of data processing. In the outcome of the proceeding of the JHA Council of 8 December 2016, it is mentioned that Ministers were "in favour of continuing the discussion in order to identify solutions that struck a balance between individual rights/citizens' security and privacy and allowing law enforcement agencies to do their work".

The EU has already taken steps to tackle the challenges of widespread encryption. At the JHA Council in December 2016, EU Justice ministers discussed the challenges of criminal justice in relation to the use of encryption technologies, based on a report from the Slovak presidency that devised a four step approach[7]. In June 2017, the European Council conclusions on security and defence stressed that an effective fight against terrorism and crime online "call[ed] for addressing the challenges posed by systems that allow terrorists to communicate in ways that competent authorities cannot access, including end-to-end encryption, while safeguarding the benefits these systems bring for the protection of privacy, data and communication." An action plan was set out by the Commission in 2017[8], and the issue of encryption continues to be discussed at technical level with law enforcement agencies and Members States[9] or recently in the TELECOM Working Party[10].

---

7 see 14711/16, " Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report"; 23/11/2016. The 4-phased approach comprised (1) a "reflection process under the flagship of the Commission […] with the purpose to define practical solutions that would allow the possible disclosure of encrypted data/devices", (2) the improvement of expertise at EU and national level " to face current and future challenges stemming from encryption", (3) a discussion on encryption challenges by the members of the European Judicial Cybercrime Network and (4) the deepening of " the practical/operational aspects of the encryption-related trainings for law enforcement authorities provided by EU entities".

8 COM(2017) 608 final; Communication from the Commission to the European Parliament, the European Council and the Council - Eleventh progress report towards an effective and genuine Security Union; 18.10.2017. The report called for 1) the granting of EUR 5 million to Europol's decryption program; 2) the development of a toolbox of alternative investigation techniques; 3) wider stakeholder dialogue with service providers and industry partners; 4) additional funding of EUR 500,000 for training for law enforcement under the 2018 annual work programme of the Internal Security Fund Police; 5) an establishment of an observatory function overseeing continuous assessment of technical and legal aspects; and 6) the development of a network of law enforcement actors.

9 For example the High-level stakeholder dialogue on encryption with prosecutors, DG HOME and DG JUST (13 November 2019) in The Hague.

10 see Commission working paper 1939/2020 INIT "Deployment of DNS-over-HTTPS - Background paper from the Commission" which aimed at informing the discussions of the 18 February 2020 TELECOM Working Party.

Europol and Eurojust now publish a yearly observation report on encryption and its impact on investigations and prosecutions (so far two such reports have been prepared[11]), as well as a joint report on the common challenges in combatting cybercrime[12]. In November 2018, the CATS invited the Commission to develop further the solutions to end-to-end encryption (E2EE) which had been discussed at technical discussions with Member States and Commission experts at Europol[13].

The Commission has provided a grant of €5M to Europol's European Cybercrime Centre (EC3) to develop their technical capabilities to tackle device encryption, including the setting up of a new decryption system in cooperation with the Joint Research Centre (JRC) of the Commission[14]. The Commission (via Internal Security Fund-Police) has also given one grant (and will give another one later this year) to the European Cybercrime Training and Education Group[15] (ECTEG) to develop and deliver training courses related to encryption, i.e. from non-specialist police officers to forensics experts.

On 8 October 2019, the Council in its conclusions on combating child sexual abuse stated: "The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full respect of privacy and fair trial guarantees consistent with applicable law."

---

11 *First report of the observatory function on encryption*, joint report by Europol and Eurojust, January 2019
Second report of the observatory function on encryption, joint report by Europol and Eurojust, February 2020

12 https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime

13 See 14654/18 CATS 21 November 2018 *Summary of discussion.*

14 COM(2017) 608 final; Communication from the Commission to the European Parliament, the European Council and the Council - Eleventh progress report towards an effective and genuine Security Union; 18.10.2017.

15 The ECTEG is composed of European Union and European Economic Area Member States law enforcement agencies, international bodies, academia, private industry and experts. It aims at providing training and education material to international partners, harmonizing cybercrime training internationally, sharing knowledge and collaborating with industry and academia. The ECTEG works in close cooperation with Europol EC3 and CEPOL, which are both members of its advisory group.

On 11 December 2019, the United States and EU stated that: "We also acknowledged that the use of warrant-proof encryption by terrorists and other criminals – including those who engage in online child sexual exploitation – compromises the ability of law enforcement agencies to protect victims and the public at large. At the same time, encryption is an important technical measure to ensure cybersecurity and the exercise of fundamental rights, including privacy, which requires that any access to encrypted data be via legal procedures that protect privacy and security. Within this framework, we discussed the critical importance of working towards ensuring lawful access for law enforcement and other law enforcement authorities to digital evidence, including when encrypted or hosted on servers located in another jurisdiction."[16]

The increasing use of encryption protocols by service providers however shows that the EU now needs to **go further and address the wider trends in this regard**. Strengthening the EU response to heightened encryption practices is necessary and urgent to prevent access to relevant criminal data from becoming more difficult than it already is or even impossible. Now is the time for the EU to act on this.

2. Encryption practices - state of play

Encryption is not a monolithic field. It is crucial to understand that issues stemming from the use of encryption are distinct from one another and involve completely different incentives for the concerned parties. They should therefore be dealt with separately in order to tailor distinct responses to each type of encryption usage.

The types of encryption usage most relevant for the law enforcement and judicial authorities may be broadly categorised into five main groups: 1) **device encryption**; 2) encryption of **communications**; 3) **custom encryption applications**; 4) **encryption across integrated platforms**; and 5) **the encryption of the protocols underpinning the basic functioning of the Internet**. Encryption, therefore, aims at protecting access to data whether this **data** is **at rest** (e.g. stored on a device, on a server or in the cloud) or whether it is **in transit** (actively moving from one location to another). A detailed description of these five types of encryption usage is provided in the Addendum to this paper.

16 https://www.consilium.europa.eu/en/press/press-releases/2019/12/11/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting/

The widespread use of encryption across these five domains should be recognised as part of **a wider trend**, by which service providers are **unilaterally implementing** changes to their encryption practices, **without actually engaging with the EU or Member States to address concerns of law enforcement and judicial authorities in the roll-out**[17]. The direct consequence of these changes is that even if the law authorises interception of communications and the interception is warranted by a judge, prosecutor, or similar function required by Member States legislations in a specific case, it still cannot be carried out because of encryption technology and the way it was implemented by industry.

In a recent high level stakeholder dialogue meeting[18] organised by DG HOME, Eurojust and the European Judicial Cybercrime Network within Eurojust in the presence of DG JUST, prosecutors from various Member States reiterated their concern that the recent developments in all fields of encryption might lead to LEAs becoming **incapable of accessing data necessary for criminal investigations and prosecutions despite having the legal power to do so**. The discussion highlighted that most existing solutions to bypass encryption (which do not work in all cases) are resource intensive, often extremely costly and can only be used for some high value targets, with some countries pointing to their limited forensic capabilities and the fact that increasing investment in these capacities is met with ever decreasing results. The discussion also stressed that the industry should play a stronger role in allowing lawful access for LEAs.

---

17 Rene Mayrhofer, Google's Director of Android Platform Security, commented that locking out law enforcement was an "unintended side effect" of its latest security features, see https://www.vice.com/en_us/article/yw8vm7/android-security-locking-out-law-enforcement-unintended-side-effect.

18 High level stakeholder dialogue on encryption with prosecutors, DG HOME and DG JUST (13 November 2019) in The Hague.

In Australia, the Assistance and Access Act 2018[19] introduced a warrant system with three levels of technical warrants (technical assistance request, technical assistance notice and technical capability notice). The third level warrant, issued with the appropriate safeguards, can force any company to submit data in unencrypted form as long as the device / data requested has been specifically identified[20]. In the UK, under Section 253 of the Investigatory Powers Act (2016), a telecommunications or postal operator can be served with a "technical capability notice" issued by the Secretary of State following the approval of a Judicial Commissioner. The technical capability notice can force the provider to comply with any obligation it dictates, including "obligations relating to the handling or disclosure of any information".

---

[19] The Assistance and Access Act (2018) allows law enforcement officials to ask a judge for a warrant and require evidence from tech companies through three possible channels:
(1) a technical assistance request which allows LEAs to request voluntary assistance from a company to submit information that they can easily access/is in their technical capability,
(2) a technical assistance notice by which the company is served with a notice that requires it to help law enforcement. This is used in case the company needs to be compelled to cooperate (e.g. due to shareholders' disagreement). The company can then be protected from liability for submitting the requested data,
(3) a technical capability notice which can only be issued at the joint request of the Attorney General and the Minister for Communications. It requires a provider to develop a new capability where the provider is not already capable of offering that type of assistance, such as asking Apple to open up one of its phones or keep a specific phone out of an update package. Providers may only be asked to build or use capabilities that can provide targeted access to data where this does not remove electronic protection or jeopardise the information security of general users. The device or communication needs to be specifically identified. The technical capability notice has never been used so far.

[20] See UK Investigatory Powers Act (2016), Australian Assistance and Access Act (2018).

With the EARN IT Act, bipartisan legislation has recently been introduced in the US Senate to ensure a first step related to higher level of scrutiny on some limited aspects of encryption practices[21] and has paved the way for a broader legislative debate on encryption in the US while not yet proposing legislation to deal with broader aspects of encryption.

Facebook's planned 'privacy-focused' move (which includes end-to-end encryption applied by default to all messages sent via Facebook Messenger) offers an opportunity to engage Facebook directly on the issue. The potential roll-out by browser-makers of encrypted internet protocols[22] in European markets, following trials in the US in 2019, presents a similar opportunity. It is important to keep in mind that the business model of companies which relies on access and analysis of public and private user data remains intact despite encryption of some services such as the Facebook Messenger App.

It is high time to examine these encryption practices and the political and legislative responses to them in detail; and develop **a comprehensive approach** to address all aspects of the widespread adoption of encryption. Relevant stakeholders including EU institutions, Member States and their law enforcement and judicial agencies, EU JHA Agencies, service providers should be engaged in a constructive dialogue, in the perspective of legislative action. This would help break the trend of unregulated encryption practice and aim towards a robust EU regulatory framework which both addresses citizens' legitimate privacy concerns, and the concerns of LEAs which are increasingly encountering the problem of being unable to prevent and investigate criminal activity.

---

21 See draft bill (OLL20148) introduced by Sen. Lindsay Graham and 9 cosponsors: *Eliminating Abusive and Rampant Neglect of Interactive Technologies* (EARN IT) Act of 2019. Aimed at combatting child sexual exploitation, the bill sets up a National Commission on Online Child Sexual Exploitation Prevention which will be tasked with drafting best practices "that providers of interactive computer services may choose to implement to prevent, reduce, and respond to the online sexual exploitation of children". Any online service provider which currently cannot be prosecuted for the content it hosts thanks to an immunity under Section 230(e) of the Communications Decency Act of 1996 will now be held accountable for unlawful content published on the site by its users if it hasn't complied with the best practices defined by the National Commission. Internet companies would therefore have to "earn" their exemption from liability under section 230. It is expected that implementing additional encryption protocols could be considered by the National Commission as going against those best practices.

22 For more details on encryption of internet protocols, including DNS over HTTPS, please see the addendum.

3. Reframing the debate: Explaining the law enforcement and judicial perspective

The result of such unilateral changes in encryption practices has been to create a **persistent narrative** that places service providers, whose entire business model is sometimes built on the exploitation of users' data, as the protectors of users' private data. Governments and international institutions, including law enforcement and judicial authorities, are meanwhile portrayed by the technology companies as challengers to citizens' privacy and data protection. This is concerning.

It must be reiterated that **data protection, respect for privacy and the importance of encryption in ensuring modern, secure and ethical technological change, remain at the forefront of the EU's legal framework**. One cannot have privacy without security and safety and vice versa.

Thus, law enforcement agencies seek to fight impunity, apprehending offenders while following due process. Whatever the level of technological development may be, it is essential for governments to be able to investigate and prosecute serious crime, which requires enforcing existing laws on lawful interception, to keep citizens safe. It should also be noted that access to electronic evidence is central to ensure a fair trial and can benefit not only the rights of victims but also of criminals (through the discovery of exculpatory evidence).

4. Way forward

4.1 Guiding principles for an optimal solution

An **optimal solution** to the problem is one that would **allow users to enjoy the benefits of encryption** with regards to privacy and data protection **while allowing law enforcement agencies to preserve their capability to lawfully intercept** communications or **gain lawful access to encrypted devices and encrypted data** when this is warranted by a judge, prosecutor, or similar empowered official. Given the complexity of the issues, this needs to be an ongoing process, which should also include risk and impact assessments and regular reviews. It is relevant to break down the encryption challenge, yet all the five forms of encryption need to be addressed[23].

---

[23] In a contribution to the debate on encryption, the Carnegie Endowment for International Peace suggested that the effort should focus on data at rest in mobile devices, which they regard as "the area most likely to enable fruitful debate among diverse communities-of-interest and most likely to lead to clearer characterization of risks and benefits." However, such an approach would not be sufficient. Carnegie Endowment for International Peace, Encryption working group, *Moving the encryption policy conversation forward*, September 2019. The East West Institute has also made a contribution to the debate: East West Institute, *Encryption policy in Democratic Regimes: Finding convergent paths and balanced solution*, 2018.

Preliminary analysis carried out by Commission services suggests that such a solution would need to respect the following **guiding principles**:

- Solutions constituting a **blanket weakening**, **banning or limiting of encryption**, such as the creation of a so-called 'backdoor'[24] (permanent access point) for LEAs **should not be supported.**
- **Upon lawful request**, issued or validated by a judiciary authority, **companies that are providing encryption services should be able to provide data in readable format[25].**
- Solutions for access to encrypted information by authorities should be **targeted**, deployable in the **least intrusive** way possible, and only where there is a **legitimate need backed by the appropriate legal authorisation**, together with transparent reporting and legal redress.
- Technical solutions for access should benefit from **state-of-the-art security measures** in order to avoid introducing weaknesses and should adapt to the architecture and business model of the service provider. Companies providing encryption for their products will often be best placed to identify the best and most secure technical solution.
- Appropriate **safeguards** are required, commensurate with the level of intrusiveness, which may vary according to the type of encryption and should include the possibility for judicial review.
- The **non-proliferation of the tools** that law enforcement use **to bypass encryption** should be ensured. This will help prevent the unfettered exploitation of these tools by malicious actors and the global weakening of encryption because of them.

---

24 It is important to distinguish between Back-Door (allows a third party to gain unlimited access to IT systems or to application functions unnoticed and unauthorised by the user and provider bypassing all security features (e.g. authentication, logging, encryption of the connection) and Front-Door (unnoticed only by the unnoticed only by the user and within the context of the intended scope of functions, this allows a third party to gain authorised and unlimited access to IT systems or application functions by means of the security features included by the provider (e.g. authentication, logging, encryption of the connection.)

25 Hence, a Front-Door approach should be sought.

4.2 Recommendations

(1) Explore regulatory solutions to protect lawful access

First of all, the EU should pursue **regulatory measures**[26]. Legislation is needed to address the problem of encryption. Some of our key partners have already taken steps in that direction. The EU too should now look to legislate in this domain and define the "European way" of regulating encryption. A legislation requesting access, upon lawful mandate, to electronic evidence in unencrypted, readable form was one of the demands set out in a recent joint declaration of the European chiefs of police with regards to 5G[27]. General principles on obligations of service providers to provide readable, unencrypted access could be set out in the planned Digital Services Act.

The EU could also explore the possibility to increase transparency and reporting obligations for service providers with regard to the evolving technical and technological aspects of encryption practices in the context of preventing and supporting the fight against criminal activities.

The EU can leverage the strength of its single market to ensure device manufacturers and service providers create technologies that meet law enforcement needs in the future while preserving the benefits of privacy.

(2) Political discussion of encryption issues

Member States and JHA Agencies should **reflect and engage in COSI** on challenges that emerging encryption pose to the ability of law enforcement and judicial authorities to fulfil their functions. Raising awareness around this issue is particularly critical to increase the collective understanding of the issue and develop appropriate solutions at EU level.

---

26 The draft e-evidence regulation currently being discussed in the European Parliament states that data should be provided regardless whether it is encrypted or not (recital 19), but does not further address encryption, which requires a specific response. COM/2018/225 final - 2018/0108 (COD), Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

27 Joint Declaration of the European Police Chiefs on 5G, 2 September 2019: "Legal obligation for electronic communication providers to extract a complete, (near) real time and unencrypted surveillance copy, legal obligation to cooperate with lawful technical investigative measures."

(3) Build an updated picture of the field of encryption at EU level through a multi-stakeholder dialogue and engagement

On a more technical level, enforcement and judicial authorities of Member States and EU JHA agencies, in particular Europol and Eurojust, should continue the dialogue to understand the most pressing issues regarding encryption. In addition to the observation reports on encryption by Europol and Eurojust, together with the COM, Europol and Eurojust have started a dialogue with Member States LEAs and prosecutors to understand their needs and for them to share their practical difficulties as well as legal challenges[28]. This forum could now meet regularly and be opened more broadly to technical experts from other EU agencies and bodies (eu-LISA, ENISA, EDPS…) for a more comprehensive approach to these issues. The future **EU innovation hub** for JHA Agencies could be a relevant stakeholder to address this issue and offer an assessment of possible solutions.

This multi-stakeholder dialogue should be informed by a forward-looking function based on the annual observatory function report to identify current and upcoming developments with a view to developing a pro-active and multi-faceted response.

(4) Direct engagement with service providers

The EU should **work together with the service providers operating across Europe** throughout their process for the creation of encrypted tools, to agree on and comply with an approach that ensures lawful access to data is not impinged. This direct engagement should be held at a technical level so as to be able to assess critically the technological solutions that may be advanced by industry players.

After legislation with legal obligations to provide access in readable format is in place, the dialogue would primarily deal with the "how". Creating the additional legal obligation for providers to engage with regulators on a technical level and be transparent on the features of their encryption technologies would favour mutual understanding between regulators and service providers and facilitate the enforcement of existing legislation on lawful interception.

---

[28] Such as the legal obligation for LEA to disclose approaches to access encrypted data in court

(5) Influence standard setting within international bodies

Member states and EU Institutions should be encouraged to **collectively challenge** changes to the encryption landscape in **the international standards bodies**, particularly the Internet Engineering Task Force (IETF) to ensure they are involved in the development of international standards and technological norms, impacting encryption and wider cyber security for the years to come. This is especially important with regard to evolving encryption of fundamental internet protocols. Similarly to the approach on 5G[29], the Commission could explore to finance the participation of law enforcement from Member States and Europol in standard setting bodies.

(6) Strengthen training to improve law enforcement's understanding of these issues

Along with other issues related to new technology, addressing the criminal abuse of encryption needs to be even more incorporated in law enforcement training. Stepping up **CEPOL's training programs** in this field would allow to increase the understanding of law enforcement officials throughout Europe of encryption and their knowledge of the most recent developments and techniques with regards to tackling encrypted devices or communications, including better exploiting data other than encrypted content data, such as metadata. Measures to avoid the proliferation of such techniques would need to be part of the training.

(7) Inform the public debate about the law enforcement and judicial perspective and the need to avoid impunity

The EU and its Member States should seek to be increasingly present in the public debate on encryption, in order to **inform the public narrative** on encryption by sharing the law enforcement and judicial perspective and explaining the need to avoid impunity in line with European values and EU law. This avoids a one-sided debate mainly driven by the private sector and other non-governmental voices. This may involve engaging with relevant advocacy groups, including victims associations that can relate to government efforts in that area. Engagement with the EP will also be key to prepare the ground for possible legislation.

---

[29] In the wake of EU CTC and Europol's alert on potential unable lawful interception in 5G infrastructures, the Commission has taken specific measures, amongst which the funding of attendance of law enforcement representatives at the 3GPPP ad hoc working group (SA3-LI).

5. Questions for discussion

Delegations are invited to reflect and express their views on the following questions:

- What are the most pressing challenges related to the use encryption that law enforcement and judicial authorities are facing in your Member State? How are your national authorities tackling or planning to tackle these challenges?
- What is your view on the proposed guidelines for an optimal solution?
- How the EU can best support Member States to address these challenges? What is your view on the proposed recommendations?