Questionnaire on improving criminal justice in cyberspace

Summary of Responses

The Commission services circulated a questionnaire on cross-border access to electronic evidence amongst Member States, which was developed taking into account previous and ongoing activities, including the GENVAL evaluation, and sought to complete the picture. The questionnaire was launched on 29 July 2016 and closed in October 2016. The detailed replies received from **27 Member States** (all except **PL**) provided valuable additional information which is reflected below. The national replies were coordinated at national level amongst different responsible ministries, the judiciary and law enforcement authorities, providing a comprehensive overview of the current state of play within the Member States.

The questionnaire focusses on current practices in the Member States concerning 1) **direct cooperation** between law enforcement authorities and private sector service providers, 2) **mutual legal assistance** or mutual recognition procedures and 3) **enforcement of jurisdiction in cyberspace**, namely other measures that law enforcement authorities could use to obtain e-evidence in cases when it is not clear they would operate within their own jurisdiction.

The replies revealed that there is **no common approach** to obtain cross-border access to digital evidence, for which each Member State has developed its own domestic practice. There is a large variety of approaches adopted by the Member States' law enforcement and judicial authorities as well as by the service providers. This diversity, which seems mainly due to the lack of a legal framework and of a common approach on how to access e-evidence and deal with requests to share information, creates legal uncertainty for all the stakeholders involved and represents an obstacle to joint and cross border investigations.

Direct cooperation, in particular when the service provider is outside the domestic jurisdiction

Criteria to distinguish between domestic and foreign service providers when making a request

• EU Member States and their judicial and law enforcement authorities have taken diverging approaches as regards the use of the connecting factors for the exercise of an investigatory measure allowing for access to e-evidence. There are different ways of determining whether a provider is to be considered domestic or foreign and the criteria to distinguish between domestic and foreign service providers vary significantly among the Member States, ranging from the "*main seat of the service provider*" (**AT, RO, HR, SK, IE, NL, EL, CZ, DE, DK, ES, SI, IT, EE, FR, LT, LU, MT, HR, BG**) and "*the place where services are offered*" (**SE, BE, LV, CZ, ES, PT**) to "*the place where data is stored*" (**AT, HU, HR, CZ, DK, LU, FR**) and a *combination of alternatives*. Regarding the business link, currently there is no common understanding amongst countries what constitutes the offering of services in a territory.

Normal practice within domestic jurisdiction

• Regarding the normal practice within domestic jurisdiction, whereas the results indicate that at least 20 Member States do not use different definitions for service providers in relation to investigatory measures used to obtain access to e-evidence (**AT, HU, SE, BE, NL, LV, DK, ES, EL, PT, FI, UK, IT, EE, FR, LT, SK, LU, IE, SI, HR**), at least 6 Member States indicated to use different definitions in relation to investigatory measures used to obtain access to e-evidence (**DE, RO, HR, CY, CZ, MT**).

Voluntary v Mandatory cooperation

• 17 Member States (**AT, RO, SE, HR, NL, EL, LV, CZ, DE, DK, FI, SI, IT, EE, LU, MT, BG**) indicated that they consider direct requests sent from national authorities directly to a service provider in another country as **voluntary** for the provider to comply with, while at least 7 Member States (**BE, CY, ES, PT, UK, FR, LT**) indicated that orders served on services providers not present in the territory are considered as **mandatory**.

• Even when this mechanism is considered mandatory, it is very difficult to assess whether the Member States can actually **enforce** it. This is also due to the lack of a specific legal framework for these requests: **AT, RO, BE, HR, IE, NL, EL, LV, CZ, DE, DK, ES, FI, PT, SI, UK, IT, EE, FR, LT, LU, BG** apply to these cases the same framework as for domestic requests. At least 3 Member States indicated that the direct cooperation with service providers in other countries is regulated specifically (**SE, CY, MT**).

• Only a few countries (**SE, BE, NL, CZ, FR, PT, IT, LT**) have concluded (informal) agreements with foreign service providers, while 18 Member States indicated they haven't (**AT, SI, FI, ES, DK, RO, HU, HR, EE, CY, SK, IE, EL, LV, DE, LU, MT, BG**). **UK** referred to the planned UK-US agreement.

Ability of service providers to respond to requests

• The majority of national legislations (**AT, RO, HU, SE, BE, HR, CY, SK, NL, EL, LV, DE, DK, FI, PT, SI, UK, IT, EE, LT, LU, MT, IE, BG**) do not cover/allow that service providers established in the Member State respond to direct requests from law enforcement authorities from another EU Member State or third country. Moreover, the domestic law of only 2 Member States allows service providers established in those countries to cooperate directly with law enforcement authorities from other Member States or third countries (**ES** and **FR**).

Definition of types of data

• The **definition** of types of data (subscriber, traffic and content data) varies significantly among Member States, while specific categories of data exist in several countries. It appears that at least 14 Member States use a definition of subscriber data (**AT, RO, SE, EL, LV, DE, DK, ES, FI, PT, SI, UK, MT, BG**), 17 Member States use a definition of traffic information (**AT, RO, SE, BE, SK, EL, LV, DE, DK, ES, FI, PT, SI, UK, LT, MT, BG**) and 9 Member States use a definition of content data (**AT, RO, EL, DE, DK, ES, FI, FR, MT**). At least 5 Member States do not have any definition of data categories: **HU, HR, IT, EE, LU**.

Data requested directly from service providers are generally subscriber (**AT, RO, HU, SE, BE, HR, CY, IE, NL, EL, LV, CZ, DE, ES, PT, SI, UK, IT, EE, FR, LT, LU, MT**) and traffic data (**AT, RO, HU, BE, HR, CY, IE, NL, EL, LV, CZ, DE, ES, SI, UK, EE, FR, LT, LU, MT**), while in a few Member States it is also possible to request content data (**BE, CY, IE, NL, LV, DE, ES, EE, LT, LU**) and "other data" (**SK, EE, DE, DK, MT**), specifically in emergency situations.

Current practices regarding procedures, means of transmission, responding time

• Practices also diverge as regards the **procedures** for making the direct requests, i.e. the authority which can initiate the process (generally the police, followed by the prosecutor and the judge), the modality for launching a request or transmitting e-evidence (normally via email or web portal, but in some other cases with paper or fax or via all the possible means). The only common feature seems to be the lack of a central repository in the Member States.

• There is no common approach on how the service providers react to requests from foreign law enforcement authorities and it appears they respond differently depending on which country requests come from, with a minimum responding time of a few minutes in certain countries to a maximum of 1 month or more in others.

Ability of law enforcement to make a request

• The questionnaire indicate that at least 18 Member States allow for their law enforcement authorities to cooperate directly with service providers in other Member States and third countries (**SE, BE, HR, CY, NL, EL, LV, DE, DK, ES, FI, UK, IT, FR, LT, LU, MT, BG**). However, at least 5 Member States indicated that they only allow for their law enforcement authorities to cooperate directly with service providers in third countries (**AT, RO, PT, SI and EE**). At least 3 Member States indicated that they do not allow their law enforcement authorities to make requests for direct cooperation by service providers in any other country (**HU, SK and IE**).

Admissibility in Court

• Admissibility in Court of e-evidence gathered outside the MLA mechanism does not generally constitute a problem for the majority of Member States (**AT, RO, HU, BE, CY, IE, DK, ES, FI, PT, IT, EE, NL, FR, LU, MT, UK, SE**) with the exception of a few Member States where this is not allowed by domestic laws (**LV, EL, UK, BG**) or it is subject to other or stringent conditions (**RO, SK, NL, LT, HR, CZ, DE, SI**), showing the lack of a common view on the principle of voluntary disclosure without an MLA among Member States.

Mutual Legal Assistance (MLA) with third countries

Legal framework

• As regards cooperation with countries outside the European Union, Mutual Legal Assistance (MLA) is in this area mainly based on international law, notably the Council of Europe Budapest Convention on Cybercrime (indicated by **AT, RO, HU, BE, HR, CY, SK, NL, LV, CZ, DE, DK, ES, FI, PT, SI, IT, EE, FR, LT, LU, MT, BG**). Besides that, there are agreements concluded by the EU (notably, the Agreement on MLA between the EU and the U.S.) and several bilateral agreements, which most Member States have concluded with the US, followed by Canada and China.

Challenges and grounds for refusal

• When it comes to cooperation with the U.S. in particular, challenges identified concern the use of MLA procedures for access to information where under U.S. law no MLA request is required, such as for subscriber or traffic data. MLA requests for such information significantly increase the overall volume of requests and contribute to slowing down the system. The use of MLA for such requests can be attributed to various reasons, including (1) where the issuing of a direct request is not permitted under the law of the issuing country; (2) where enforceability of the request is desired; and (3) a lack of awareness of the issuing authority about alternative channels.

• The admissibility of MLA requests is subject to the receiving countries' legal system, which may result in a refusal of the MLA request (most Member States indicated as ground for refusal the difficulty to establish probable cause (**AT, RO, SE, BE, NL, EL, DK, FI, FR**), followed by the lack of dual criminality (**AT, HU, BE, EL, CZ, ES, PT, MT**), data not available due to deletion (**AT, SE, CY, EL, FR, BG**), data located in another country (**SI**)).

Types of data

• MLA is often used to obtain access to content data (**AT, RO, HU, SE, BE, HR, CY, SK, IE, NL, EL, LV, CZ, DE, ES, FI, PT, SI, FR, IT, DK, LT, LU, MT, BG**), but it is also used to obtain other types of information, including subscriber (**AT, RO, HU, SE, BE, HR, CY, SK, NL, EL, LV, CZ, DE, ES, FI, SI, IT, FR, LT, LU, MT, BG**) and traffic data (**AT, RO, HU, SE, BE, HR, SK, IE, NL, LV, CZ, DE, ES, FI, PT, SI, IT, DK, FR, LT, LU, MT, BG**). "Top" third countries to which most Member States send the requests are the US and Canada.

Current practices regarding procedures, means of transmission, statistics, deadline

• The systematic use of MLA for all types of access requests for electronic evidence is increasingly viewed as problematic as the requests take too long to be processed (a minimum of 1 month in **FI** to a maximum of 18 months in **SE**), there are no fixed deadlines for responding (**AT, BE, HR, CY, IE, LV, DE, ES, SI, UK, FR, MT, BG** except **PT**), and the mechanism is complex and diverges from country to country. In most of the countries the formal procedure for issuing an MLA is initiated by prosecutor (**HR, SK, IE, NL, EL, LV, CZ, DE, DK, PT, SI, FR, LT, LU, MT, AT, RO HU, SE, BG**), followed

by judge (**AT, HR, SK, NL, ES, UK, FR**), law enforcement (**CY, LV, DK, FI, MT**), diplomatic channel (**HR, NL, IT**) or central authorities (**HR, CY, IE**).

• Although MLA requests are made following formal channels, it is difficult to keep track of both requests and responses to third countries with the effect that most Member States do not have available statistics for e-evidence (**AT, RO, HU, SE, BE, HR, SK, LV, DE, ES, FI, PT, SI, IT, FR, LT**).

• The means of transmission are generally in need of improvement as most of the Member States make use of letter, fax or email, with very few countries using secure channels.

Enforcement of jurisdiction in cyberspace

Alternative mechanisms to obtain cross-border e-evidence under specific circumstances

• EU Member States have taken different approaches in allowing their law enforcement and judicial authorities to use alternative mechanisms to obtain cross-border access to electronic evidence in the specific circumstances indicated below.

• Indeed, there are cases where it is **impossible to determine a service provider responsible for the processing or storage of data**. In these cases, law enforcement authorities make use of different techniques across the EU, such as, according to the replies, "police to police cooperation", "agency to agency cooperation", "international legal assistance", "obtaining of consent of the person", "search and seizure techniques". At least 10 Member States clarified that this depends on specific circumstances under their national legislation (**AT, IT, RO, ES, LT, EE, CZ, DK, UK, MT**). Only 1 country (**BE**) indicated to have legislation in place and 1 Member State (**NL**) indicated that this option was considered as part of an ongoing legislative process. At least 13 of the EU Member States (**PT, HU, SE, HR, CY, SK, EL, LV, DE, FI, SI, FR, LU**), however, indicated the impossibility for law enforcement authorities to access e-evidence under these complex circumstances.

• In some Member States, law enforcement authorities make use of investigative techniques to access e-evidence also **when the location of e-evidence is unclear or impossible to establish**. Tools used across the EU range from "remote access" and "search and seizure" to "multiple MLA requests" and "instruments of international cooperation". In particular, at least 4 Member States indicated that law enforcement or judicial authorities can directly access electronic evidence when it is unclear what the location of the information is or when it is impossible to establish the location of the information (**BE, ES, PT, FR, BG**), whereas 8 Member States indicated that this is not allowed under their national legislation (**HU, SE, HR, CY, EL, LV, FI, SI**) and at least 14 Member States clarified that this depends on specific circumstances (**AT, RO, LU, MT, EE, SK, NL, CZ, DE, DK, UK, IT, LT, HR**).

Difference between the framework for obtaining access to stored data and real-time collection of data

• In the situations described above (when it is impossible to determine a service provider responsible for the processing or storage of data and when the location of e-evidence is unclear or impossible to establish) at least 13 EU Member States differentiate between the framework to obtain access to stored data and real time collection of data as far as their domestic law specifically addresses situations of loss of location or refusal of cooperation by foreign providers and/or authorities (**AT, SE, HR, PT, SK, NL, HU, BE, CZ, ES, EE, FR, LT, BG**), whereas 7 countries (**RO, EL, LV, FI, SI, UK, IT**) indicated they do not make any difference and 4 countries (**CY, DE, LU, MT**) indicated this is not applicable according to national law.

Use of police-to- police cooperation

• The majority of Member States make use of police-to-police cooperation (**AT, RO, SE, EL, LV, PT, CZ, IT, DE, DK, ES, UK, NL, FR, LT, MT, HR, CY, SK, BG**), whereas 3 countries indicated they do generally make use of the MLA channel (**BE, HU, LU**).

Admissibility in court of e-evidence gathered through police-to police cooperation

• Evidence gathered through police to police cooperation is admissible before the court in 7 Member States (**AT, SE, EL, DK, ES, IT, FR**), however, there are several EU countries (**RO, HU, CY, SK, LV, LU, LT, CZ, DE, MT, SI, EE, HR**) in which admissibility is subject to stringent conditions or to a MLA or it is not foreseen by law and rather considered as "intelligence".