SIRIUS EU Digital Evidence Situation Report

3rd Annual Report

2021

EUROPOL

EUROJUST

EUROPEAN JUDICIAL NETWORK
Connecting Justice

3RD ANNUAL SIRIUS EU DIGITAL EVIDENCE SITUATION REPORT

The SIRIUS Project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under grant agreement No PI/2017/391-896.
This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

INDEX

Catherine De Bolle

EXECUTIVE DIRECTOR, EUROPOL

This third report on the EU digital evidence situation is timely and highly relevant in a time of rapid digitalisation. Digitalisation has an impact on virtually all criminal activities and security threats we encounter in the EU. Similarly, law enforcement and judicial authorities must increasingly rely on digital solutions in enforcement and judicial processes.

Nothing has made it clearer than the COVID-19 pandemic that there is a pressing need to embrace and integrate digitalisation into our working processes and prepare our systems. Law enforcement authorities were able to adapt quickly to an unprecedented situation relying on some of the digital solutions already in place and provided by Europol and those that were deployed in response to the reality of a global pandemic. This experience has clearly demonstrated the powerful potential of digital processes and the ability of handling digital evidence securely and verifiably.

Effective policing in the digital age largely relies on effective cooperation between law enforcement and judicial authorities at national and European level. This report is an outcome of the close partnership between Eurojust and Europol working together on issues of mutual concern. I have made it a priority for Europol to continue to develop the relationship with this key partner identifying synergies and additional areas for cooperation wherever possible. I am satisfied with the progress so far and look forward to further collaboration in the future.

At Europol, we will continue to push forward in terms of technology and expertise available to law enforcement and continue to work together with partners at EU level, in the Member States and the private sector.

Ladislav Hamran

PRESIDENT, EUROJUST

The SIRIUS project has established a solid reputation as the EU's central knowledge hub in the field of cross-border access to electronic evidence. Eurojust proudly contributes to the project, knowing that it provides a crucial set of services - including guidelines, trainings and practical tools – to all partners in the security chain dealing with electronic data acquisition in criminal investigations and prosecutions.

This third joint Report reflects the complexity that results from a constantly evolving digital landscape and fragmented legal framework. It also shows how the global COVID-19 pandemic forced the EU's judiciary to develop innovative approaches and adapt existing processes. By mapping core issues and trends, we hope to provide practitioners and policy-makers with a better understanding of the challenges and opportunities related to electronic evidence.

Clearly emerging from the report is the notion that our success in the fight against organised crime depends on the strength of our mutual partnerships. As long as we work together, I am convinced that we can strike the right balance between obtaining access to electronic evidence and upholding the fundamental rights and liberties of our citizens.

Didier Reynders

EU COMMISSIONER FOR JUSTICE

"The annual SIRIUS EU Digital Evidence Situation Report is a must-read fact finding report for policy-makers. It presents a clear picture of the challenges that practitioners still face to obtain electronic evidence. While criminals have taken advantage of the COVID-19 pandemic, the report shows that it has also made it more difficult for law enforcement and judicial authorities to obtain electronic evidence. In the light of these challenges, it is more important than ever that co-legislators agree on new rules to obtain electronic evidence. Crime committed with digital means needs to be prosecuted as efficiently as offline crime."

EXECUTIVE SUMMARY

The COVID-19 pandemic led to an acceleration in the digitalization of everyday life for a large portion of the population in the European Union (EU), while criminals quickly and dynamically adapted their modus operandi in several areas. In this context, **EU law enforcement and judicial authorities, as well as Online Service Providers (OSPs) faced challenges in the field of electronic evidence** and had to adapt existing processes. While the volume of requests continued to increase, and policy making in relation to electronic evidence advanced slowly in 2020, the challenges in the field remained the same. This report looks back at 2020, presenting data that include surveys conducted with EU law enforcement and judicial authorities, as well as interviews with representatives from ten OSPs.

From a law enforcement perspective, the pandemic led to longer delays to receive responses from OSPs, while a quarter of agencies had their capacity to submit requests negatively impacted. Although satisfaction with existing procedures to obtain evidence decreased, a majority of EU law enforcement officers remained satisfied and continued to rely on the existing electronic evidence process. For the first time, the use of online portals scored higher than e-mail as a preferred submission channel, while the preference for Single Point of Contact (SPoC) for centralization of requests continued to increase. Moreover, **this year's report confirms that the main challenges for law enforcement continue to be the long delays for Mutual Legal Assistance (MLA) process and the lack of standardisation in OSPs policies**. It is also worth noting that **the SIRIUS platform appears for the first time as the first-ranked source of information** to be consulted when EU officers need assistance in relation to direct requests for electronic evidence.

From the perspective of EU judicial authorities, social distancing and restrictive measures introduced due to the global health pandemic, caused reduced capacity which resulted into a more lengthy procedures. Yet, some of the developed solutions, such as acceptance of electronic documents, electronic communication and videoconference court hearings, were embraced by the judicial society. Besides the already challenging context in 2020, **the length of the MLA procedures formally engaging with non-EU OSPs was reported as the main issue (73.5% of respondents), whereas regarding direct engagement with the foreign OSPs, a majority pinpointed the short/ non-existent data retention periods (57.1% of the respondents)**. The recent preliminary rulings of the Court of Justice of the European Union (CJEU) concerning retention of data and lack of a common and uniform legal framework as a result thereof, bring multiple practical challenges and an additional layer of complexity to cross-border investigations involving electronic evidence.

Finally, **from the perspective of the majority of OSPs interviewed**, the restrictions associated to the pandemic led to temporary backlogs in processing requests for

electronic evidence and required changes and flexibility in existing processes, while having large impact over staff. **The volume of data requests submitted by EU authorities increased +27.1% from 2019 to 2020, with Germany and France accounting for 65.5% of them. The overall success rate of EU requests increased from 62.6% to 66% in 2020**. In this context, the collaboration with SPoCs for the centralization of requests in several EU Member States continued to be highly beneficial, leading to streamlined communication and faster response time for requests. The main reasons for refusal or delay in processing EU direct requests for voluntary cooperation were: legal basis absent or incorrect, wrong legal entity addressed and procedural mistakes.

The last chapter of the report brings **recommendations** to improve effectiveness of cross-border access to electronic evidence:

For EU Law Enforcement Agencies:

- Use Standardised Model Forms for data preservation and disclosure requests under voluntary cooperation
- In law enforcement agencies where not yet established, create Single Points of Contact for electronic evidence requests to OSPs under voluntary cooperation

For EU Judicial Authorities:

- Stimulate national capacity building initiatives on the available instruments and processes to request and obtain electronic data from other jurisdiction
- Enhance the interconnection, know-how and expertise exchange among EU judicial practitioners in the field of electronic evidence

For Online Service Providers:

- Disseminate updates about policies and changes in processes to EU authorities also through SIRIUS
- For small and medium OSPs that do not have yet established processes for engagement with law enforcement in the context of criminal investigations: join the SIRIUS Programme for OSPs
- For OSPs that already have established processes for engagement with law enforcement in the context of criminal investigations: take into account the perspectives of law enforcement and judicial authorities presented in this report when updating policies

KEY FINDINGS

The SIRIUS platform on the EPE appears as the **highest ranked source of information** for Law Enforcement Agencies seeking assistance to prepare direct requests

Almost half of EU Law Enforcement Agencies reported an **increased need in electronic evidence** after March 2020, while experiencing **longer delays** in receiving responses from OSPs

The **main issue for judicial authorities**, identified by 57.1% of respondents, was **short data retention periods** or the **absence of data retention policies**

There was a significant increase in data disclosure request in 2020, including an **increase of 112% in emergency disclosure requests** compared to 2019

Shift in the submission channel preference: the use of **online portals** dedicated to Law Enforcement is the **preferred method to submit requests**

Companies are unanimous: **the establishment of Single Points of Contact** for the centralisation of data requests is **highly beneficial** to the process

TESTIMONIALS

- *"We received prompt answers and valuable information through Direct Requests to Uber, Netflix, PlayStation Network and Facebook/Instagram that were crucial to our investigations. The SIRIUS platform, Law Enforcement forum, OSP finder, and SIRIUS guidelines were very useful in that processes"*

- *"I would truly like to say "Thank you" [to the SIRIUS project] for trying to do as much as you can. I do truly believe that sometime in future we would be able to centralize our requests for electronic evidence on an EU Law Enforcement platform"*

ABOUT THE SIRIUS PROJECT

The SIRIUS project is a central reference in the European Union (EU) for knowledge sharing on cross-border access to electronic evidence. Today, the project is co-implemented by Europol and Eurojust in close partnership with the European Judicial Network (EJN), and it receives EU funding from the Service for Foreign Policy Instrument of the European Commission. SIRIUS offers a variety of services, such as guidelines, trainings and tools, to help with accessing data held by Online Service Providers in the context of criminal investigations. These services are available to law enforcement and judicial authorities via a restricted online platform and a mobile application.

Back in 2017, when the project was first launched[1], the digital environment already offered various layers of complexity to security practitioners: it had become clear that digital data were paramount to solving cases in a wide array of crime areas. Criminals, on their part, were already tech savvy and highly flexible, emerging as early adopters of new business models and disruptive technologies.

At the time of publication, the project has developed a community of over 5,500 users from law enforcement and judicial authorities from 46 countries, representing all EU Member States and a growing number of third countries. It has maintained a dialogue with more than 55 OSPs, developed over 50 reference documents for law enforcement and judicial authorities, created a contact directory of over 800 companies and trained more than 1,500 officers on various aspects related to cross-border access to electronic evidence.

In the last four years of existence, SIRIUS has grown in close synchrony with the evolution of the digital space and of the debate at European and global level on Internet governance and cross-border access to electronic evidence and finally became the EU central reference for knowledge-sharing in electronic evidence it is today. Looking ahead, the project will further leverage its established visibility and position to support an even larger number of law enforcement and judicial authorities in developing the knowledge related to the retrieval of electronic data.

CONTEXT

In 2020, the COVID-19 pandemic and the social distancing measures put in place to contain the spread of the virus had deep worldwide repercussions. The crisis had a profound impact on society and led to an acceleration in the digitalization of everyday life for a large portion of the population in the EU. The unprecedented social changes triggered by the pandemic created new opportunities for organised crime groups to gain illicit profit. Criminals quickly and dynamically adapted, intensifying activity in several areas, including cybercrime, distribution on counterfeit and substandard goods, frauds and scams, as well as organised property crime. Moreover, the month of March 2020 saw a concerning spike in the number of child sexual abuse cases, as

children experienced confinement at home and increased their time spent online[2].

The legal process in obtaining electronic evidence had also been affected by both the restrictions put in place during the pandemic and the fact of working from home. For example, this led to prioritization of such requests on the basis of urgency/seriousness of the crime. Adhering to the circumstances, the EU Member States were adopting new solutions, such as electronic transmission of requests (i.e. by email) as the most effective means in the current situation[3].

Though the Commission proposed on 17 April 2018 the e-evidence legislative package[4] to improve cross-border access to e-evidence, it has not been adopted. Thus, the applicable regulations in the area of electronic evidence remained unchanged in 2020. Yet, some important steps for moving forward in the legislative procedure were noticeable. The European Parliament adopted its position on the e-evidence legislative package[5] in December 2020[6], containing a number of amendments in relation to the proposal of the European Commission from April 2018[7]. As the General Approach of the Council of the European Union was already completed in March 2019[8], the adoption of the position by the European Parliament opened a path to begin with inter-institutional negotiations. Depending on the outcome, it could radically change the possibility to obtain electronic evidence in a swift and reliable manner to allow for more effective criminal investigations.

In addition, the year 2020 presented landmark rulings of the Court of Justice of the European Union (CJEU) of October 2020 on data retention[9], which increased calls for a coherent response at EU level[10]. However, further proceedings before the Court were initiated and can be expected to influence discussions in the coming months.

Furthermore, other initiatives such as the negotiation of bilateral EU-US agreements on cross-border access to electronic evidence advanced slowly in 2020. Although the negotiations on a Second Additional Protocol to the Council of Europe 'Budapest' Convention on Cybercrime continued in 2020, the text was only adopted on 17 November 2021 and should be open for signatures in May 2022[11].

Therefore, in 2020, law enforcement and judicial authorities continued to rely on voluntary cooperation between authorities and OSPs, or on international judicial cooperation mechanisms such as Mutual Legal Assistance (MLA) and the European Investigation Order (EIO) to request the disclosure of user data in the context of criminal investigations.

On the one hand, the experience of EU authorities shows that voluntary cooperation with a foreign-based private entity in possession or control of the data is not only a key tool for success, but also the fastest channel to obtain non-content data. Despite being efficient instruments, direct requests under voluntary cooperation are entirely dependent on the willingness of OSPs to cooperate. Lack of enforceability leads

to potential struggles for the competent authorities. On the other hand, the existing formal judicial cooperation mechanisms for retrieval of cross border electronic evidence is often regarded as strikingly long. At the same time, judicial cooperation is often the most suitable instrument when content data is necessary for investigations, when information obtained by voluntary disclosure would not be deemed admissible as evidence in the requesting State's court, or ultimately if the process of voluntary cooperation is not pursuable.

In this context, this report analyses the situation of the use of electronic evidence in criminal investigations in the EU in 2020 and also touches upon the impact of pandemic to the work of judicial authorities, law enforcement and OSPs in this area.

SCOPE

The third SIRIUS EU Digital Evidence Situation Report has the same scope as the first two editions. It aims to present data, rather than offer conclusions, on the use of electronic evidence by EU law enforcement and judicial authorities in criminal cases, this time with a focus on 2020. To achieve this goal, this report includes data collected from competent authorities in all EU Member States, and from OSPs with important relevance to investigations in the EU, taking into account the impacts of the COVID-19 pandemic in this field.

As for the previous editions, this report can contribute to the identification of trends and core issues with a view to improve the effectiveness of criminal investigations and prosecutions.

METHODOLOGY

This report has been developed with information collected from publicly available sources, as well as from exclusive interviews and surveys conducted with competent authorities and OSPs, as described below.

Information from companies' publicly available transparency reports regarding governmental requests for data disclosure

The transparency reports analysed for the purpose of this report were: Airbnb, Automattic, Cloudflare, Dropbox, Facebook, Google, LinkedIn, Microsoft, Reddit, Snap, TikTok, Twitter and Verizon Media. For the analysis and graphs presented in the report, only OSPs that reported more than 100 requests in 2020 were included[12].

Data referring to the volume of disclosure requests submitted by EU authorities to OSPs in 2018 and 2019 differ from the numbers published in previous editions of this report. The reason for this is two-fold. First, as of 1 October 2021, when the draft of this report has been finalised, Apple had not yet published data for their transparency report referring to the second semester of 2020. Therefore, data from Apple has been excluded from the analysis to ensure the data from different years is comparable.

Second, information relating to the United Kingdom (UK) has been subtracted from the years 2018 and 2019 to ensure the figures are comparable to those from 2020, since the UK is not an EU Member State anymore.

Online surveys with European Union law enforcement

Europol conducted a survey amongst law enforcement agencies and collected 208 responses from representatives from all EU Member States, during April, May and June 2021. The survey was conducted online through password-protected form and the responses were anonymous.

Online surveys with European Union judicial authorities

In order to gather insights on cross-border requests and access to electronic data in criminal investigations in 2020, the legal frameworks surrounding the field as well as COVID-19 impact on digital data acquisition processes, Eurojust engaged with the EU's judiciary community. Accordingly, in April 2021, Eurojust submitted a survey tailored for EU judicial authorities, reaching out to the judiciary community on the SIRIUS Platform, members of the European Judicial Cybercrime Network and the contact points of the European Judicial Network. In total, 49 in-depth responses were received from representatives of 24 EU Member States[13]. The compilation of this information formed the basis of what is now presented in this report.

Furthermore, this report also presents the views expressed by judicial authorities during EJN meetings (53rd Plenary Meeting of the European Judicial Network under the Finnish Presidency 20-22 November 2019 and 56th Plenary Meeting of the European Judicial Network under the Portuguese Presidency 29 June 2021) and the needs of practitioners to improve the current legal framework for gathering electronic evidence.

Interviews with Online Service Providers

Europol and Eurojust engaged via video call or e-mail with representatives from Airbnb, Facebook, Google, Microsoft, Snap, TikTok, Twitter, Uber, Verizon Media and WhatsApp between April and July 2020 for the purpose of gathering data for this report. The findings presented in this report should not be taken as the official formal position of any of the aforementioned private entities.

The main topics discussed with these companies were:

- Main reasons for refusal or delay in processing of requests from EU authorities in criminal investigations;
- The impact of the COVID-19 pandemic to the electronic evidence process;
- Future challenges in the area of cross-border data disclosure requests.

THE PERSPECTIVE OF LAW ENFORCEMENT

A. Success cases

Behind each number in any statistical analysis on electronic evidence, which will follow in this chapter, there is a real investigation. The extracts reported below are the direct feedbacks provided anonymously by EU law enforcement officers in relation to some of their recent success cases. These stories cover several crime areas and once again demonstrate the importance of digital data for law enforcement to save lives, locate victims and criminals, identify suspects and prevent cybercrime. Officers were requested not to share sensitive details about their cases via this survey[14].

Terrorism

- *"In 2020, electronic evidence was essential for three investigations on terrorism. All the offenders were users of social media or messaging apps (e.g. Snapchat, Twitter, Instagram, Facebook and Telegram). It was possible to obtain basic subscriber Information from several of them, but really hard to obtain content. We are still trying to obtain content of accounts via legal process"*

- *"In the context of investigations on terrorism, evidence obtained upon a decree of the Public Prosecutor through the Facebook Law Enforcement Portal has been important"*

Child sexual abuse

- *"An Emergency Disclosure Request to Instagram allowed me identify my suspect's IP address and devices and I was able to track down a pedophile. The suspect was convicted and now serves 8 years in prison"*

- *"With the information received from OSPs, we were able to tie a pedophile to specific crimes and locate his physical address"*

- *"In a large case involving multiple children abused online, we managed to identify some of the victims thanks to electronic evidence provided by Snapchat and Instagram. We used IP addresses, names and phone numbers and connected those to our national databases"*

- *"I was able to access data that was important for investigating sexual abuse of children with information from email provider Yahoo"*

- *"We were able to investigate many reports from the National Center for Missing & Exploited Children (NCMEC) due to the possibility to request the disclosure of data via the Google Law Enforcement Request System"*

- *"Though Snapchat did not answer our initial request, they observed our reported account and eventually reported it to NCMEC. We received information through NCMEC and were able to identify the original offender"*

- *"It took one request via Mutual Legal Assistance process to Snapchat and two direct requests to Google and WhatsApp to establish the identity of a child predator that had raped a 9-year-old child. No physical evidence or even a security camera footage showing the offender with the child helped to identify him, but the electronic evidence allowed us to identify and capture him. It took over a year for the MLA process to be completed and the data preservation period of the most important IP-address was just about to expire (only a few days left)"*

- *"Thanks to the SIRIUS platform, I became aware that it is possible to use NCMEC help*

in obtaining data from companies regarding CSE cases"

Murder

- *"A case of a serial killer two years ago. A profile at Badoo was the only known information available at the beginning of the investigation. We submitted an EDR to the company and their response included an email address linked to the suspect. We found a Facebook account linked to this e-mail, so we sent an EDR to Facebook. Their response gave as very important results (including IP addresses) that helped us to identify the suspect"*

Missing persons

- *"Thanks to requests for electronic evidence to OSPs we found missing minors and the information the OSP's provided helped to solve cases of National importance"*

Cybercrime

- *"During the past year, we had to focus our investigations on 'phishing' practices aiming to steal credit card information and national digital signature credentials. With this kind of investigation, the sites created by criminals are up usually for a very short time and then they are taken down. As a police entity, it is difficult to have the legal requirements ready to follow the act. However, during the past year we have contacted a number of website hosting companies, which have assisted us to obtain access to the deployed phishing kits"*

Fraud

- *"We had a case of fraud case involving the use of the Revolut app. Victims were being tricked into sending money to an account for different services regarding hiring in EU countries. Revolut quickly responded to our request with information highly relevant to our investigation, giving us the opportunity to find out the criminals (two in this case) and partially recovering the money"*

- *"At the beginning of this year, a successful operation has been executed with the operational support of the EUROPOL. Using the SIRIUS requests templates we submitted a preservation request with the aim to preserve and secure the affected Google accounts, which was successfully executed by Google"*

Several crime areas

- *"Electronic evidence is essential in all our investigations"*

- *"Child Sexual Exploitation Cases, ransomware attacks, e-frauds, suicide threats. SIRIUS is a very useful platform where we can find important information for our department and for our Cyber Crime Division investigations"*

- *"All our investigations into child pornography, illegal dissemination of sexually explicit material, and the misuse of credit cards have based their accusatory thesis on electronic data obtained from foreign-based service providers"*

- *"Many investigations on threats, extortion, impersonation, and drugs have benefited from electronic evidence found on mobile phones in use by suspects and related data on 'Cloud' accounts which have been requested, many times, from foreign service providers"*

Crime area not informed

- *"We asked an OSP to provide Basic Subscriber Information and Traffic Data via Direct request, after we consulted the SIRIUS guidelines for that specific OSP. The same company had previously not complied with our requests, but because we follow the instructions on the SIRIUS*

guidelines and were more specific on the datasets that were required, and specified why the information was pertinent, the company disclosed the information and we could move forward in an investigation which otherwise would have been stuck. The use of an MLA was not an option in this particular situation, so that was a success"

- *"We received prompt answers and valuable information through Direct Requests to Uber, Netflix, PlayStation Network and Facebook/Instagram that were crucial to our investigations. The SIRIUS platform, Law Enforcement forum, OSP finder, and SIRIUS guidelines were very useful in that processes"*

- *"Our department received useful data from Facebook, Instagram and Google upon emergency disclosure requests. In all cases templates and guidelines from SIRIUS, were used. We also received information after direct requests on a voluntary basis from Registrars (templates and guidelines from SIRIUS were used)"*

- *"Information from Amazon allowed us to solve a case and identify a suspect but we had to request the disclosure of data through police-to-police cooperation with the United States"*

- *"A Canadian OSP refused my preservation request because it had been issued by authorities outside of Canada. My national Cybercrime Unit forwarded the request via Interpol. After that, the Canadian Police made my request to the company, which was successfully accepted"*

Feedback regarding SIRIUS

- *"I do not know if it is appropriate to use this space for my gratitude towards SIRIUS platform, but I would truly like to say "Thank you" for trying to do as much as you can. I do truly believe that sometime in future we would be able to centralize our requests for electronic evidence on an EU Law Enforcement platform"*

B. The impact of the COVID-19 pandemic on law enforcement's acquisition of electronic evidence

In 2020, the implementation of social distancing measures and lockdowns in EU countries affected the work of law enforcement in the field of electronic evidence. At the same time, criminal activity has shown high adaptability to the evolving reality of Member States. For instance, criminals have taken advantage of the situation to increase sales of counterfeit and substandard high in demand products, as well as adapt cybercrime activity including pandemic-themed campaigns of phishing, ransomware, malware and business email compromise attacks. In this context, health-related organisations have been particularly targeted[15]. Moreover, with children spending more time online, child sexual abuse has remained a critical concern for law enforcement, with statistics indicating that the amount of related material available online has rapidly increased in the EU[16].

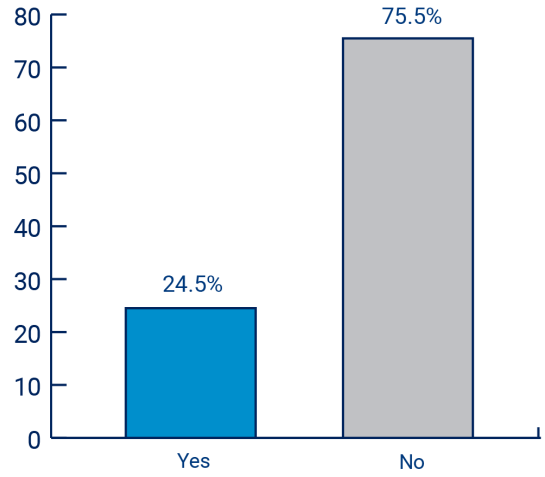
Almost half of officers surveyed stated that the need for electronic evidence increased and that they started experiencing longer delays to obtain responses from OSPs. A surge in the digitalization of everyday life to a large portion of the population could explain the increased need for electronic evidence. Moreover, the pandemic and the challenges

related to the social distancing measures also affected the workforce within OSPs, which also impacts the delays for responses to law enforcement. These impacts to OSPs will be further analysed in the chapter *Perspective of Online Service Providers*.

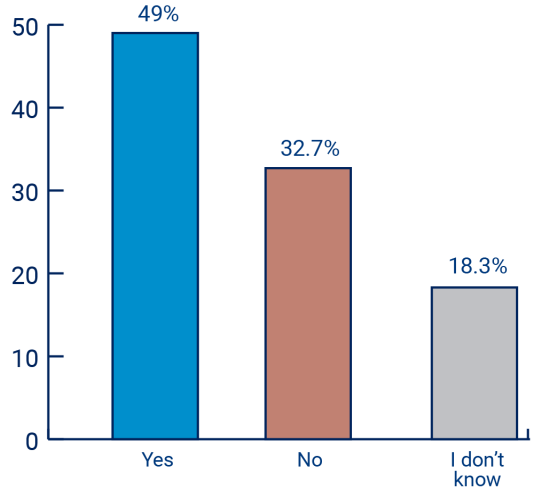
Almost 25% of officers reported that the capacity of their department to submit data disclosure requests to OSPs was negatively impacted after March 2020. This is related to the fact that part of the workforce started to work from home and that existing processes, which required physical presence at the place of employment, had to be reviewed. Some officers had their access to computers, office material and printers temporarily restricted and in some cases it was not possible to collect required manual signatures from authorised officials and scan signed requests.

The results presented in the graphs below confirm the impact of the pandemic in the electronic evidence process from a law enforcement perspective, leading to delays in a number of criminal investigations and potentially nudging changes in internal processes of police departments, with a view of rendering some procedures less dependent on the exchange of physical documents. These results include responses from officers in all EU Member States.

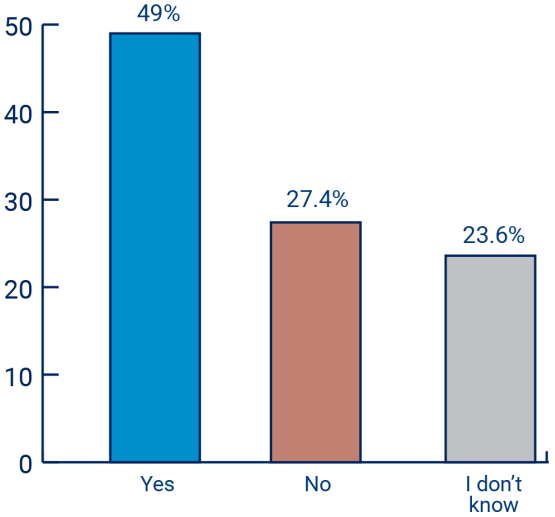
Has the capacity of your department to submit data requests to Online Service Providers been negatively impacted after March 2020 because of constraints related to social distancing measures?



Has your department experienced an increase in the need for e-evidence after March 2020?

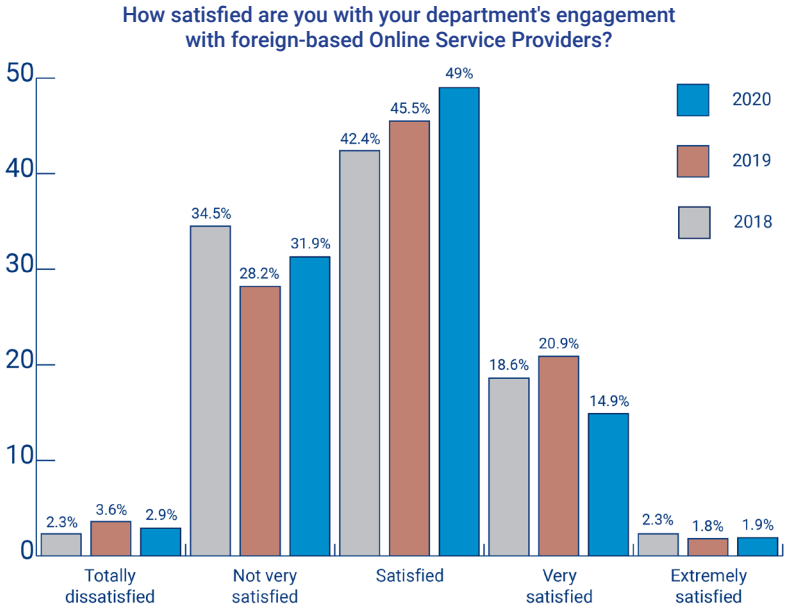


Did your department experience longer delays to receive responses from companies for data disclosure requests after March 2020?

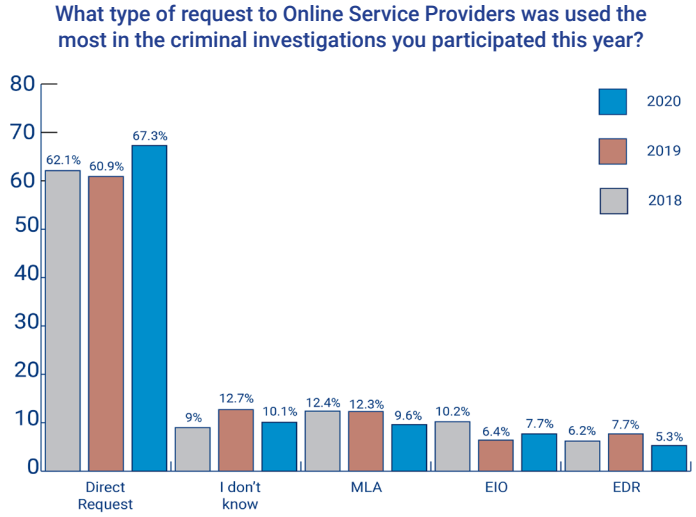


C. Engagement of EU law enforcement with foreign-based Online Service Providers

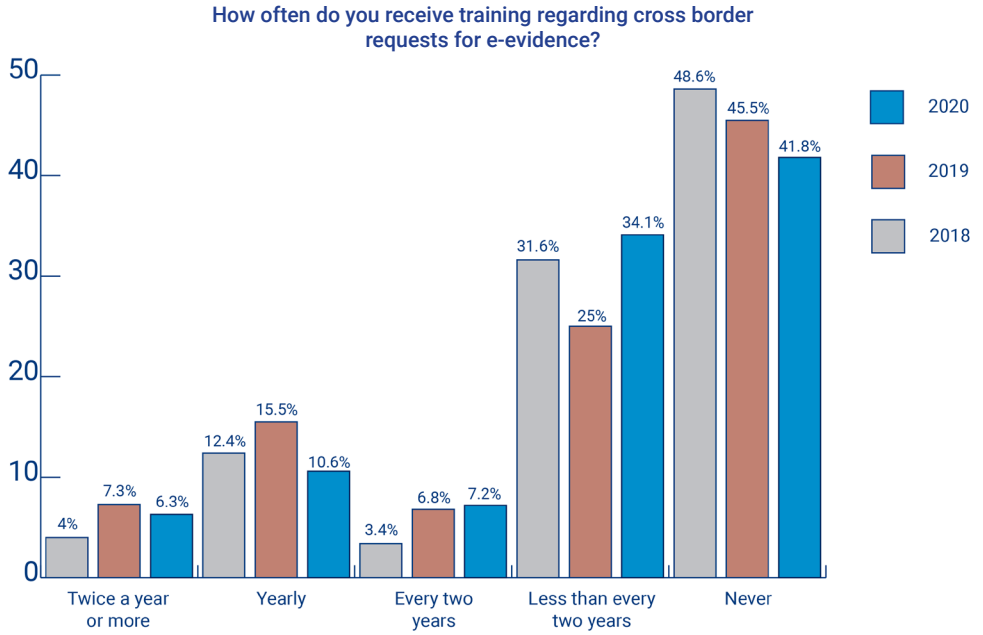
The satisfaction rate of officers with the process to request data from OSPs in criminal investigations has been recorded since 2018. This year, 65.9% of officers reported being satisfied, very satisfied or extremely satisfied, which represents a decrease of -2.3% in relation to the previous year. Nevertheless, in view of the existing challenges in the electronic evidence process and the new challenges imposed by the COVID-19 pandemic, the satisfaction rate remains remarkably high.



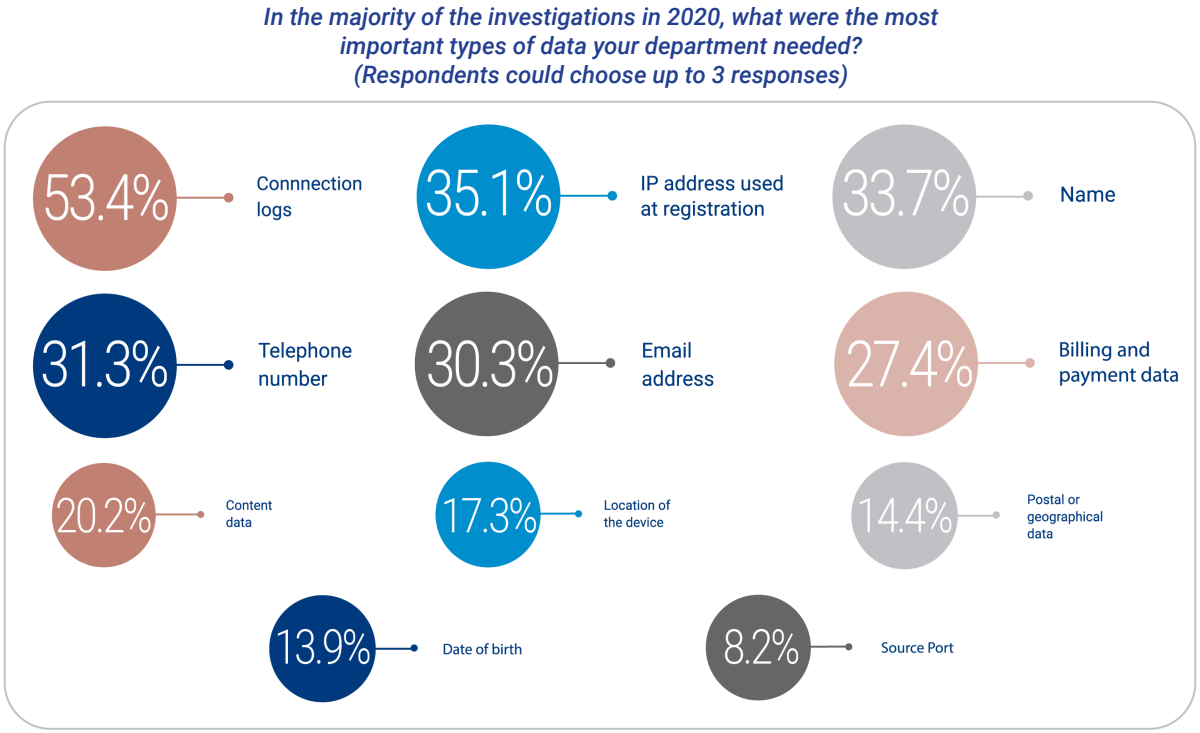
Direct requests from law enforcement to foreign-based OSPs for disclosure of data under voluntary cooperation remained the most common type of request in investigations with the participation of law enforcement officers. There was an increase of 6.4% in responses that indicated direct requests as the main type of request. This result is followed by MLA, EIO and Emergency Disclosure Request (EDR), in this order, all scoring less than 10% of responses in 2020.



Data shows a positive trend of the consistent decrease in the number of officers that report never receiving training regarding cross-border requests for electronic evidence. From 2018 to 2020, that number fell -6.8%, but it remains at a high value of over 40% of responses.

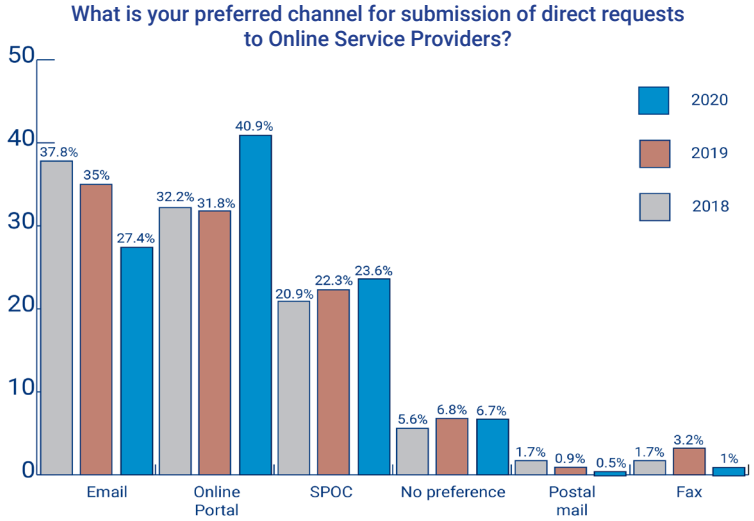


In 2020, the most relevant type of data for criminal investigations was “Connection Logs”, which indicate date, time and IP address of connections. “Connection logs” has been indicated by more than half of all the respondents. The second most important type of data was “IP address used at the registration” of a user account on the concerned platform. That result is followed by name, telephone number and e-mail address linked to the targeted account.

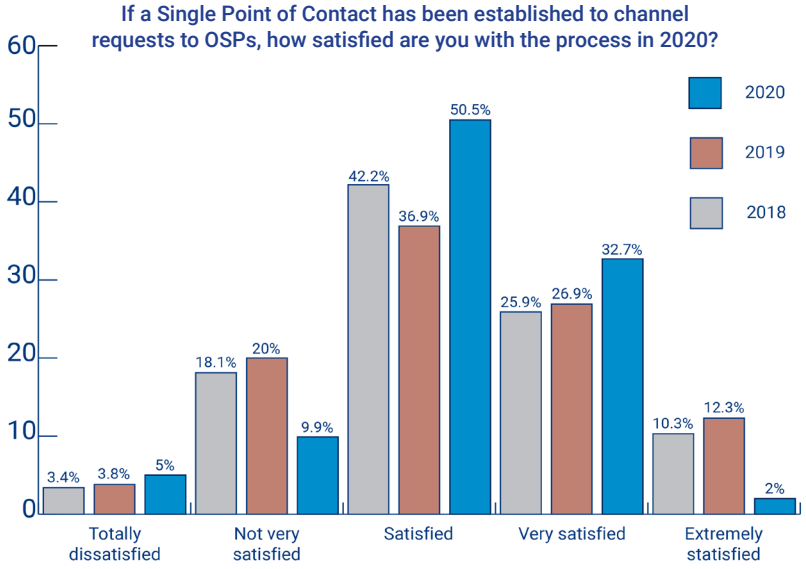


D. Submission of cross-border requests

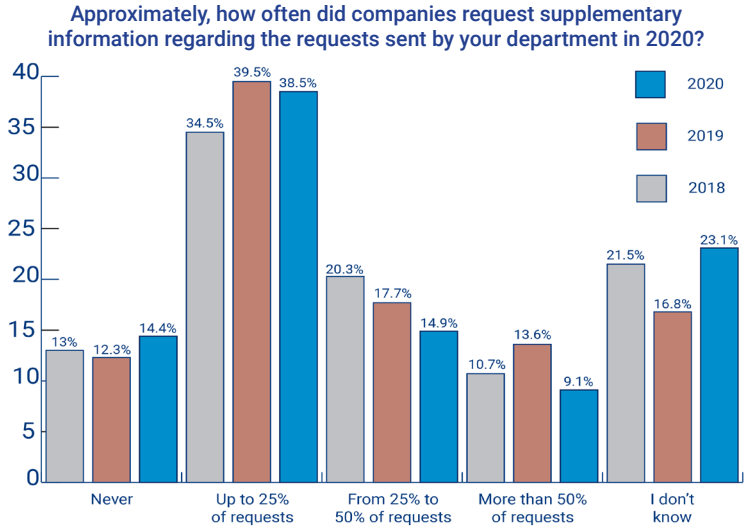
There was a shift in the preference for submission channel in 2020. For the first time, the use of online portals dedicated to law enforcement became the preferred method, scoring higher than e-mail. Online portals for submission of law enforcement requests have been established individually by several OSPs[17]. They are often described as more secure and more informative than e-mail, since it is generally possible to check the status of requests, provide supplementary information and obtain records in a secure environment. Furthermore, it is worth noting that the preference for the submission of requests via Single Points of Contact (SPoCs)[18] at agency level continues to increase.



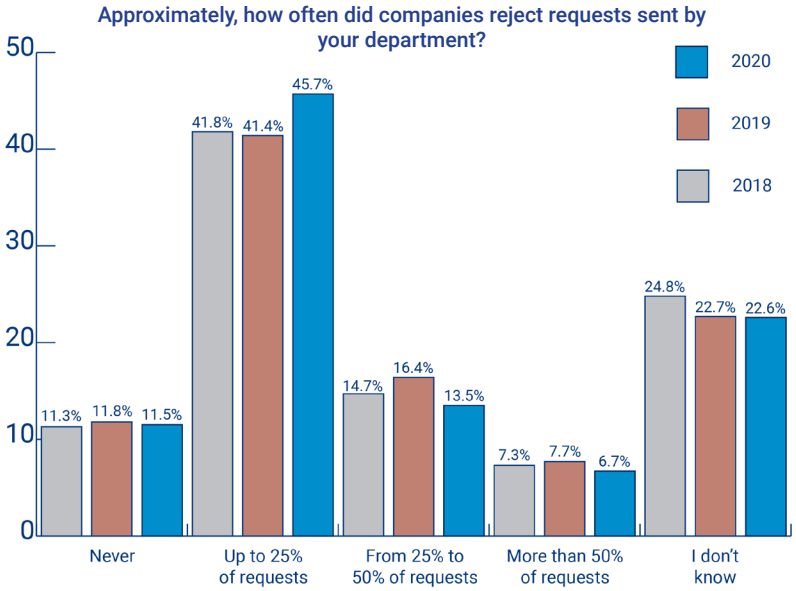
Specifically in those agencies where SPoCs have been established, the satisfaction rate with their processes also continues to increase. Over 85% of officers report being satisfied or more than satisfied with their SPoC, a considerable increase of over 9% in relation to the previous year. This result confirms the benefits of the SPoC approach, which was largely analysed in the *SIRIUS EU Digital Evidence Situation Report 2020*.



The frequency of requests from OSPs for supplementary information has remained low over the three years. In 2020, the majority of officers indicate they were never asked to provide additional information or that it happened only in less than a quarter of their requests.

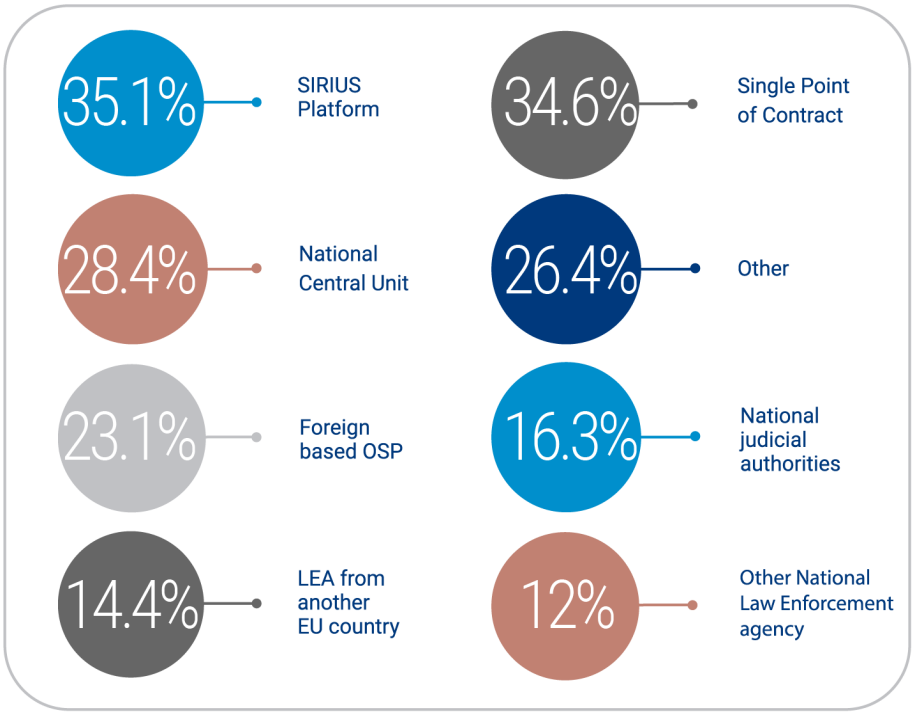


In 2020, there was also a slight decrease in the number of officers indicating that many of their requests were rejected by OSPs. This represents a positive trend of increased success rate, indicating higher quality of requests and more familiarity of requesting officers and OSPs with applicable regulations and requirements.



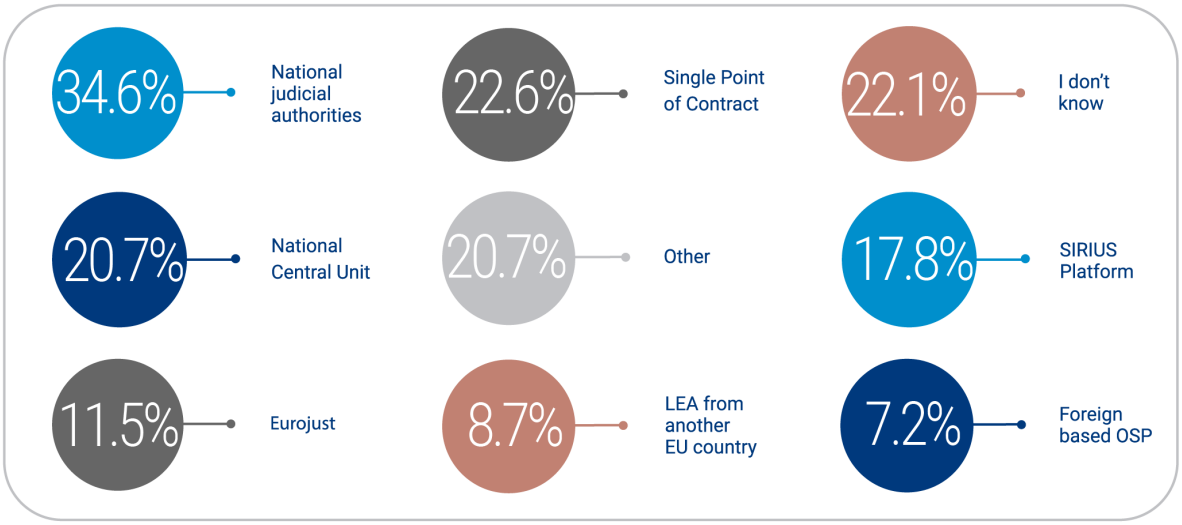
The restricted SIRIUS Platform appears for the first time as the first-ranked source of information to be consulted when officers need assistance in relation to direct requests for electronic evidence. SIRIUS offers a wide range of knowledge products, including detailed information regarding OSPs, contact details of hundreds of OSPs, templates, requirements for different types of requests and legal standards that must be observed. In the survey, the SIRIUS platform is followed by SPoCs and law enforcement central unit, which are also consulted in relation to cross border voluntary cooperation.

In case your department needed assistance to prepare direct requests to companies, who did you consult? (Respondents could choose up to 3 responses)



In relation to MLA, the National Judicial Authorities are consulted by over 34% of officers, while over 22% indicate they request assistance to SPoCs. In fact, the results of the survey in relation to the assistance needed to both direct requests and MLA confirm once again the relevance of the SPoC units in the electronic evidence process.

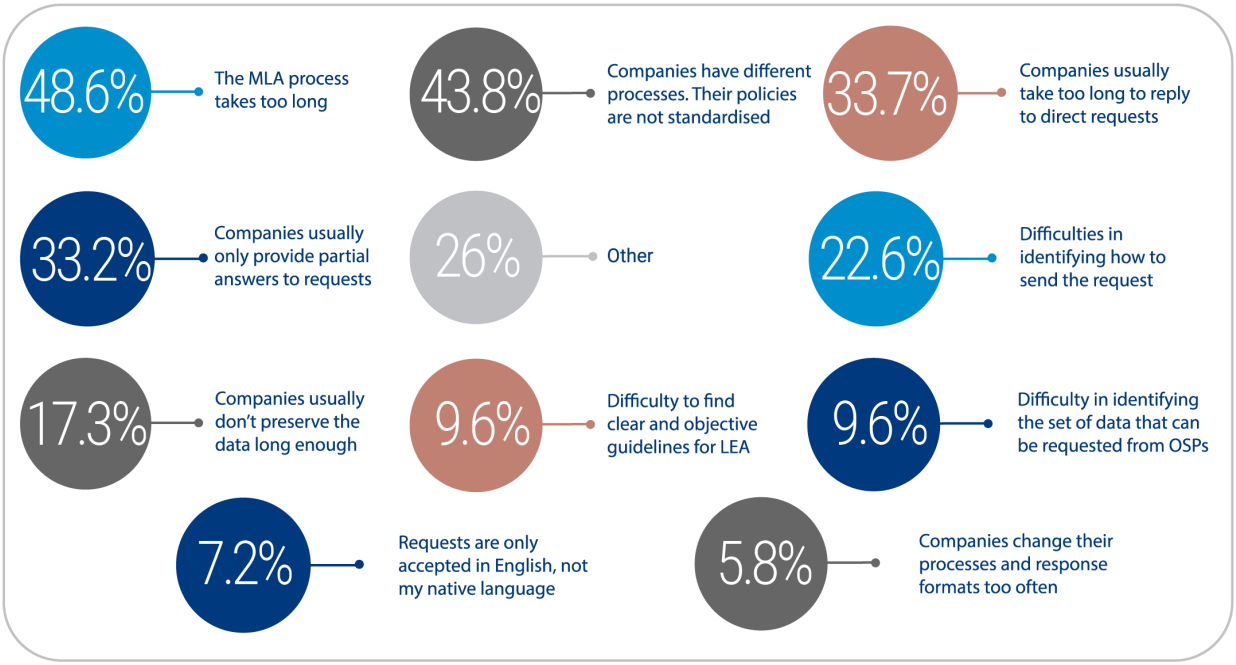
In case your department needed assistance to prepare Mutual Legal Assistance requests, who did you consult? (Respondents could choose up to 3 responses)



E. Issues encountered by EU law enforcement

The three main issues encountered by EU law enforcement in the process to obtain access to electronic evidence remained the same as in the previous report and all gained additional relevance by scoring even higher percentages when comparing results for 2019 and 2020. The first main issue is the long delay in MLA process, chosen by almost half of the respondents. In second place, appears the lack of standardization in OSPs policies, which mainly relates to direct requests for data disclosure via voluntary cooperation. Finally, the third issue is the delay for OSPs to reply to direct request, which is related in part to the challenges posed by the COVID-19 pandemic, as explained previously in the section **B.** of this chapter. Other issues that scored more than 5% in the survey appear in the graphic below.

What are the main issues your department encountered in requests to foreign-based Online Service Providers? (Respondents could choose up to 3 responses)

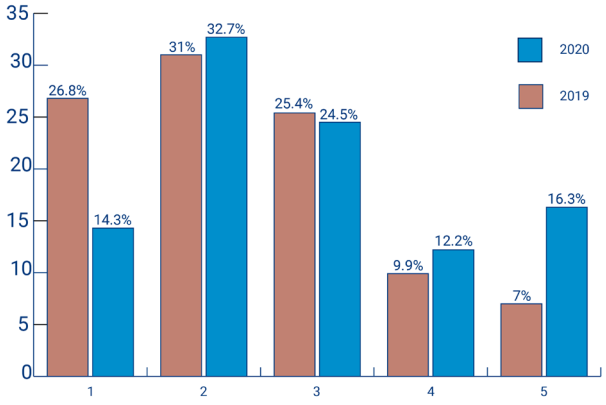


F. The relevance of Online Gaming Platforms in investigations

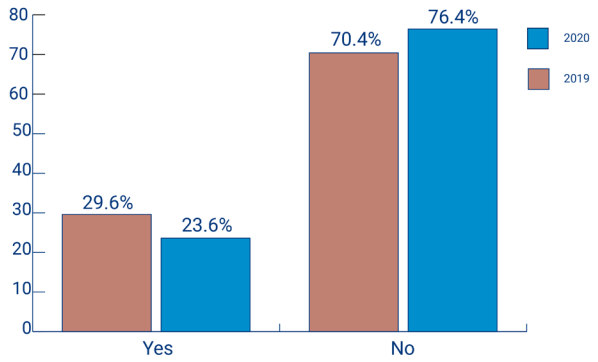
Online Gaming Platforms (OGP) continued to gain relevance in investigations in 2020. There was a considerable increase of almost 12% in the responses from officers that indicate a high relevance of 4 or above, in a scale from 1 to 5. Even though the survey indicates an increased relevance of OGP in investigations, over three quarters of officers state their department has not submitted any request to these companies, which is more than in the previous year. The low rate of submission of requests to OGP may have different reasons. For instance, it is possible there is less awareness among law enforcement in relation to how these companies operate, where their legal entities are based and the type of data they hold, when compared to OSPs in different industries. There may also be different standards applied

by OGPs, with a more restrictive approach in relation to cross-border direct requests under voluntary cooperation or lack of publicly available information regarding their policies for law enforcement requests in criminal investigations. For instance, some large gaming companies such as Sony, Roblox and Ubisoft do not have publicly available guidelines dedicated to law enforcement requests for electronic evidence, like OSPs in other industries.

What was the relevance of online gaming platforms in criminal investigations conducted by your department ? (1 – not relevant at all to 5 – very relevant)



Did your department submit any requests for data disclosure to foreign-based online gaming companies?



THE PERSPECTIVE OF JUDICIAL AUTHORITIES

The judicial cooperation instruments (the MLA procedure and the EIO) as well as bilateral voluntary cooperation requests to foreign-based private entities currently are the most essential mechanisms for obtaining electronic evidence. However, when speed is essential to avoid losing evidence, judiciary needs to look for alternative solutions in order to keep up with the constantly evolving digital landscape and fragmented legal framework. Multiplicity of legislation in domestic and international level suggest a wide range of channels and legal instruments to retrieve digital data in criminal investigation, which might bring either an opportunity or a challenge to authorities.

In addition to those, in 2020 the global health pandemic of COVID-19 had a significant impact on the EU judiciary[19]. This impact is both negative and positive, as potentially some of the developed solutions (e.g. acceptance of electronic documents, electronic communication instead of paper/post, videoconference court hearings[20]) will potentially remain preferable as a precaution for the recurrence of similar situation and/or because it proved its relevance to the process.

A. Success cases

An increasing number of criminal investigations and prosecutions are dependent on the effectiveness of the gathering of electronic information as relevant pieces of information are often available in electronic format. In some cases, they represent the most important piece of evidence to enable a criminal investigation to move forward and/or to attribute criminal activity to the perpetrators. Even more, in several circumstances, electronic information is the only resource available in a case. The needs and solutions to obtain this “piece of a puzzle”, might not be matching at first sight.

The multiplicity of potentially applicable rules at national and international level offers a wide range of channels and legal instruments to resort to for retrieval of electronic data. On the other hand, it introduces a high legal uncertainty not only for the judiciary or law enforcement authorities, but also EU authorities, member states, citizens and private entities.

Despite the present challenges and continuously changing technological and legislative landscapes, the first-hand experiences collected from the representatives of judiciary clearly show that cooperation with private businesses is vital, both at domestic and international level. The reliance on collaboration, support, direct cooperation and partnership is a key for success, combating criminals and criminal networks that quickly embrace and adopt to the technological developments. The majority of the success cases describe the cooperation and the input provided by the private sector as the only solution, vital, excellent, quick, useful, comprehensive and very good. The following examples of some first-hand experiences point towards that[21].

- *"In Child Sexual Abuse Material (CSAM) and Child Sexual Exploitation Material (CSEM) cases the cooperation of OSP is very good."*
- *"In an ongoing criminal case, Freelancer.com [showed] excellent cooperation and provided necessary information that helped to identify the perpetrator quickly and in a modifiable format. Payoneer.com, also provided in an ongoing criminal case information very quickly, and in another ongoing criminal case Paypal provided us with a very comprehensive overview of the victims and even agreed to do a video call to specify some aspects."*
- *"In general, any information request made to Facebook or Instagram are promptly answered, with all the additional data requested as well."*
- *"I do think Google and Microsoft provide the best interaction with Law enforcement agencies."*

B. The impact of COVID-19 pandemic to judicial authorities on the acquisition of electronic evidence

Social distancing measures and lockdowns had an impact[22] on the daily work of judicial authorities and on the procedures for acquisition of electronic evidence, in both positive and negative terms. This year's report reflects the effects of the COVID-19 pandemic perceived by the judicial authorities. A common positive outcome, identified by 28.6% of the respondents, is the acceptance of electronic documents, namely as a consequence of the digitalisation of work, while 42.9% indicated no positive impacts were experienced following the introduction of restrictive measures. Additional positive effects are listed in Table 1.

Table 1: Positive effects of the COVID-19 pandemic

Germany, Latvia, Italy, Netherlands, Denmark, Sweden, Belgium, Romania	Digitalization and therefore acceptance of electronic documents.
Croatia	Acceptance of documents and faster communication with email; many things went online, like EIO; simplification of procedure.
Estonia	In Estonia, there were some positive tendencies, for example we had trials, where the evidence were presented to the court electronically, because the accused person participated via video call. Now, it is also possible that parties of the proceedings are giving their written testimony in the pre-trial investigation. Courts also accept, that everyone does not have to always be physically in the court, but can participate via video call or not at all, if it does not violate the procedural rights of the party.
Hungary	Use of electronic communication become more general, answers were mainly provided in digital format.
Luxembourg	Improvement of electronic transmission / correspondence.
Malta	Using more applications like Zoom and Teams and avoiding too much correspondence.
Portugal	Implementation of direct digital communication channels; reply in digital format, mainly by e-mail, instead of paper/post; the electronic means of communication were more intensively used - thus more speed.
Slovak Republic	With more and more cases connected with cybercrime (partly related to the COVID-19 pandemic), there are more experienced investigators and prosecutors.

Considering the negative effects caused by the pandemic, 34.7% of the respondents claimed procedures became longer. This is reported as the effect of the reduced capacity caused by social distancing and restrictive measures. However, still 30.6% declared no negative impacts were experienced.

Further negative effects reported by the judicial authorities surveyed are listed in Table 2.

Table 2: Negative effects of the COVID-19 pandemic

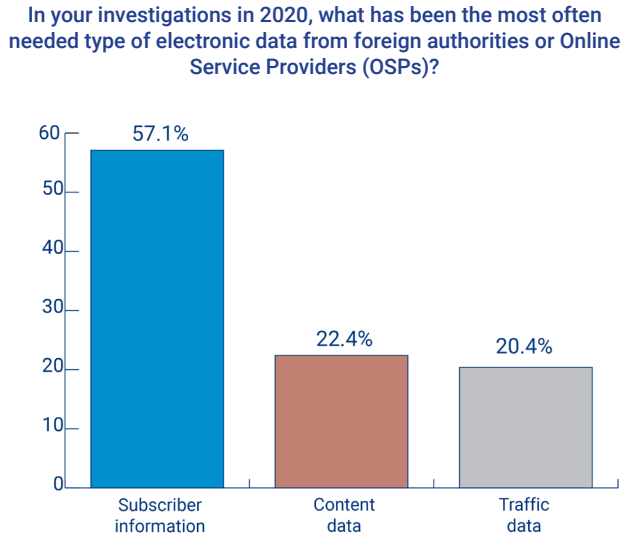
Belgium	Capacity problems lead to more delays in the execution of requests. Less formal requests often are also ill founded, not correctly motivated. Due to the lockdowns, there was not always someone present in the office or could not be reached in time, so that delays in the execution sometimes meant that digital evidence was lost.
Croatia	Reduced means of travel; lots of requests; reduced capacity due to the social distancing measures, confidentiality.
Estonia	In many of the criminal cases, where we before had coordination meetings with other participants of the Joint Investigation Teams or law enforcement agencies abroad, we had to adjust our working methods. Nevertheless, we were able to even plan a Joint Action Day during the travel restrictions time, so it is still possible to cope. Because of the health reasons, it was very difficult to plan court hearings, especially in a bigger organised crime cases, where defence (but also witnesses and victims who are not interested in participating) used the pandemic to prolong the agreed schedule.
Germany	The pandemic slowed down the work flow pretty dramatically which is why requests took longer, people were not available.
Ireland	We had limited time to complete work with having to mind our children at the same time.
Latvia	The MLA and EIO took more time than often, because the responsible services were busier in this situation. Reduced capacity due to the social distancing measures.
Malta	Lockdown in courts and in other institution.
Netherlands	Restrictive measures in place due to the pandemic have led to some delays in some investigations. For example interviewing witnesses/searching delayed due to lockdown in an area. Played out both domestically and with legal aid requests made by us.
Portugal	A number of people working from home in communication providers - thus less speed when responding to requests.
Slovak Republic	In some states only requests for most serious offences were executed. The execution of some requests was much longer than it used to be. Communication possibilities were also reduced; there were difficulties with hearing witnesses abroad so the MLA took too long.
Sweden	Longer responses when court decision needed for the execution.

C. Cross-border requests and data disclosure

The data in need

Depending on the type of the investigation, different types of electronic data are needed. The data categories provided by the Council of Europe 'Budapest' Convention on Cybercrime and its Explanatory Report, namely Basic Subscriber Information, Traffic Data and Content Data, were used as a reference in the survey.

The compiled information indicated that Basic Subscriber Information[23] – such as name, e-mail or phone number – was the most sought electronic data from foreign authorities or from OSPs during the investigations conducted in the EU in 2020. The leading position of Basic Subscriber Information as the most needed type of data remained unchanged comparing to the investigations of 2019 presenting a similar, and sensibly higher percentage, to the one presented in the SIRIUS EU Digital Evidence Situation Report 2020[24]: 57.1% compared to 52.9%.



The Budapest Convention on Cybercrime and its suggested concept of electronic data division into three categories is considered a common starting point and is often used as a reference for general classification and definition of data categories. Nevertheless, they are not a unique scale as no common legal framework exists.

The different ways of data categorisation may be taken from other legal instruments, from national legislation or even from the varying policies of OSPs. Businesses use different ways of categorisation of data that they collect according to their business models and types of services that they provide.

The EU judicial authorities provided a more detailed overview drawn from their personal experience in the field in 2020. Among those who selected "subscriber information" as the most needed type of electronic data from foreign authorities or OSPs, the following explanation were collated:

- *"Most likely the mere number of possible accounts checked will have resulted in numerously more requests regarding subscriber information then traffic/content data (which also require crimes of a certain level)."*
- *"The trend is that data is requested in a combination of two or all three categories. In most cases, the requests aim to obtain subscriber and traffic data. The high portion of requests aim to obtain all three categories of data."*
- *"Most of the investigations of cybercrimes – but also of crimes that use computer networks, or that are committed within computer networks – require, as a very first information, subscriber information, in view of locating the perpetrator of that crime. Thus, requesting subscriber information is needed in most of the cases, at the very first step of the investigation. A number of cases cannot move ahead without this type of information."*

Following the Basic Subscriber Information, the categories of Content Data that refers to the actual content of a communication –

such as photos, e-mail/messages content, files - and Traffic Data – such as connection logs, IP addresses, number of messages – share almost the equal relevance. Yet, in relation to 2019 results, a decrease in requests for Traffic Data (20.4% from 32.4%) and an increase in the requests for Content Data (22.4% from 14.7%) is recorded.

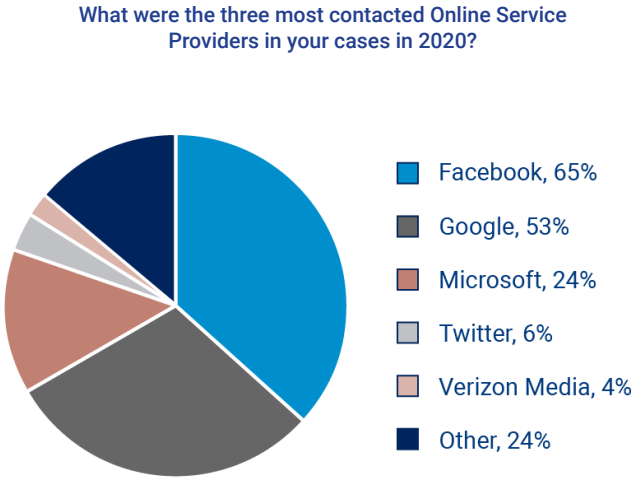
Among those selecting Content Data, as the most needed type of electronic data from foreign authorities or OSPs in 2020, some of the respondents provided further explanations:

- *"Content data is essential and the most difficult to obtain."*
- *"Content data, because in most cases where you ask for content data, you often also request subscriber/traffic data."*
- *"All - Basic Subscriber Information, Content Data, Traffic Data; we need simple information, but in almost every case we need content and sometimes traffic data."*

The feedback received from the judicial authorities is of no surprise, given the different level of sensitivity based on the interference of the disclosure of the data with persons' private lives which also implies differentiated protection of the different data categories.

An addressee of a request

At the receiving end of the requesting process, be it under voluntary cooperation or judicial assistance, ultimately, there are the OSPs. Whether based in the same jurisdiction of the requesting authority or with a worldwide presence, when asked to indicate the three most contacted companies in 2020, EU judicial authorities surveyed returned a quite clear and somewhat predictable overview. As in 2019 it shows a significant predominance of three major U.S.-based tech companies: Google, Facebook and Microsoft[25].



The category of "Other", comprises OSPs that were not mentioned more than once. Among the mentioned OSPs were such companies as PayPal, Apple, Rakuten (Viber service), which have a well-established market and geographical presence, yet, in this overview, they are far from the relevance granted to the top ranking. In addition, this category also represents local OSPs, such as Azet.sk, operating in Slovak Republic, and Melita, operating in Malta.

A Production Order – domestic measure with cross-border effects

The Budapest Convention on Cybercrime provides another option – production order – to request disclosure of Basic Subscriber Information that considers the global reach of services offered by OSPs, regardless of their location. According to Article18[26] "*(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control*".

Therefore, under Article 18, competent authorities can request Basic Subscriber Information from those OSPs that are established outside the domestic jurisdiction but that, at the same time:

- **are in possession or control** over that data: evidence does not need to be physically in possession of the OSP and can therefore be stored elsewhere as long as remotely accessible (e.g. in the cloud); and;
- **offer their services in the territory**: even without a physical of legal presence a company can have a real and substantial connection with the users by means of the services provided.

This measure is also not without limitations. Even if a production order under Article 18 has extra-territorial effects, it remains a domestic measure and, as such, needs to respect the domestic legislation of the issuing State as well as being subject to legal safeguards (e.g. in relation to data protection, human rights and liberties). In addition, providers may remain subject to legal requirements in their country of establishment. Finally, although providing a basis for production orders with a cross-border effect, Article 18 of the Budapest Convention does not provide a basis for enforcement in case of a lack of response[27].

The respondents from 50 % of surveyed Member states reported that the provisions under Article 18 of the Budapest Convention on Cybercrime are included into their national legal frameworks. However, this picture is incomplete as respondents from some countries did not provide a comprehensive answer to this question.

Some respondents who indicated the possibility to issue domestic production orders addressed to foreign-based OSPs offering their services within the territory, shared explanations and direct reference to their national legislation, as presented in Table 3.

Table 3: Reference to national legislation on domestic production orders addressed to foreign-based OSPs

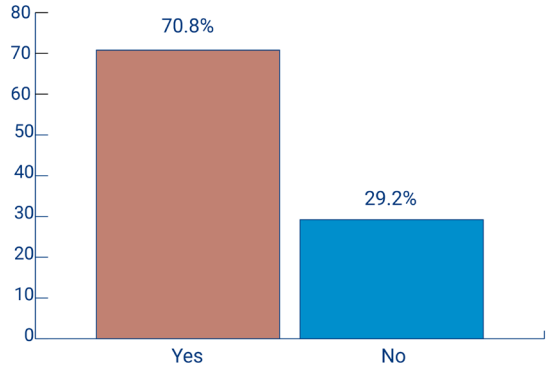
Estonia	There is no special legal framework required under Estonian law. If the data is provided voluntarily and the request to provide it was within Estonian law, it can be used as an evidence in court. Code of Criminal Procedure § 215. Obligation to comply with orders and demands of investigative bodies and Prosecutor's Office (1) The orders and demands issued by investigative bodies and the Prosecutor's Office in the criminal proceedings conducted by them are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia. The orders and demands issued by investigative bodies and the Prosecutor's Office are binding on the members of Defence Forces engaged in missions abroad, if the object of criminal proceedings is an act of a person serving in the Defence Forces. Costs incurred for compliance with a demand or order shall not be compensated for. [RT I, 21.06.2014, 11 - entry into force 01.07.2014] (2) An investigative body conducting criminal proceedings has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately. (3) A preliminary investigation judge may impose a fine on a participant in proceedings, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court order at the request of the Prosecutor's Office. The suspect and accused shall not be fined. [RT I, 23.02.2011, 1 - entry into force 01.09.2011]
Ireland	In a case where an OSP is situated abroad, then the Criminal Justice (Mutual Assistance) Act 2008 allows for an application to Court under section 72 for an international letter of request for evidence. The order would be technically a domestic order but under an MLA request. It is not a domestic production order[28].
Portugal	Article 14 of the Cybercrime Law (Law 109/2009, of 15 September), Article 14 Injunction for providing data or granting access to data 1 - If during the proceedings it becomes necessary for the gathering of evidence in order to ascertain the truth, obtain certain and specific data stored in a given system, the judicial authority orders to the person who has the control or availability of those data to communicate these data or to allow the access to them, under penalty of punishment for disobedience. 2 - The order referred to in the preceding paragraph identifies the data in question. 3 - In compliance with the order described in paragraphs 1 and 2, whoever has the control or availability of such data transmits these data to the competent judicial authority or allows, under penalty of punishment for disobedience, the access to the computer system where they are stored. 4 - The provisions of this Article will apply to service providers, who may be ordered to report data on their customers or subscribers, which would include any information other than the traffic data or the content data, held by the service provider, in order to determine: a) the type of communication service used, the technical measures taken in this regard and the period of service; b) the identity, postal or geographic address and telephone number of the subscriber, and any other access number, the data for billing and payment available under a contract or service agreement, or c) any other information about the location of communication equipment, available under a contract or service agreement. 5 - The injunction contained in this article may not be directed to a suspect or a defendant in that case. 6 - The injunction described under this article is not applicable to obtain data from a computer system used within a legal profession, medical, banking, and journalists activities. 7 - The system of professional secrecy or official and State secrets under Article 182 of the Code of Criminal Procedure shall apply mutatis mutandis.

Principle of admissibility

The potentially applicable rules for the disclosure of the information are not limited to domestic legislation in the country where the requesting authority is based, but concern also the specific requirements or processes in place by the private entities themselves. However, the main focus on the general respect of legislation is admissibility of the obtained information as evidence in the court. Therefore, collection of electronic evidence should be compliant with all the relevant legal safeguards to be considered admissible. Otherwise, if such information is not properly gathered it will compromise the outcome of the criminal proceeding at the end.

When cross-border voluntary cooperation is regarded, the majority of the EU Member States surveyed (70.8%) indicated that evidence gathered directly addressing a foreign-based private entity is considered as admissible in court.

Does your national legal framework allow electronic data to be gathered via cross-border voluntary cooperation by directly addressing a private entity and can the data gathered in this way be admitted as evidence in court?



Some respondents who indicated that in their countries evidence is considered admissible in court, provided explanations referring to their national legislation, as presented in Table 4.1.

Table 4.1- Admission as evidence of data gathered via direct requests to foreign-based OSPs

Belgium	If the OSP offers services in Belgium, electronic data can be gathered via cross-border voluntary cooperation by directly addressing a private entity. The information obtained can be used. Article 32 of the Preliminary Title of the Code of Criminal Procedure stipulates that evidence is inadmissible only if: - the law explicitly sanctions the disrespect of formal conditions by the inadmissibility of the evidence; or - the irregularity committed puts into question the reliability of the evidence; or - the use of the evidence would be contrary to the right of a fair trial.
Estonia	This is allowed according to the Code of Criminal Procedure Article 65 "Evidence obtained on ships during voyages and in foreign states": (1) Evidence taken in a foreign state pursuant to the legislation of such state may be used in criminal proceedings conducted in Estonia unless the procedural operations performed in order to obtain the evidence are in conflict with the principles of Estonian criminal procedure taking into account the specifications provided for in subsection (2) of this section. (2) If the object of criminal proceedings is an act of a person who serves in the Defence Forces and has committed the act outside the Republic of Estonia, evidence taken in a foreign state may be used in criminal proceedings unless the procedural operations performed in order to obtain the evidence are in conflict with the principles of the Estonian criminal procedure regardless of the fact of whether the procedural operation was conducted on the basis of a request for assistance or not. (3) If an act to which the Penal Code of Estonia applies is committed on board a ship during a voyage, the documents prepared by the master of the ship pursuant to § 73 of the Merchant Shipping Code are the evidence in the criminal proceedings[29].

Regarding the respondents who indicated that such evidence is not admissible in their country, additional remarks were received only from the judicial authorities of Slovak Republic, as presented in Table 4.2.

Table 4.2 - Admission as evidence of data gathered via direct requests to foreign-based OSPs

Slovak Republic	An official MLA request is needed in order to use the obtained information as evidence in the criminal proceedings; otherwise, it may be used for intelligence purposes.

Direct access to electronic data

While having national legislation is a safeguard for a potential admissibility of evidence gathered via direct requests from private entities established in other jurisdictions, it might not be necessarily the best approach to follow. Depending on the circumstances, even when investigations have a transnational dimension and cross-border exchange of electronic information is envisaged, EU authorities might not opt to engage with OSPs.

Such circumstances refer to the situations when parties involved in a case (for example the holder of a targeted account, a suspect, a witness) are willing to provide access to electronic information voluntarily, with the consent of the data subject or on the basis of the authorisation of the competent legal authority.

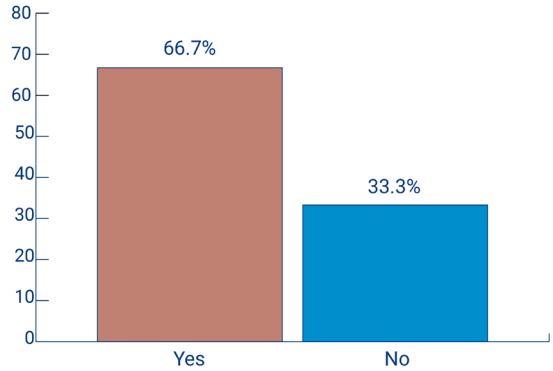
The Budapest Convention on Cybercrime provides an additional alternative form to directly access electronic information[30]. According to the Article 32: *"(1) A Party may, without the authorisation of another Party: (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system"*.

The three key aspects of what Article 32 establishes are:

- **the cross-border aspect:** investigative authorities can obtain information stored in a different jurisdiction.
- **the automatic recognition:** information gathered on this basis as evidence in court is recognised without the need to issue a process under judicial assistance (EIO / MLA).
- **the consent:** the consent of the person who has the lawful authority to disclose the data.

In regard to this investigative measure, a majority of countries surveyed (66.7%) reported it as being incorporated in their national legislation.

Does your national legal framework (for example, on the basis of the Article 32 (b) of the Budapest Cybercrime Convention) allow cross-border direct access to electronic information?



Some respondents provided additional information in relation to their national legal frameworks, distributed in Table 5:

Table 5 - Cross-border direct requests for data disclosure with consent of the data subject

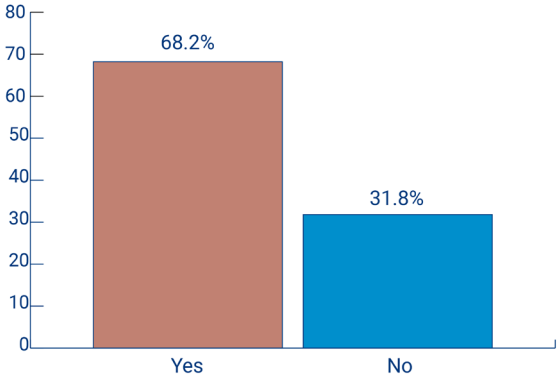
Belgium	Art. 88ter Belgian Code of Criminal Procedure: The investigating judge may extend the search in a computer system or part thereof, begun pursuant to Article 39a, to a computer system or part thereof located in a place other than that in which the search takes place: – if this extension is necessary to reveal the truth about the crime that is the subject of the search; and – if other measures would be disproportionate, or if there is a risk that evidence would be lost without this extension. The extension of the search in a computer system may not extend beyond the computer systems or parts thereof to which the persons entitled to use the computer system under investigation, in particular, have access.(…) If it emerges that these data ARE NOT ON THE TERRITORY OF THE STATE, they will only be copied. In that case, the examining magistrate will immediately inform the Federal Public Service Justice, which will inform the competent authority of the State concerned, if this can reasonably be determined. In the event of extreme urgency, the examining magistrate can order the extension of the search referred to in the first paragraph orally. This order shall be confirmed in writing as soon as possible, stating the reasons of extreme urgency.
Estonia	There is no special legal framework required under Estonian law. If the data is provided voluntarily and the request to provide it was within Estonian law, it can be used as an evidence in court. The legal ground for obtaining this kind of information from another jurisdiction is the same, as in the previous point - Article 65 of the Code of Criminal Procedure.
Ireland	If the national police service in Ireland needed data from a subject and that subject consented to the data being disclosed, then typically the police service would request the data subject to obtain the evidence and hand it over to them.
Portugal	Article 25 of the Cybercrime Law – Law 109/2009, of 15 September, Article 25 Cross-border access to computer data stored when publicly available or with consent The competent foreign authorities without prior request from the Portuguese authorities, in accordance with the rules on transfer of personal data provided by Law No. 67/98 of 26 October, may: a) access data stored in a computer system located in Portugal, where publicly available; b) receive or access through a computer system located in its territory, the data stored in Portugal, through legal and voluntary consent of the person legally authorized to disclose them.

Agreements on public-private partnerships

Similarly, judicial authorities were asked if in their respective countries any public-private partnerships and/or memorandums of understanding were in place with the industry. These agreements are usually intended to strengthen and facilitate either operational or strategic cooperation in criminal matters with telecommunication or other businesses which can have implications to a more swift access to electronic evidence.

The survey indicates that in the majority of countries surveyed (68.2%) such agreements are not in place. However, this does not preclude from the possibility that judicial authorities are not fully aware of the existence of such arrangements as it is the case of two countries where ambiguity is reported as perceived by the respondents.

Are there any public-private partnerships/memorandums of understanding in place with the industry to strengthen and facilitate cooperation in criminal matters?



Although providing a negative answer, the representatives of Slovak Republic and Estonia substantiated their answer with additional information presented in the following Table 6.1 to be read in additional to what is presented in the following Table 6.2:

Table 6.1 – Examples of public-private agreements to facilitate cooperation in criminal matters

Estonia	It is a common practice though, that financial institutions (banks, transfer services) have dedicated a special e-mail address for law enforcement requests.
Slovak Republic	I don´t know about the Memorandum of Understanding of that kind. However, there is a mechanism of National expert group against cybercrime, where public and private authorities may discuss issues of the common interest.

In those EU Members States where such dispositions are established (31.8%), the approaches vary quite significantly from one country to the other, as reported in the following Table 6.2:

Table 6.2 – Examples of public-private agreements to facilitate cooperation in criminal matters

France	Groupe de Contact Permanent (GCP) (Permanent Group of Contact)
Hungary	Law enforcement agencies and the prosecutor's office have direct access points to telecommunication subscriber information and traffic data, through an IT interface. A prosecutor's permission is needed.
Portugal	Protocols with Google, Facebook and Microsoft were signed even before the now existing online platforms.

As noticeable from the divergent practices on the national level, reflected in the above mentioned Tables 6.1 and 6.2, such partnerships are not limited to voluntary cooperation for data disclosure streaming towards US service providers, but are perceived by the authorities as legal cooperation with industry in a broad sense.

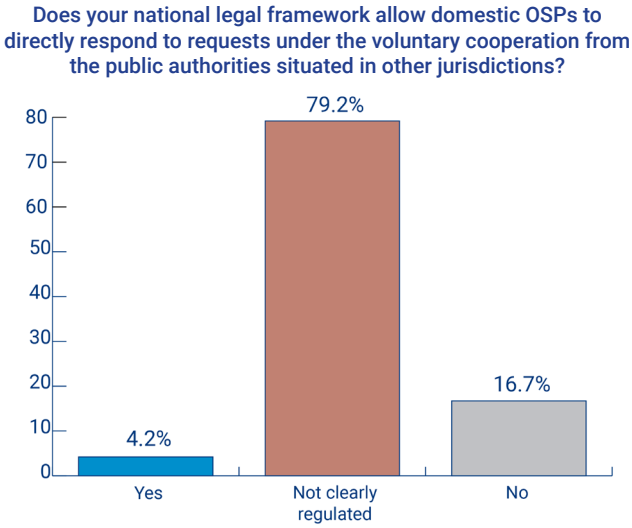
Domestic legal framework in relation to direct requests to OSPs

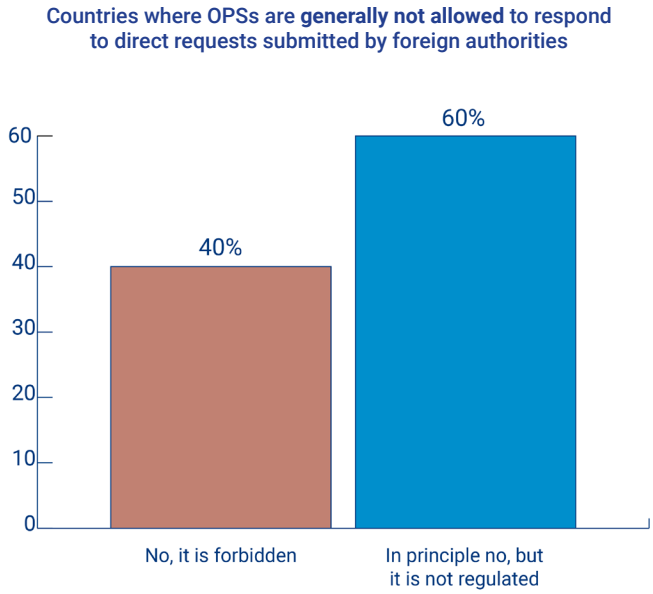
The public-private partnership entails a two-way process: submission of a request to a foreign based company, production and disclosure of information. It is interesting to reverse the situation and look at it from the perspective of the addressees: are OSPs – assuming it is part of their internal policies – allowed by their national legal frameworks to comply with direct requests coming from foreign-based authorities?

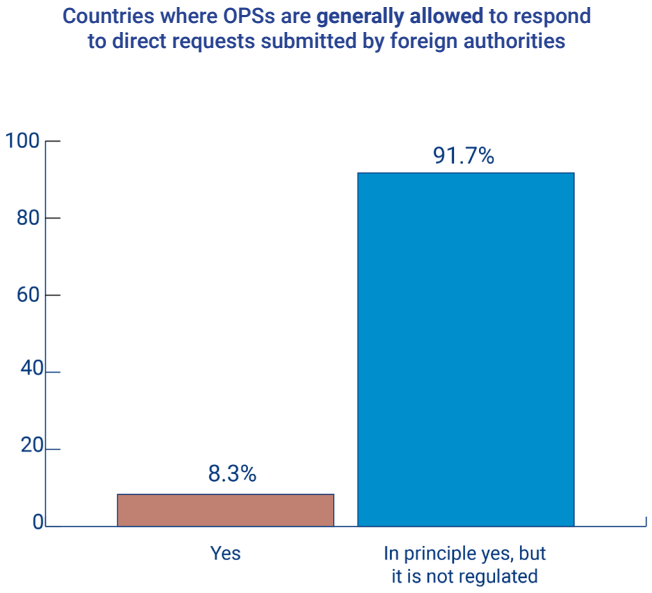
The survey reveals that in the vast majority of the countries which took part in it (79.2 %) this matter lacks of a clear regulation in their respective national legal frameworks. Further breaking down data reported as "not

clearly regulated", most of the countries surveyed (45.9%) states that in principle OSPs are allowed to respond to data request, while for the 25.0% of member states in principle this is not applicable. In a minority of countries (8.3%) ambiguity still persists on this mechanism.

Only respondents representing 4.2% of the surveyed member states provided that OSPs are generally allowed to respond when they receive requests directly from foreign authorities as opposed to the 16.7% who indicated that such option would not be possible.







The results indicate that lack of regulation causes a high uncertainty also for globally active businesses. Even more, companies may be caught in conflicts where abiding by the laws of one country makes them in breach of that of another[31].

Further, looking to the received feedback through a looking glass, it is again interesting to see how a "general principle" based on practice prevails on the legal prescriptions:

1. Within the countries where OPSs are generally **not allowed to respond to direct requests submitted by foreign authorities**, 60 % based response on a general practice while respondents from other 40 % Member states declared that no regulation is in place.

Some respondents provided further explanation as reported in Table 7 to be read in additional to what presented in Table 8 as well:

Table 7 - Countries that generally do not allow domestic OSPs to respond to direct requests from foreign authorities

The Netherlands	The Dutch Penal Code does not provide for this legal figure, but we do see possibilities for making agreements with OSPs if, for example, the country where the OSP is based agrees or if the data is hosted on our territory.
Romania	Only EIO and MLA.
Slovak Republic	The providers are under obligations to respond to the national authorities within the limits of the national legislation.

2. Within the countries where OSPs **are generally allowed to respond to direct requests submitted by foreign authorities**, still the representatives of the absolute majority of the countries (91.7 %) report it as based on a general practice while only feedback received from 8.3 % minority suggests that such regulation is in place.

Substantiating their choice, some respondents provided additional explanation as reported in Table 8:

Table 8 - Countries that generally allow domestic OSPs to respond to direct requests from foreign authorities

Belgium	The Law of 13 June 2005 on electronic communication, explicitly stipulates which authorities are competent to directly request data from a provider. Foreign authorities are not included in this list (but also not explicitly excluded). So should OSP's located in Belgium offer services in other countries and if that country's national law foresees in direct requests, it can be possible.
France	Dispositions of the "Loi de blocage française" (French blocking law).
Ireland	Ireland is the European headquarters of most large US tech companies. Police services from all over Europe contact these companies outside of the MLA system looking for information. These OSP will provide subscriber information without an MLA. They may also provide other data, such as traffic data, but they will not provide content data without an MLA.

3. The feedback received from representatives of 8.3 % Member states, suggested **ambiguous replies** in regard to their national legislation, which proves the difficulties in interpreting legal regime when no established legal framework is in place.

D. Challenges to EU judicial authorities

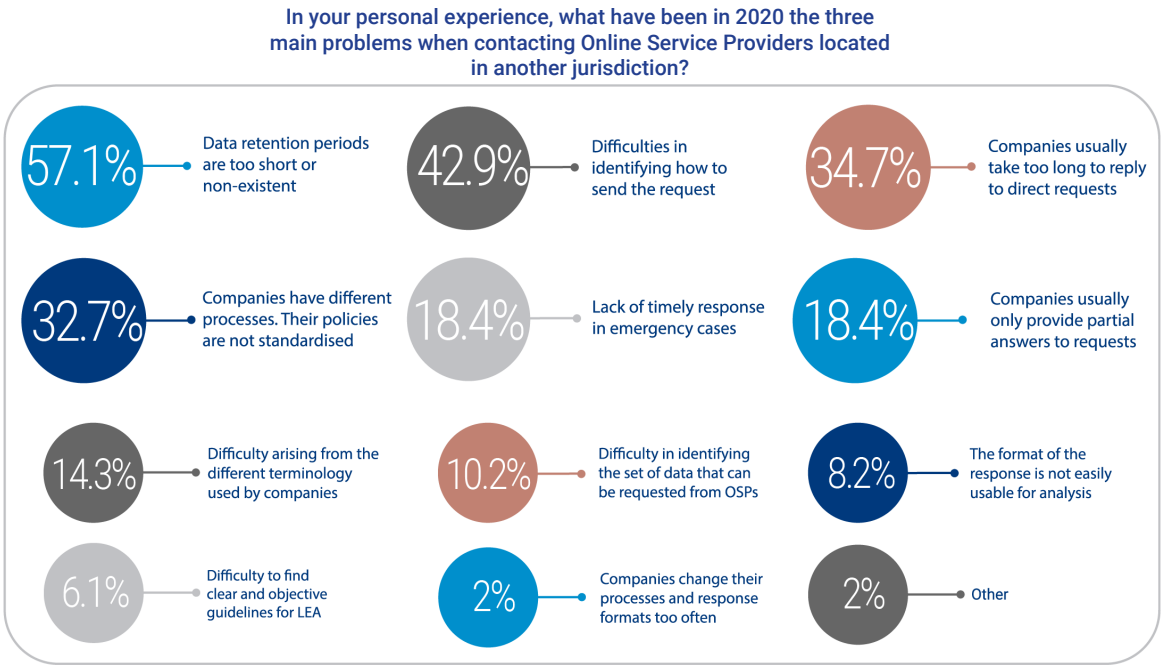
Unique investigation, similar problems

As highlighted in this report, the possibility to directly engage with OSPs based in foreign jurisdiction is with no doubt an efficient tool that allows prompt disclosure and transmission of relevant electronic data to be used as evidence for investigation and prosecution of crime. However, this process is not without some specific challenges.

The challenges, as also identified by the

survey feedback, are often related to the unique nature of each investigation, where the element of time is crucial and any deviation, obstacle or criticality encountered can have a very significant impact on the final outcome of a case.

The EU judicial representatives were requested to identify the three most challenging aspects faced while contacting foreign OSPs with requests for electronic evidence under voluntary cooperation. In 2020, the predominant issue, pinpointed by the 57.1% of the respondents, was the **short data retention periods** of the information collected after a preservation request / order is submitted to the private companies.



The 42.9% of respondents expressed their difficulty in identifying how and where to send requests to companies (for example, establishing the correct entity responsible for cooperating voluntary with public authorities) whereas the 34.7% recognised as an issue the length of reply by OSPs when dealing with incoming requests for data disclosure. For 32.7% of respondents, the main issue identified is the different processes and policies applied by OSPs.

Following, additional problems reported yet with a lower prevalence were:

- "Lack of timely response in emergency cases" and "companies usually only provide partial answers" are equally represented: 18.4%
- Difficulties arisen from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 14.3%
- Difficulty in identifying set of data that could be requested from companies: 10.2%

- Format of the response is not easily usable for analysis (for example, non-editable PDF form): 8.2%
- Difficulty to understand or find clear and objective guidelines provided by the company: 6.1%
- Companies change processes and response formats too often: 2%

In addition, some representatives of the EU judicial authorities provided the following reflections on the problems they faced directly interacting with the OSPs in their investigations in 2020. Those difficulties were related to the identification of the relevant jurisdiction and addressee, the lengthy period until replies are received, incomprehensive replies, or lack of cooperation overall as listed in the following Table 9:

Table 9 - Issues faced by judicial authorities in interacting with OSPs in 2020

Estonia	Many OSPs, especially cryptocurrency entities, do not want to cooperate with law enforcement and reply late or not at all.
Ireland	Difficulty identifying the relevant person to address the request to. Difficulty with MLA process, where the paperwork is prepared here in Ireland, transmitted through our Central Authority and then just gets lost in the receiving state.
Luxembourg	Identify the location of the stored data and the relevant entity responsible for it
Romania	OSPs provide partial answers.
Poland	No response or refusal to provide data.
Slovak Republic	Absence of uniform or single application form for all OSPs and one procedure for all OSPs
Spain	Depending on the evidence needed, even with large scale fraud committed against medium or little firms (which meant that they were left with no money whatsoever to continue their activity), the process for obtaining information is too long and, given that OSPs allow registration with any denomination or address (even fake ones), sometimes absolutely useless.

A tendency of reoccurring issues

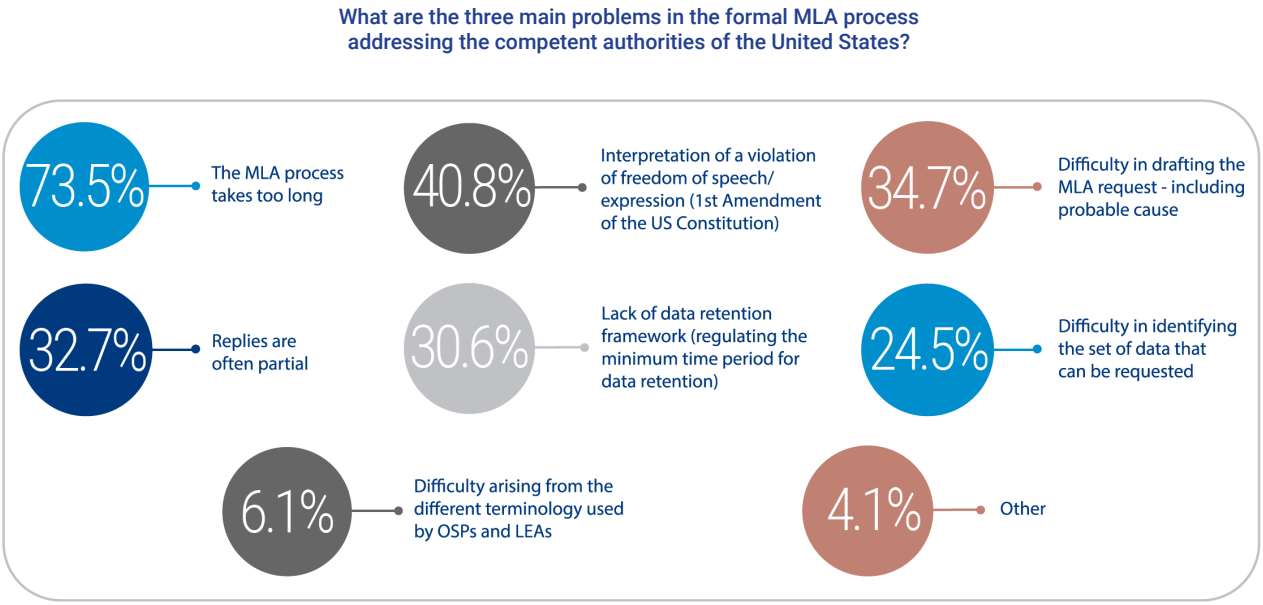
Comparing the information featuring the SIRIUS EU Digital Evidence Situation Report 2020, a clear tendency is emerging. Even if representing different weights, the reoccurring issues polling higher in the recent years refer to:

- the short data retention periods
- the difficulty in identifying correct methods and channels for the submission of requests.
- the perceived lack of timely responses from OSPs to direct requests
- the very diversified policies in place among companies
- the lack of timely response in emergency cases.

The MLA processes towards competent authorities in the United States

Looking for the insights in their criminal investigations in 2020, the EU judicial authorities were asked to identify the main problems encountered with MLA processes towards competent authorities in the United States. The vast majority (73.5%) of respondents reported the long time needed for MLA procedures as the most challenging issue encountered in 2020. Proving again, that this is a recurring and long-standing challenge for the EU authorities.

Following this main procedural issue, 40.8% and 34.7% of respondents identified respectively the "Interpretation of a violation of Freedom of speech/expression (First Amendment of the Constitution of the US)" and the "Difficulties in drafting the MLA requests including probable



cause" as problematic when addressing legal processes to authorities based in the U.S. Another relevant problem, identified by the 32.7% of respondents, is that replies are often partial while for 30.6% of respondents recognised the lack of a data retention framework as one of the main issues.

Lastly, additional problems reported yet with a lower prevalence among the surveyed are:

- Difficulty in identifying set of data that could be requested: 24.5%
- Difficulties arisen from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 6.1%
- Other: 4% (e.g. impact of COVID-19 to the length of the procedure).

Taken all together, looking back at what was reported in the SIRIUS EU Digital Evidence

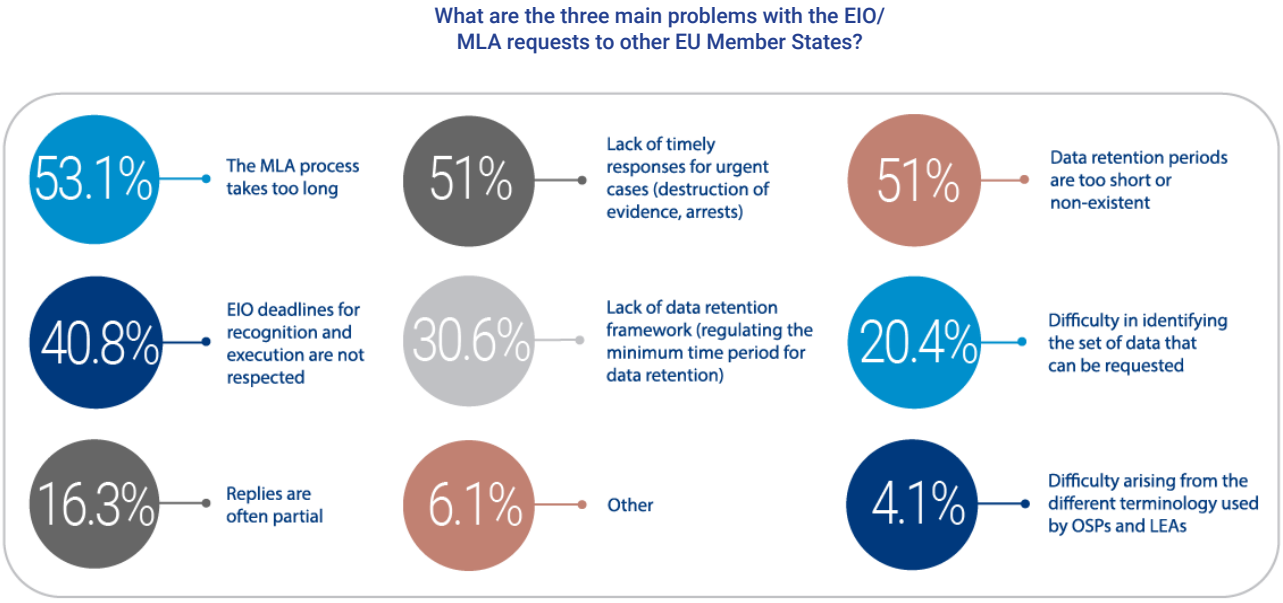
Situation Reports reflecting the situations in 2019 and 2018, the three main challenges highlighted in 2020 appear to be the same both in terms of content and actual impact on daily activities of EU authorities.

Despite the recurring challenges, some experience of the judicial authorities demonstrates that in some instances a good degree of cooperation is established between EU and US authorities, as testified by a respondent who noted: "*In recent years, the execution of MLA requests by the U.S. authorities has improved. Almost daily communication with the U.S.: central authority is very helpful* […]".

The EIO/ MLA processes towards competent authorities in other EU Member States

Not all the OSPs are U.S.-based and several have legal entities established in EU territory. When seeking a disclosure of data, such entities can be addressed via judicial cooperation channels, and therefore the EU judicial authorities were asked to identify the main problems with the EIO/ MLA requests to other EU Member States.

Regarding the use of the EIO or MLA with other EU Member States, 53.1% of respondents identified the length of the procedure as the main problem, followed closely by the 51% who equally identify the lack of timely responses when it comes to urgent cases and the short data retention period as a main issue.



Further, the "length of EIO procedure" was identified by the 40.8% of respondents while the "lack of data retention framework" was indicated as a relevant challenge by the 30.6% of surveyed. For the 20.4% of the respondents, the main issue is the difficulty in identifying the set of data that can be requested and for the 16.3% of the surveyed "replies are often

partial", whereas a minority (4.1%) described the "difficulty arisen from the different terminology used by OSPs" as an issue. Finally, among those who selected "Others" (6.1%) one of the respondents added: "No comprehensive information available due to direct cooperation between judicial authorities. One of the problem is the type of providers /e.g. hosting/VPN".

A comparison to the last year's SIRIUS EU Digital Evidence Situation Report, shows that even if with different weights, the general reference to the length of procedures, element of time in providing response and in relation to data retention periods as well as lack of related frameworks keep emerging as the most prominent ones among EU authorities.

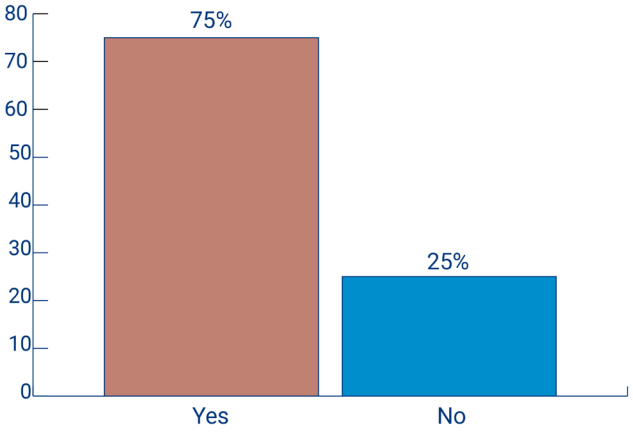
The data retention regime

It goes without saying that the request and disclosure of data for investigation and prosecution of crimes are only possible when the actual information are stored, retained and potentially accessible from OSPs. At European level the current absence of a unified data retention regime of electronic communication data, resulting from the annulment of the Data Retention Directive by the CJEU poses challenges to cross-border investigations involving electronic evidence. The growth of volume of available personal data was accelerated by intense use of social media and the proliferation of connected devices which lead to increased concerns related to privacy and data protection. Accordingly, rules related to data retention have been subject of discussions regarding mainly the balance between obligation for OSPs to retain data and the interference with the right to privacy. The aforementioned has undoubtedly, affected the data retention regulation in different Member States, resulting in a landscape that is far from being homogenous across the EU.

Looking at this recurrent element identified in the survey as one of the key issues, the EU judicial community was asked whether at national level a regime regulating retention of data is in place.

The analysis of the received responses shows, that in the majority of the EU countries surveyed (75%) a data retention regime is in place while 25 % of the surveyed countries do not have a domestic regime on this matter.

Is there a data retention regime in place in your country in relation to data held by the OSPs?



Some of the respondents who reported having a data retention regime in their Member States substantiated their choice with the additional explanations provided in the following Table 10:

Table 10 - Countries that have a data retention regime in place

Ireland	Following the case of Digital Rights Ireland, the Irish legislation dealing with retention of data under the 2006/24/EC Directive - the Communications (Retention of Data) Act 2011 has been challenged in court. We no longer use this Act to obtain evidence from OSPs. There is a high profile murder case Graham Dwyer v DPP & Ireland which has gone to our Supreme Court on this point and the Supreme Court has made a preliminary reference to the CJEU.
Portugal	6 months and 1 year, being 1 year for the more serious offenses

On the other side of the spectrum, those who reported not having a data retention regime in place in their Member States, further described what is detailed in Table 11:

Table 11 - Countries that do NOT have a data retention regime in place

Belgium	The Belgian Constitutional Court, by decision of 19 July 2018, asked for a preliminary ruling (Case C-520/18) concerning the processing of personal data and the protection of privacy in the electronic communications sector. Following the CJEU decision, the Constitutional Court recently annulled the current data retention laws. Articles 126 and 127 of the Electronic Communications Act (13/06/2005) no longer stand, as they impose a general and indiscriminate obligation on providers to retain traffic and location data. Providers are thus no longer obliged to keep these data. It is up to the courts to judge the validity of already collected data. New legislation in development.
Germany	The data retention regime is formally in place but suspended by the Federal Network agency which does - as long as the legislator does not provide a new regime which complies with the rulings of the National Constitutional Court and the CJEU - refrain from orders against the OSPs.

Additionally, in this year's survey reference was made to some recent preliminary rulings of the CJEU in order to verify whether they had an impact on the national legislation with regard to data retention regime, specifically:

Table 12 - Preliminary rulings of the CJEU

6 October 2020 **LA QUADRATURE DU NET AND OTHERS** *Joined Cases C-511/18, C-512/18, C-520/18*[32]	EU law does not allow general and indiscriminate retention of traffic and location data. By contrast, some measures are allowed, for specific purposes, under certain conditions: • General and indiscriminate retention, in case of a serious threat to national security; • Targeted retention, limited to categories of persons or using geographical criterion; • Expedited retention in case of serious criminal offences or attacks on national security; • General and indiscriminate retention of IP addresses assigned to the source of an Internet connection; • General and indiscriminate retention of data relating to the civil identity of users. Automated analysis and real-time collection by service providers is allowed in specific situations. EU law does not allow general and indiscriminate retention of personal data by providers of access to online public communication services and hosting service providers[35].
6 October 2020 **PRIVACY INTERNATIONAL** *Case C-623/17*[33]	General and indiscriminate transmission of (and thus access to) T&L data to security and intelligence services for the purpose of safeguarding national security is not allowed[36].
2 March 2021 **PROKURATUUR** *Case C-746/18*[34]	Access to a set of traffic or location data, allowing precise conclusions to be drawn concerning a person's private life, is allowed only in order to combat serious crime or prevent serious threats to public security, regardless of the duration of the access and quantity or nature of the data. The public prosecutor's office cannot be granted the power to authorise access of a public authority to traffic and location data for the purpose of a criminal investigation[37].

On this matter, some respondents provided further comments reported in Table 13.

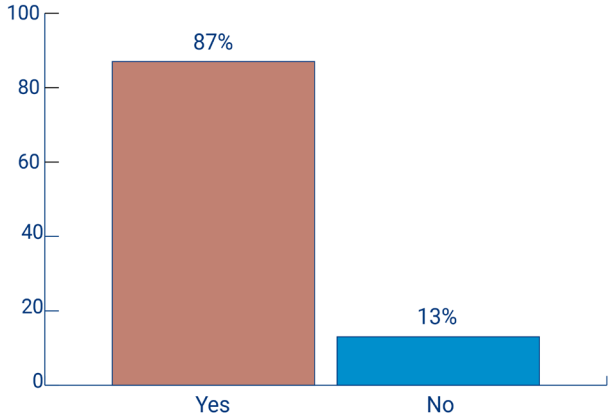
Table 13 - Impacts of the CJEU rulings

Estonia	Because of the case K. v Prokuratuur C-746/18 of 2 March 2021, Estonian Ministry of Justice is preparing changes in the Code of Criminal Procedure so that in the future, data can only be collected with the court order, not with a prosecutor's permit, as it has been so far. Estonian Supreme Court has not yet decided on further positions from the before mentioned case, but is expected to do so in the next months.
France	Yes, data retention regime is in place consequently to the "Quadrature du Net" ruling.
Lithuania	I consider that the current National legislation governing the storage and use of electronic data in criminal proceedings is in line with the above-mentioned rulings of the EU Court of Justice and is in line with the principles of the Charter of Fundamental Rights of the European Union.
Luxembourg	The data retention provisions need to be amended based on the recent rulings.
Spain	The doctrine derived from the CJEU is being ignored.
Sweden	So far there has been no effect of the recent rulings of CJEU.

Data preservation regime

Considering data preservation, most of the EU countries surveyed (87 %), reported having an established regime for data preservation in relation to data held by OSPs. Just a small minority of countries (13 %) reported not having a national regime in place.

Is there a data preservation regime in place in your country in relation to data held by the OSPs?



Most of the EU Member States where such dispositions are in place have provided further information and reference to their national legislation as reported in Table 14:

Table 14 - Additional elements of data preservation regime

Belgium	When investigating of crimes/criminal infractions and if there are grounds for believing that data stored, processed or transmitted by means of a computer system is particularly vulnerable to loss or to alteration, any officer of the judicial police may, by a well-founded and written decision, order one or more natural or legal persons to retain the data in their possession or under their control (art. 39ter Belgian Code of Criminal Procedure).
Estonia	According to the Electronic Communications Act, OSPs have an: § 111-1. Obligation to preserve data (2) The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data: 1) the number of the caller and the subscriber's name and address; 2) the number of the recipient and the subscriber's name and address; 3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address; 4) the date and time of the beginning and end of the call; 5) the telephone or mobile telephone service used; 6) the international mobile subscriber identity (IMSI) of the caller and the recipient;

Estonia *(continued)*	7) the international mobile equipment identity (IMEI) of the caller and the recipient; 8) the cell ID at the time of setting up the call; 9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved; 10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated. (3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data: 1) the user IDs allocated by the communications undertaking; 2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network; 3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication; 4) the user ID or telephone number of the intended recipient of an Internet telephony call; 5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services; 6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID; 7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone; 8) the Internet service used in the case of electronic mail and Internet telephony services; 9) the number of the caller in the case of dial-up Internet access; 10) the digital subscriber line (DSL) or other end point of the originator of the communication. [RT I 2007, 63, 397 - entry into force 15.03.2009] (4) The data specified in subsections (2) and (3) of this section shall be preserved for one year from the date of the communication if such data are generated or processed in the process of provision of communications services. Requests submitted and information given pursuant to § 112 of this Act shall be preserved for two years. The obligation to preserve the information provided pursuant to § 112 rests with the person submitting the request."
Finland	Information Society Code, Section 157 - Obligation to store data for the purposes of the authorities. Notwithstanding the provisions of this Part concerning the processing of traffic data, an undertaking designated by a separate decision of the Ministry of the Interior that has submitted a telecommunications notification (operator under the retention obligation) shall ensure, under the conditions prescribed below, that data under the retention obligation as referred to in subsections 2 and 3 are retained in accordance with retention times laid down in subsection 4. Data to be retained may be used only for the purposes of solving and considering charges for criminal acts referred to in Chapter 10(6)(2) of the Coercive Measures Act (806/2011). The retention obligation applies to data related to: 1) a telephone service or SMS service provided by an operator under the retention obligation including calls for which a connection has been established but the call remains unanswered or is prevented from being connected due to network management measures; 2) Internet telephone service provided by an operator under the retention obligation, meaning service provided by a service operator enabling calls that are based on Internet protocol through to the end customer; 3) Internet access service provided by an operator under the retention obligation; In services referred to in subsection 2(1 and 2) above the retention obligation applies to the name and address of a registered user or a subscriber, subscription identifier and data that can be used to identify a communications service user or communications, including call transfers, according to the type, receiver, time and duration of communications. With regard to service referred to in subsection 2(1) the retention obligation applies to data that can be used to identify the device used and the location of the device and the subscriber connection it uses in the beginning of communications. With regard to the service referred to in subsection 2(3) above the retention obligation applies to the name and address of a subscriber and registered user, subscription identifier, installation address, and data that can be used to identify the communications service user, the device used in communications and the time and duration of the service. The data to be retained must be limited to what is necessary for identifying the facts referred to above in this section, with due consideration to the technical implementation of the service. The data of the services referred to above in subsection 2(1) must be retained for 12 months, the data of the services referred to in subsection 2(3) for 9 months and the data of the services referred to in subsection 2(2) for 6 months. The data retention time starts with the time of the communications.

Finland *(continued)*	The retention obligation does not apply to the contents of a message or traffic data generated through the browsing of websites. A requirement for the retention obligation is that the data are available and generated or processed in connection with publicly available communications services provided on the basis of this Act or the provisions of the Personal Data Act (523/1999). Further provisions on a more specific definition of data under the retention obligation may be issued by Government Decree. Technical details of data under the retention obligation are defined in a Finnish Communications Regulatory Authority regulation.
Hungary	Basic subscriber information, traffic information can be provided usually for 1 year.
Italy	All categories of data are preserved but for different periods depending on category.
Latvia	An electronic communications merchant has the following obligations: in accordance with the procedures specified in Section 71. 1 of this Law, to ensure the storage of the retained data for 18 months, as well as their transfer to the institutions referred to in Section 71. 1, Paragraph one in accordance with the procedures specified by law, if these institutions so request.
Lithuania	Paragraph 2 of Article 65 of the Law on Electronic Communications of the Republic of Lithuania imposes an obligation on providers of public communication networks and / or public electronic communication services to preserve and provide the data generated or processed by them for the investigation, detection and prosecution of serious and very serious crimes. This data to the competent authorities must be provided free of charge. Paragraph 6 of Article 66 of the Law establishes the obligation to store data for 6 months from the date of communication.
Luxembourg	Chapter X. - Rapid storage of computer data, (L. 18 July 2014) Art. 48-25. (L. 18 July 2014) Where there is reason to believe that data stored, processed or transmitted in an automated data processing or transmission system, useful for the manifestation of the truth, may be lost or altered, the State Prosecutor or the investigating judge may have the data promptly and immediately stored for a period not exceeding 90 days.
Portugal	Subscriber and traffic data (6 months/1 year).
Slovak Republic	Section 91 of the Code of Criminal Procedure provides for expedited preservation [under Article 29 of the Budapest Convention on Cybercrime]. If data freezing (for the future communication) is in question, yes, such mechanism also exist in data freezing (Section 116 of the Code of Criminal Procedure).
Slovenia	Every available data connected to a user.
Spain	Law 25/2007. Article 3. Data subject to conservation. 1. The data to be kept by the operators specified in Art. 2 of this Law, are the following: a) Data necessary to trace and identify the origin of a communication: 1) With regard to fixed network telephony and mobile telephony: i) Call telephone number ii) Name and address of the subscriber or registered user. 2) With regard to Internet access, Internet e-mail and Internet telephony: i) Assigned user identification, ii) The user identification and telephone number assigned to any communication accessing the public telephone network, iii) The name and address of the subscriber or registered user to whom an address of Internet protocol (IP), a user ID or phone number b) Data required to identify the destination of a communication: 1) With regard to fixed network telephony and mobile telephony: i) The number or numbers dialled (the destination number or telephone numbers) and, where other services are involved, such as the number or numbers to which the calls are transferred, ii) The names and addresses of registered subscribers or users. 2) With regard to Internet e-mail and Internet telephony: i) The user identification or telephone number of the recipient or recipients of a telephone call over the Internet, ii) The names and addresses of subscribers or registered users and the user identification of the recipient of the communication. c)Data required to determine date, time and duration 1) For fixed network telephony and mobile telephony: the date and time of the start and end of the call or, where appropriate, of the call service messaging or multimedia service. 2) With regard to Internet access, Internet e-mail and Internet telephony: i) The date and time of connection and disconnection of the registered Internet access service, based on a given time zone; and the Internet Protocol address, whether dynamic or static, assigned by the Internet Access Provider to a communication, and the identification user or subscriber or registered user, ii) The date and time of connection and disconnection of the Internet e-mail service or Internet telephone service, based in a given time zone.

Spain *(continued)*	d)Data required to identify the type of communication 1) For fixed network telephony and mobile telephony: the telephone service used: type of call (voice transmission, voice mail, conference, data), supplementary services (including forwarding or transferring calls) or messaging or multimedia services used (including short message services, advanced multimedia services and multimedia services). 2)With regard to Internet e-mail and Internet telephony: the Internet service used. e)Data required to identify user communication equipment or what is considered to be communication equipment: 1)With regard to fixed network telephony: the source and destination telephone numbers. 2) With regard to mobile telephony: i) Source and destination telephone numbers, ii) The international mobile subscriber identity (IMSI) of the calling party, iii) The international identity of the mobile equipment (IMEI) of the calling party, iv) The IMSI of the party receiving the call, v) IMEI of the party receiving the call, vi) For anonymous prepaid services, such as prepaid card services, the date and time of the first activation of the service and the location label (the cell identifier) from which the service has been activated. 3) With regard to Internet access, Internet e-mail and Internet telephony: i) The home telephone number in case of access by dialling, ii) The digital subscriber line (DSL) or other identifier terminal point of the author of the communication f) Data required to identify the location of mobile communication equipment: 1) The location tag (cell identifier) at the beginning of the communication. 2) The data that make it possible to fix the geographical location of the cell, by reference to the location label, during the period in that communications data are kept. 2. No data revealing the content of the communication may be retained under this Act.

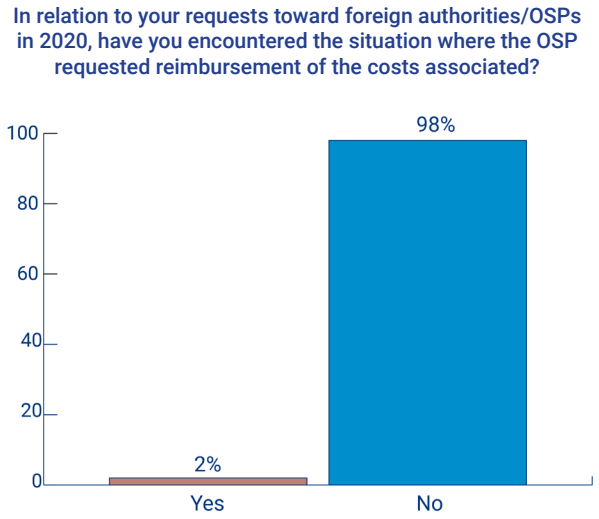
Cost reimbursement system

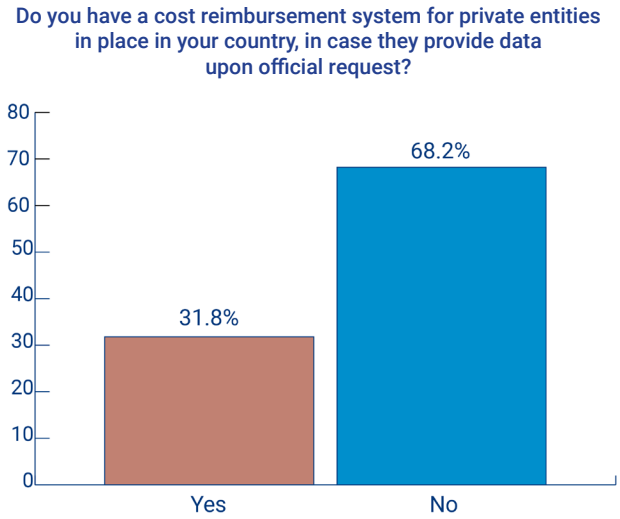
Looking ahead at potential future challenges that could have a role in the process of request and disclosure of electronic information, two questions of the survey focused on the so-called cost-reimbursement system. Such system entails that OSPs may seek reimbursement for the expenses occurred in responding to authorities' requests for information as provided by law or domestic legislations (e.g. cost of data storage device, postal fees). For instance, the U.S. federal law allows charging governmental authorities in exchange of their cooperation[38] and some EU Member States (e.g. Austria and Belgium) have similar provisions in place too[39].

This mechanism, features as a standard part of some OSPs policies, nevertheless, it seems limited and not widely applicable to EU-based direct requests for data as only 2 % of the respondents indicated that in their investigations in 2020, OSPs or foreign authorities posed them a request of cost reimbursement.

The comparative analysis of the feedbacks received on the matter shows that the majority of EU Member States surveyed do not have a cost reimbursement system in place (68.2 %) and the vast majority (98%) of the respondents stated that they have never received a claim for compensation of the costs associated with reply to a production order in their investigations in 2020.

The situation on the domestic legal framework related to cost reimbursement as well as its actual application either by the OSPs or foreign authorities to which request is submitted,





demonstrates, that such a mechanism does exist, yet its current application is quite sporadic. Among those respondents who reported having a cost reimbursement system in place domestically, Belgium specified: "*Following the national law on costs related to criminal procedures, certain costs can be reimbursed if they meet the conditions set out in our national law. The Royal Decree of January 9th 2003 on the modalities of the legal obligation to cooperate following a judicial request relating to electronic communications, holds further specifications*." In parallel, only one respondent reported having experienced receiving a bill for the handing over of the data from an OSP.

Even though cost reimbursement system has not yet appeared as having a significant impact in accessing digital data, it has a huge potential to transform into a future growing trend impacting data acquisition process to a greater extent.

Encryption

Another long-standing issue which poses concrete and significant challenges in the field of electronic evidence is related to encryption. This topic was not specifically addressed by the survey, yet as pointed out by several sources[40], because of wide application of encryption, existing techniques such as interception are less effective or technically impossible, and encryption may lead to loss of critical intelligence, attribution possibilities and evidence.

Acknowledging that encryption has become an essential component for safeguarding fundamental rights, digital sovereignty and innovation[41], the call of law enforcement and judicial authorities for specific provisions to be introduced[42] in order to obtain the information needed as evidence for investigations cannot be underestimated. Criminal organisations are increasingly using encrypted communication tools and continue to find methods to leverage the latest technologies to evade investigations[43].

At present time, what remains a certainty, is that the most pressing challenges related to the technological developments and legal landscape surrounding the field remain matter for research and discussion in search for a response.

The needs for capacity building and knowledge exchange

Looking for the possibilities to best adhere and support EU judiciary with the required know-how in relation to a cross-border acquisition of electronic information, this year, the representatives of the EU judiciary were invited to list topics of their needs and interest.

A variety of topics was identified by the surveyed judiciary ranging from language courses (mainly English) to different aspects of data acquisition channels and instruments: judicial co-operation networking in different states; constantly updated information on the possibility to obtaining evidence lawfully from service providers in different countries; voluntary cooperation procedure, the legal aspects and the reputation of service providers; common trainings of prosecutors, police and OSPs on obtaining electronic evidence; standard requests/procedures for payment services providers; sharing experiences.

All those reflected areas indicate towards the evolving landscape that law enforcement and judicial authorities have to deal with as well as the gap of expertise and know-how in the field of electronic evidence.

E. Needs of practitioners to improve the current legal framework for gathering electronic evidence according to the European Judicial Network

In addition to the mentioned challenges, in this section EJN further elaborates on the improvements needed for the legal framework on obtaining cross border electronic evidence.

Currently, the EU legal framework for obtaining any type of evidence, including electronic ones, is based mainly on the Directive 2014/41/EU on the EIO in criminal matters[43] ('EIO Directive'). This Directive allows judicial authorities in one Member State to obtain evidence from another Member State by establishing a procedure based on the principle of Mutual Recognition. Besides, the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the EU[45] ('MLA 2000 Convention') is the legal basis generally applied for Denmark and Ireland that are not bound by the EIO Directive[46].

Additionally, most EU Member States – except Ireland - ratified the Council of Europe's Budapest Convention on Cybercrime which specifies a number of legal standards and international mechanisms for cooperation against cybercrime. Under the Budapest Convention, countries are required to establish powers and procedures to allow authorities to obtain electronic evidence and to provide each other mutual legal assistance, not limited to cybercrime. The

Budapest Convention also requires legislation includes the possibility to request subscriber data directly from OSPs when services are rendered in the state party[47]. Hence, as expressed earlier, direct cooperation with the OSPs is also a key element for practitioners.

Overall, for the EU when combining the provisions of the Budapest Convention and of the system of mutual recognition provided by the EIO Directive, a number of advantages exist when trying to obtain electronic evidence compared to before 2017 when the EIO was not yet in force and transposed by the Member States[48]. However, the EIO does not cover every eventuality and does not respond to the dynamic and volatile nature of the electronic evidence. Hence, these instruments are still deemed insufficient by practitioners[49]. The issues increase exponentially when trying to obtain replies to judicial requests on electronic evidence from companies that are not based or have representatives dealing with the requests for evidence within the EU.

The European Union and the Council of Europe have been respectively working on adopting legislative instruments that would complement the current legal framework. However, to date practitioners are still facing many barriers and continuously search for legal methods that would allow them to gather cross-border electronic evidence with procedures that allow for standardisation and speed as well as sufficient regulation to ensure legal certainty, flexibility and the protection for individual and victims' rights.

During the EJN e-Evidence Working Group meetings and the latest Plenary Meetings of the EJN[50], practitioners indicated that they require that a common legal framework is provided for the EU and the international community in order to be able to obtain electronic evidence in a secure and faster manner. They pointed out particular aspects of e-evidence that need to be addressed with more effective regulation:

- voluntary cooperation and admissibility;
- data retention;
- standardised forms;
- definition of e-evidence;
- time limits;
- language.

The reasons why these particular changes are necessary are expressed further in this chapter.

Cross-border Cooperation with OSPs

In general, main OSPs offering services in the European Union have been not only been providing direct support to national authorities for the preservation and production for subscriber information, but also cooperating with the SIRIUS project to guide authorities on which type of evidence could be requested and their requirements.

However, the lack of regulation on the voluntary cooperation mechanisms requires OSPs to create internal systems for checks into the domestic legal system of the different countries. Understandably, this system also triggered companies to

set different data retention periods and individual tailored procedures which as a result demands examining different sources of information, additional time from authorities for the preparation of requests and sometimes turning them into unfruitful results. On top, the lack of enforceability creates legal uncertainty for authorities resulting in the loss of time and resources for their investigations.

A set of rules for cooperation with OSPs would provide a clear understanding for both private business and authorities on the extent of the cooperation, clear timelines and methods to obtain it.

In addition, a system that would allow the secure transmissions of requests to OSPs as intended by the e-Evidence Digital Exchange System would increase the security, use a set of criteria and elements for the exchange of information as well as provide authorities with a clear addressee for the requests for cooperation.

Admissibility of Evidence gathered by voluntary cooperation

In line with the information provided in the EJN Fiches Belges and the responses of the Member States[51], some jurisdictions deem admissible, sometimes under certain conditions, the subscriber information gathered directly by the mechanism of voluntary cooperation. Some countries, for instance Hungary, Romania, Latvia and Slovakia, indicated that a formal judicial request is needed in order to use the obtained information as evidence in the criminal proceedings; otherwise, it may only be used for intelligence purposes.

It is therefore important that the EU and/or international legal instruments include provisions that would create the conditions for Member States to incorporate in their procedural law mechanisms for obtaining this type of evidence directly from foreign OSPs that could be admissible in court across the EU.

In line with the data provided by the Survey[52] the lack of regulation causes challenges for authorities at the time of ensuring that the preservation of the electronic evidence is possible and that the production requests arrive on time to the other States.

Undoubtedly, regulation on the data retention periods across the EU would

provide authorities with a reliable system. Additionally, the type of data to be retained is also a key issue for practitioners.

Standardised forms for judicial cooperation

Also when referring to judicial cooperation, standardised forms and/or a simplified method that would be used for cross-border requests for preservation and production would facilitate the application by the receiving countries. In line with the EU practice used in mutual recognition instruments, forms would promote mutual understanding, streamline the information needed and would facilitate future translations where necessary. Hence, the later exchange with other Member States would be coherent and minimize the time spent in drafting the request.

Definition of electronic evidence

The vast majority of Member States – except France, Germany, Hungary, Latvia, the Netherlands, Slovenia and Spain[53] - do not provide for a legal definition of electronic evidence in their legislation. Although practitioners interpret the available provisions to elaborate an understanding on the elements conforming electronic evidence, others have provided indirect definitions by providing procedures for the different type of data or referring even to the Budapest Convention, the CoE Guide for the Convention and doctrine.

Summarizing the replies provided in the EJN Fiches Belges, the common approach among Member States has been that electronic evidence is information/data of evidentiary value that is kept/stored in digital format. However, the understanding of the term electronic evidence may still vary – from the broader concept that any information that is being stored in digital format (e.g., even the document that initially had a physical form, like scanned documents) to the narrower view that electronic evidence is limited to the users data that is processed by the OSPs.

As electronic evidence is required for the investigation of different type of crimes, a common definition for all practitioners could increase domestic awareness on the elements and clarify even further the procedures for acquiring this type of evidence.

Response time

It has been remarked that the current legal framework does not respond to the needs of the investigation. In accordance to the Survey for judicial authorities[54] and the experienced gathered in the discussions taken place at the EJN Plenary Meetings[55], authorities seem to attest that information, particularly, for emergency requests is not received in a timely manner.

With respects to the EIO Directive, the timelines are clearly an improvement to the MLA system, however due to the nature of the digital data, they still do not sufficiently respond to the actual needs of practitioners for obtaining electronic evidence. Producing the electronic evidence does not require

the same time and efforts as other types of evidence that require conducting of various investigative measures. To make the judicial cooperation and so the investigation effective, the replies concerning electronic evidence have to be provided as soon as possible, with that meaning not even days, but hours.

Legal instruments should therefore provide for a timely response for emergency requests as well as shorter response periods for other type of requests.

Languages

The accepted languages depend mostly on the rules of the legal instrument applicable. For example, some countries accept broader scope of languages with the Council of Europe conventions (Austria, Bulgaria, the Netherlands, Slovakia) than when working with EIO.

Along with official language(s) of the Member States, English has been considered the most common language authorities may accept requests in urgent cases. France for instance has indicated that requests addressed to the 24/7 Network, are accepted in English and French, but requests for legal assistance shall be translated in French[56].

Translations are costly and demand additional time. Additionally, the specific legal terms are not always well interpreted and might cause delays and need for clarification. Practitioners have required in several occasions to extend the language regime particularly to English, which is widely used in the practice for judicial cooperation and OSPs.

The role of main actors for judicial cooperation

EU instruments should also consider and include where relevant, the roles and support that the European Judicial Network, Eurojust and the European Judicial Cybercrime Network could provide to practitioners in order to ensure that the requests are effective.

In line with the survey conducted with judicial authorities for the purpose of this report and the experience shared with the EJN, practitioners need further guidance and training for requesting e-Evidence as the specific procedures mentioned above are of technical and complex nature.

THE PERSPECTIVE OF ONLINE SERVICE PROVIDERS

A. The impact of the COVID-19 pandemic on Online Service Providers in the electronic evidence field

The SIRIUS team engaged with representatives from Airbnb, Facebook, Google, Microsoft, Snap, TikTok, Twitter, Uber, Verizon Media and WhatsApp to discuss the impacts of the COVID-19 pandemic to the electronic evidence process from their perspective, among other topics. In those opportunities, it became clear that the pandemic affected OSPs in different ways. For instance, the majority of OSPs reported challenges and difficulties that led to temporary backlogs, required changes in existing processes and also largely impacted staff. Moreover, most OSPs stated that they acted with flexibility and were able to quickly adapt to ensure business continuity in processing requests from authorities issued in the context of criminal investigations. Overall, the main impacts to the electronic evidence process from the perspective of OSPs happened in three areas: staff, security of information and cooperation with authorities.

First, the health of staff and impact on their work remained one of the main concerns for OSPs in 2020. Some acknowledged during the interviews the challenges in the balance between personal and professional lives, impacts on mental health and in some cases difficulties in maintaining the same productivity level. The Law Enforcement Response Teams were facing difficulties with on-boarding process, training and integrating new staff virtually, without the possibility to meet in person.

Second, the security of information and systems was also a topic of concern. Many OSPs mentioned that they had to create and implement new security protocols and controls in order to allow their employees to have access to sensitive user data outside of offices premises, so they could continue to process official requests for data disclosure. New processes had to be put in place in order to ensure digitalization of all the steps. For instance, OSPs that accepted legal documents served in paper copy had to review their processes and the disclosure of business records in hardware or printed material also had to be modified.
Finally, the cooperation with authorities changed in 2020, as teams leading outreach efforts faced difficulties in turning all their activities online. These teams work to ensure streamlined communication and to train authorities in their specific processes. Because of the pandemic,

several conferences, events and meetings that promoted opportunities for training and networking were cancelled. After having to change outreach activities, some OSPs mentioned it used to be much easier to build trust and ensure dissemination of relevant information face-to-face rather than via timed online conversations. At the same time, OSPs also described higher willingness from authorities to follow more digitalised processes with a large focus on the use of Law Enforcement Portals for channelling requests. This shift to a preference for Portals as submission channels is backed by results presented previously in the chapter on the Perspective of Law Enforcement: for the first time, the use of online portals dedicated to law enforcement became the preferred method, scoring higher than e-mail in 2020.

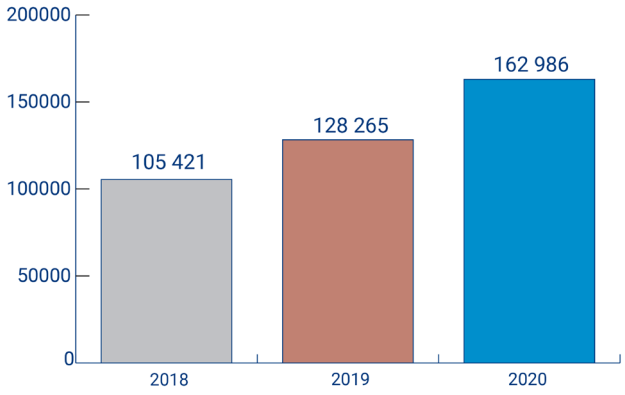
B. Volume of data requests per country and per Online Service Provider

Currently, at EU level, there is no comprehensive statistical data regarding requests from authorities to OSPs for disclosure of user data, in the context of criminal investigations. Transparency Reports published by OSPs provide a reliable source of information since many of them offer a detailed overview, including data per requesting country and type of request. However, this methodology has limitations, since it only represents a fraction of the total amount of requests. For instance, not all OSPs publish Transparency Reports or include detailed and homogeneous information about EU requests. Moreover, in situations when requesters followed an MLA procedure, it may not be possible for the OSP to identify the country that originated the request. Therefore, data presented in Transparency Reports is likely to reflect mainly direct requests from authorities to foreign-based OSPs.

The data in the analysis below includes information collected from Transparency Reports of Airbnb, Facebook, Google, Microsoft, Snap, TikTok, Twitter and Verizon Media. Note that Apple has not been included in the analysis, as in previous years, because the company had not yet published data for the second semester of 2020 by the time of creation of this report.

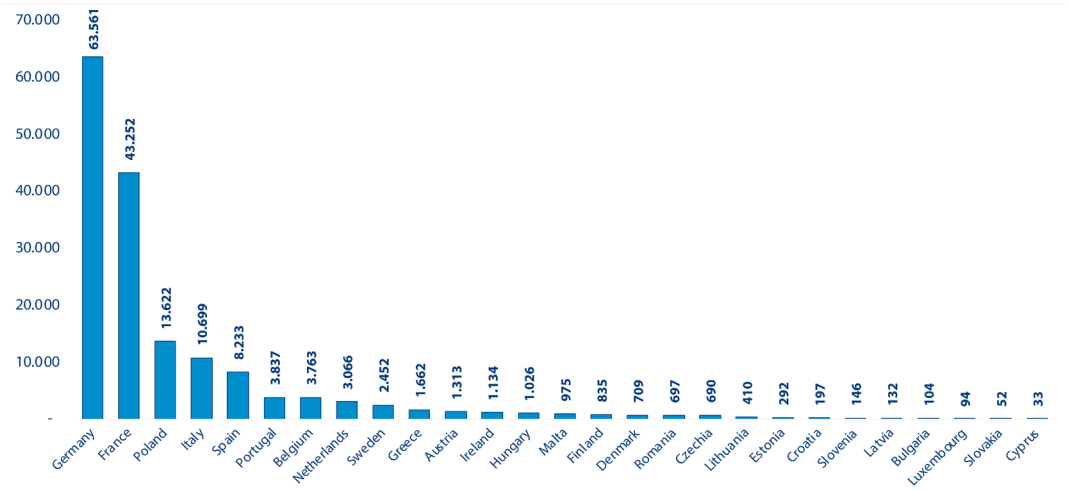
From 2019 to 2020, the volume of requests for user data submitted by authorities increased by 27.1% in the EU, to over 162.000 requests to the eight OSPs listed above. This result demonstrates how the relevance of electronic evidence continues to increase at a high pace in criminal investigations conducted in the EU, as the increase is even higher than the 21.7% variation from 2018 to 2019.

EU data requests to a number of Online Service Providers from 2018 to 2020



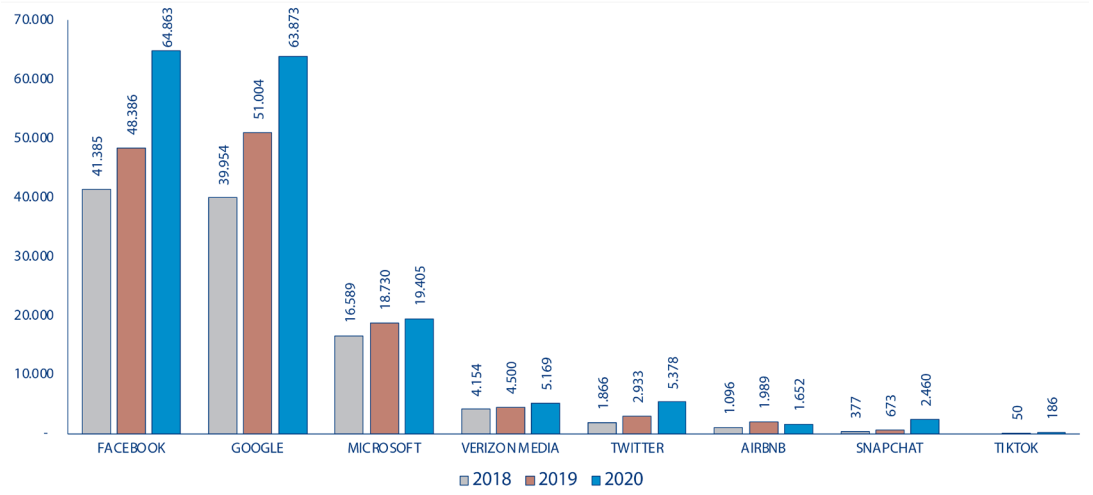
In 2020, 65.5% of the total requests in the EU were submitted by Germany and France. It is worth noting that some Member States observed a sharp increase in their volume when compared to the previous year. Ireland, for example, had 157% increase in the volume of requests submitted, while Malta had 99.4% and Denmark 73.8% more requests in 2020. Note that Ireland is the country where seven out of eight companies analysed are based in the EU. For that reason, the increase of requests from this country could have been directly impacted by the number of MLA requests originated in other countries, given that OSPs established in Ireland would receive MLA processes in the form of requests coming from Irish domestic authorities. In the opposite trend, Luxembourg had a decrease of -61.9% of requests, the largest drop among all 27 Member States.

EU data requests to a number of Online Service Providers in 2020, per Member State



Among the eight OSPs analysed, Facebook and Google received 79.0% of all the requests. Snapchat and TikTok had the highest variation rate from 2019 to 2020, while Airbnb was the only OSP that saw a decrease in the number of requests in 2020[57].

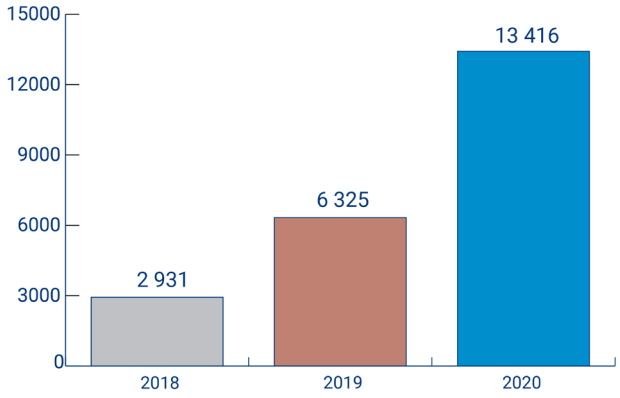
EU data requests to a number of Online Service Providers from 2018 to 2020, per company



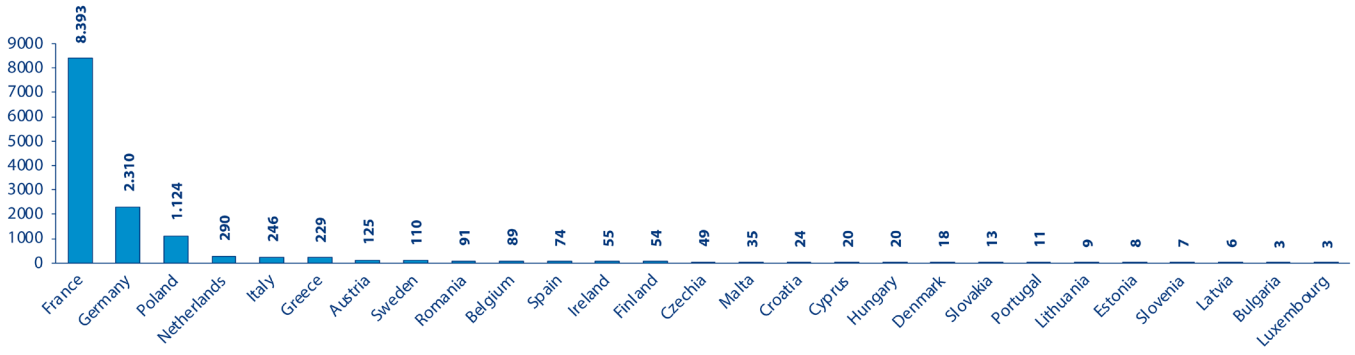
Emergency Disclosure Requests

The volume of EDRs submitted from EU authorities has had an expressive increase of 112.1%, from 2019 to 2020. The increase is specifically driven by EDRs submitted by France to Facebook, which accounted for 58.1% of all the EDRs submitted in 2020 to the eight OSPs analysed. Note that Facebook has a very restrictive definition of "emergency" which is limited to a "matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay"[58]. Overall, France submitted 62.6% of all EDR and Germany submitted 17.2%.

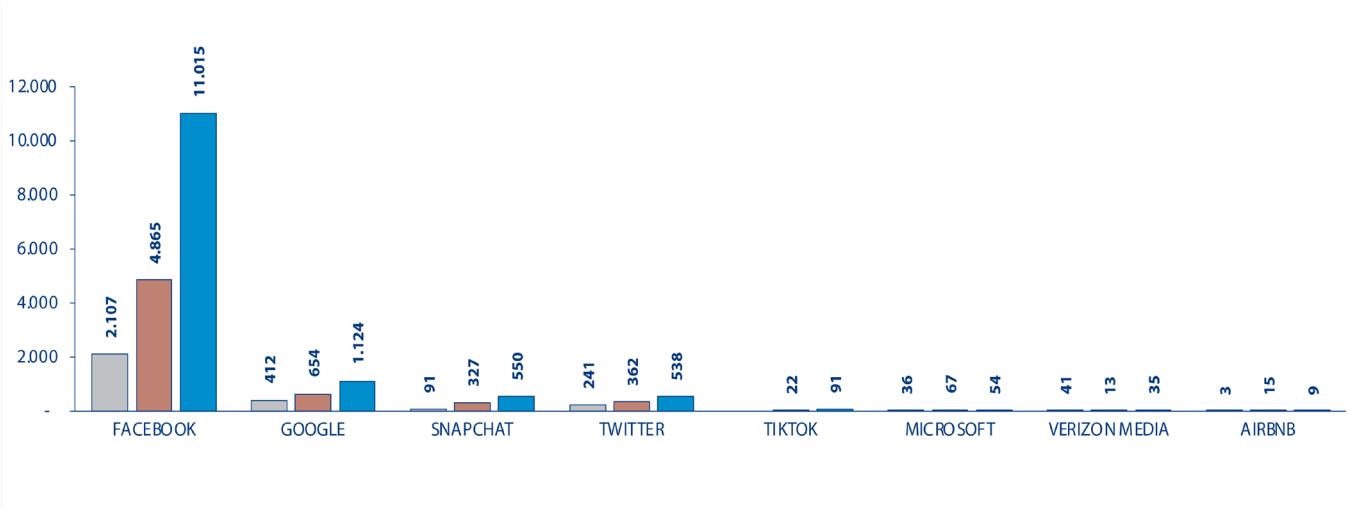
EU Emergency Disclosure Requests to a number of Online Service Providers from 2018 to 2020



EU emergency disclosure requests to a number of Online Service Providers in 2020, per Member State



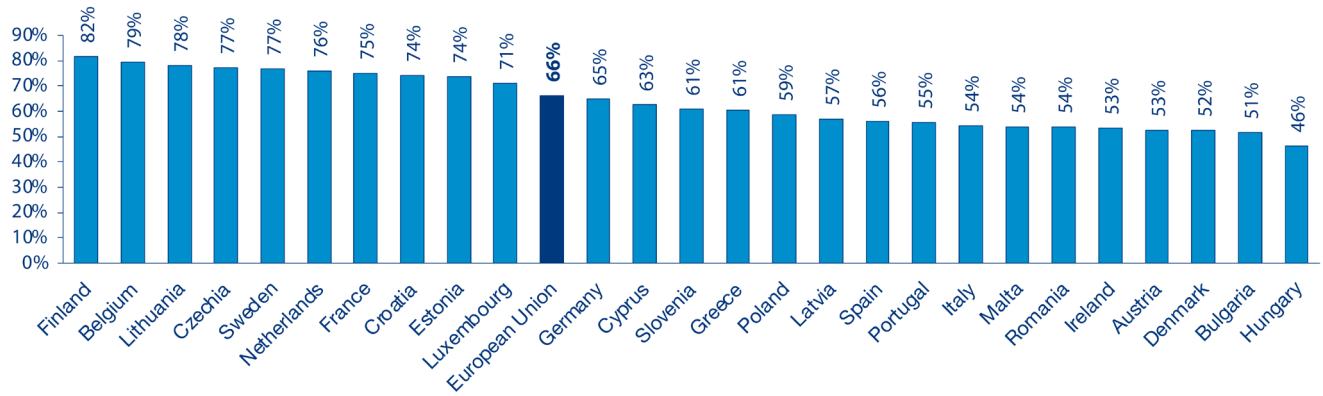
EU emergency disclosure requests to a number of Online Service Providers from 2018 to 2020, per company



C. Success rate of EU cross-border requests for electronic evidencer

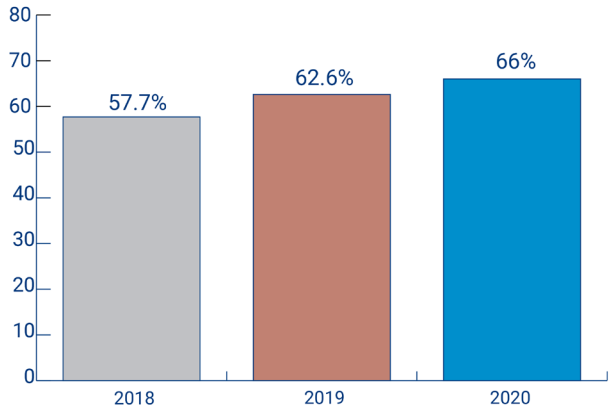
Not all the requests for user data submitted from authorities to OSPs in the context of criminal investigations are successful. Section E. of this chapter lays down the main reasons for refusal in processing direct requests for voluntary cooperation. Data from the Transparency Reports analysed[59] demonstrate that the average success rate in the EU increased from 62.6% in 2019 to 66.0% in 2020. The countries with best success rate are Finland (82%), Belgium (79%) and Lithuania (78%).

Success rate of EU data requests to a number of Online Service Providers in 2020

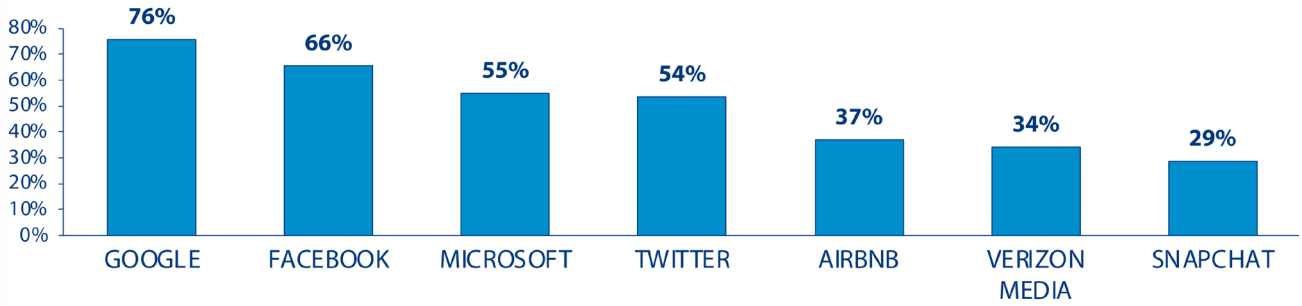


76% of requests submitted by EU authorities to Google were successful in 2020, while that rate is of 66% for Facebook. The lowest success rates are reported by Verizon Media (34%) and Snapchat (29%), two OSPs that do not accept requests under voluntary cooperation in non-emergency circumstances issued by most Member States.

Average EU Success Rate of Requests to a number of Online Service Providers from 2018 to 2020

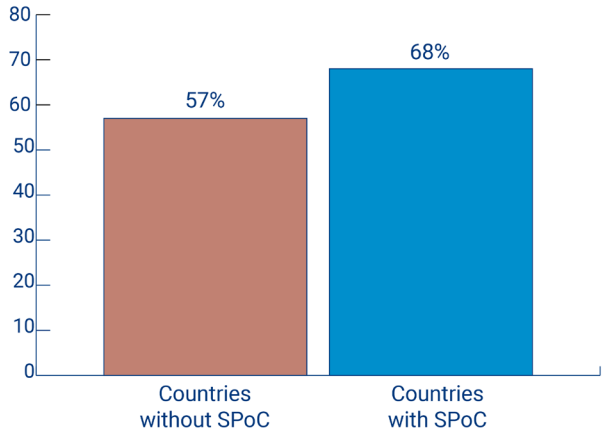


Success rate of EU data requests to a number of Online Service Providers in 2020



When comparing the average success rate for countries with or without SPoCs, it becomes clear that the establishment of such units has a positive impact on the outcome of requests. The average success rate of the 15 Member States where SPoCs have been established (Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Ireland, Latvia, Lithuania, Malta, Netherlands, Slovakia, Spain and Sweden) was 68%, compared to 57% of the other Member States, in 2020.

Average success rate of countries with or without an established SPoC for centralisation of requests in 2020



D. The experience of Online Service Providers with Single Points of Contact

The *SIRIUS EU Digital Evidence Situation Report 2020* included a complete overview of types of SPoCs, the tasks they perform and how they operate in the EU. In that report, SPoCs for centralization of requests are defined as designated persons, units or institutions who centralize, review and submit requests from governmental authorities to OSPs. These SPoCs are responsible for dealing with requests and receiving responses, acting as a reference point in relation to electronic evidence and engagement with national and foreign OSPs.

All ten companies interviewed by the SIRIUS team in 2021 were unanimous in one point: the establishment of SPoCs for centralization of law enforcement requests is highly beneficial to the overall process. The approach taken by OSPs in relation to SPoC varies, as some of them established a type of exclusive cooperation, meaning that OSPs will always ask all officers who submit requests to them in a specific country to follow the process via the SPoC. Others, will still accept requests from officers who are not part of that unit. Furthermore, how formal a SPoC unit is varies depending on the Member State and the law enforcement agency. Some have established formal units, while in other cases certain officers or other existing units were designated to act as SPoCs.

Despite the differences in the process, the benefits mentioned by OSPs in relation to the SPoC approach were:

- The establishment of a SPoC process contributes to increased quality of requests and, in consequence, leads to a decrease in response time. Because officers who are part of SPoC units are specialized in electronic evidence, they have, for example, a very good understanding of the requirements, the type of information that must be included in requests and the datasets that may be disclosed. Additionally, some OSPs mentioned that the rejection rate of requests submitted by SPoCs is considerably lower when compared to the national average;

- SPoCs make it possible to establish streamlined communication in emergency circumstances, ensuring faster processing of information;

- Updates, feedback and training material can be disseminated through a single channel, and questions from the regional units can be centralised and routed

through the SPoC. This ensures that all law enforcement community benefits from the provided information;

- Establishing SPoCs help to minimize duplication of requests regarding the same case from different units or even law enforcement agencies;

- SPoCs are efficient tools to build greater cooperation between OSPs and law enforcement agencies.

In the EU, 20 law enforcement agencies in 15 Member States have established formal units to act as *SPoC for centralization of requests*: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Ireland, Latvia, Lithuania, Malta, Netherlands, Slovakia, Spain and Sweden. Taking into account the benefits and the positive feedback reported by the OSPs, representatives from these 20 agencies are part of the **SIRIUS SPoC Network**.

This is an initiative of the SIRIUS Project to facilitate the exchange of information and best practices among these agencies and contribute to continuous capacity building of officers in the field of electronic evidence.

The Network has a restricted and secured environment within the *Europol Platform for Experts* and also has the opportunity to participate in dedicated annual events with the participation of international organizations and OSPs.

E. Reasons for refusal or delay in processing direct requests for voluntary cooperation issued by EU authorities

The section c in this chapter presents the success rate of requests in 2020, demonstrating 34% of them have been rejected in 2020 in the EU, according to the transparency reports of OSPs analysed. While this is an important figure, it does not account for those requests that had their responses delayed due to issues in the original document. When OSPs ask for supplementary information or for other changes in requests, there might be longer delays involved in the disclosure of the required records, which may have important impact in investigations. Unfortunately, there is no comprehensive statistical information available in relation to average response time or number of requests that have been impacted by such delays.

The SIRIUS Project team has collected information on the main reasons for refusal or delays in processing requests for electronic evidence during interviews conducted with ten OSPs. The issues included in this section are those that have been indicated by at least 30% of the interviewed OSPs, as shown in the Table 15. All the issues included in the table are further analysed below.

Table 15 - Main reasons for refusal or delay of direct requests according to OSPs

Reason for refusal or delay in processing direct requests for voluntary cooperation issued by EU authorities	Percentage of OSPs who mentioned this issue
Legal basis absent or incorrect	60%
Wrong legal entity addressed	60%
Procedural mistakes according to OSPs requirements	50%
Overly broad	30%
No data available	30%
Not enough information about the nature of the case	30%
Territorial limitations	30%
Lack of valid identifiers	30%
Not enough information to justify "Emergency" criteria	30%

1. Legal basis absent or incorrect

OSPs that accept data disclosure requests issued by foreign authorities often require that requests include the legal basis under the domestic regulations of the requesting country. For instance, *Apple's Legal Process Guidelines* state that "[…] *it is necessary for the requesting officer to indicate the legal basis which authorises the collection of evidential information in the form of personal data by a law enforcement agency from a Data Controller* […]"[60]. 60% of companies interviewed by the SIRIUS project team in 2021 indicate this, if not properly fulfilled, as one of the main reasons for refusal or delay in processing direct requests.

According to OSPs, requesters may misinterpret this requirement and quote legislation relating to the crime being investigated, instead of the regulation that authorises them to collect data from private entities in criminal investigations. In other situations, requests might include reference to legal basis that is not considered appropriate by the OSPs. In these cases, OSPs may reach out to the requesting authority to inform that the request does not include what they consider as a reference to a valid legal basis, however without informing what would be considered acceptable.

2. Wrong legal entity addressed

60% of interviewed OSPs indicate that one of the main issues in direct requests is the fact that it is addressed to the wrong legal entity. There are three situations that lead to such issue:

- **Requests are addressed to the subsidiary of the parent company, that is not a data controller**: because many OSPs have offices in several countries, there might be misunderstandings on which of them are data controllers in relation to what type of data.

- **The data associated to a targeted account is controlled by a different legal entity**: many OSPs have more than one legal entity acting as a data controller and which one is responsible for data of a specific user may not always be obvious. Users resident in different jurisdictions - or those that set up their accounts while being temporarily in different jurisdictions - may have their data controlled by different legal entities. In many cases, only

the OSP will be in position to state which legal entity is acting as a data controller for one specific user.

- **Requests are addressed to other OSPs entirely**: because many investigations involve requests to more than one OSP, mistakes may happen while sending out the correct requests to the companies.

3. Procedural issues according to OSPs requirements

Procedural issues were indicated by 50% of interviewed OSPs in 2021 as one of the main reasons for refusal or delay in processing direct requests. Because requirements vary depending on the company, the issues are not the same for all of them. Some OSPs report they push back on requests that lack issuing date or manual signature of the requester, while others may require that the documents contain letterhead of the requesting authority including the name of the institution, contact details and physical address.

4. Overly broad request

Requests that are not specific in the timeframe and datasets that are sought or that otherwise result in a potentially large amount of responsive data may be considered as overly broad by the companies and therefore not processed.

5. No data available

It is not rare that requests are rejected because no data is available, which is indicated as one of the main issues to 30% of interviewed OSPs. This may happen for several reasons:

- The user deleted the relevant data;

- The OSP deleted the data as part of an automated process. For instance, some companies may automatically delete IP addresses or connection logs after a specific period;

- The request contains wrong identifiers. For example, a spelling mistake in the request may lead the company to respond that there is no data related to that identifier.

6. Not enough information about the nature of the case

OSPs acknowledge that criminal investigations contain sensitive information, which must be kept confidential by authorities. However, because direct request are processed also in accordance with the policies established by the OSPs themselves, most OSPs require information about the nature of the case and the context that justifies the need for data disclosure. Such information is requested as companies feel obliged to evaluate the necessity and proportionality of requests. Furthermore, OSPs also require this information to identify if requests are indeed targeted to the data requested or are simply sent to several companies for authorities to check if any of them have any information (this type of request is known as “fishing expedition”).

30% of OSPs report in 2021 that the lack of information about the nature of the case as one of the main issues leading to delays and rejection in processing requests. These OSPs state that it is common that they have to reach out to the requesters and ask for additional information, which often leads to delays in processing requests and may even result in the rejection of the request when such information is not provided in a timely manner.

7. Territorial limitations

30% of OSPs reported that one of the main issues for refusal or delay in the process relates to requests for data about users in a different country than the requesting one. For example, when an authority in Country A requests data about a user residing in Country B, the OSP may refuse the request or ask for additional context, even if the legal entity addressed is a data controller for personal data of the residents/citizens of both countries.

Some OSPs may restrict the voluntary cooperation process to only disclose data relating to the same country, others may accept this type of requests if properly justified. For instance, in case the user from Country B was in the Country A at the moment of the crime, then OSPs may consider the disclosure of the data.

Note that in order to establish the territorial connection of users, policies vary among OSPs; for example, such a criterion could be the IP address at the moment of registration, the IP address for connection in a recent period of time, billing address, language or territorial preference chosen.

8. Lack of valid identifiers

Valid identifiers are datasets that allow OSPs to locate a specific account. They are generally unique information linked to one individual user, such as e-mail address, phone number, username or user ID, for example. However, the way online platforms operate varies a lot and understanding what is considered a valid identifier is not always simple. For instance, some platforms may allow users to change their username at any time or do not require those to be unique. Moreover, platforms often use terms such as ‘display name’, ‘vanity name’, ‘handle’, ‘user name’ and ‘user ID’ in different ways. While platforms are constantly evolving and new ones are frequently emerging, and considering over 40% of officers report never having received specific training, ensuring a clear understanding of the use of identifiers can be challenging. As a result, 30% of OSPs reported the lack of valid identifiers as one of the main reasons for refusal or delay in processing data disclosure requests.

9. Not enough information to justify an "emergency"

OSPs may set their own requirements for EDR for foreign-based authorities seeking data under voluntary cooperation, in the context of criminal investigations. Definitions, standards and requirements may vary from company to company, depending on the applicable

legislations in the jurisdiction where they are based, as well as specificities of each platform.

The majority of OSPs require EDRs to include enough context regarding the situation involving imminent threat to life or serious physical injury to a person. However, some OSPs may adopt a wider definition of "emergency", including crimes against minors, threats to critical infrastructure or matters of national security. When it comes to the requirements for EDRs, some may only need basic information about the nature of the case, while others may ask for detailed information about the situation and justification of how the data sought will be used in the investigation.

In this context, for 30% of interviewed OSPs, the lack of sufficient information to justify the emergency is one of the main reasons for refusal or delay in processing requests for electronic evidence.

F. Existing and future challenges from the perspective of Online Service Providers

Some OSPs reported that there have been considerable improvements in the process of request and disclosure of electronic evidence in recent years, as there is more and more awareness among requesting authorities regarding applicable requirements and regulations, as well as more established procedures within OSPs to process requests in the context of criminal investigations. Nevertheless, specific challenges remain, other than those related specifically to the pandemic as described in section a of this chapter. In addition, OSPs were also asked to indicate what they believe will be the future challenges in relation to electronic evidence in the years to come. The challenges reported by some of the OSPs are listed below.

Existing challenges in the electronic evidence field:

- Because of the global reach of certain OSPs, disseminating information and updates to law enforcement authorities worldwide on procedures and requirements is very challenging.

- Some OSPs also express concern with the security of the transmission of data to law enforcement in response to electronic evidence requests. They see potential for criminals to target law enforcement systems and obtain access to law enforcement e-mail accounts, indicating the need for authorities to invest in cybersecurity.

- The use of electronic signatures is a challenge, since there are no common standards at international level. As a result, it may not always be possible to confirm the authenticity of e-signatures.

Future perspectives in the electronic evidence field:

- The volume of requests from authorities for the disclosure of data in the context of criminal investigations is increasing. This might prove challenging as OSPs see the

necessity to continuously increase the resources to ensure the capacity to meet the needs.

- Several OSPs interviewed for this report mentioned that they welcome the policy-making initiatives in the area of electronic evidence. Specifically in relation to the 'E-evidence package' proposed by the European Commission, some OSPs mentioned that they do not see specific issues in relation to the deadline of 6 hours for response in emergencies included in the European Commission's proposal, as this is already possible in the majority of the cases. However, some mentioned that the deadline of 10 days for non-emergencies would require large adaptation and there would be the need for additional technical and/or human resources.

RECOMMENDATIONS

Given the pace at which the amount of requests for electronic evidence is increasing in the context of criminal investigations, as demonstrated in this Report,the EU is currently taking steps to enhance the legal framework for cross-border access to electronic evidence. However, the outcome and the legal implications of a variety of policy based initiatives, such as the EU-legislative procedure, international negotiations for the Second Additional Protocol to the Budapest Convention, and an EU-US agreement will be witnessed in the future. In the short term, this section proposes recommendations to law enforcement, judicial authorities and OSPs that can have a more immediate positive impact to the effectiveness of ongoing and future criminal investigations and prosecutions.

A. For European Union Law Enforcement Agencies

- ***Use Standardised Model Forms for data preservation and disclosure requests under voluntary cooperation***

Many of the main reasons for refusal or delay in processing direct requests for electronic evidence analysed in this report could be avoided at the drafting phase. Because of this, the SIRIUS project has partnered with international organisations for the creation of Standardised Model Forms for preservation and disclosure of data.

The Standardise Model Forms are meant to be used by law enforcement and judicial authorities in the context of criminal investigations, in compliance with applicable legislations, and have been carefully designed to facilitate the drafting process with clear and objective guidance.

The forms were created by the SIRIUS project together with the United Nations Office on Drugs and Crime (UNODC), the United Nations Counter-Terrorism Committee Executive Directorate (UN CTED), as well as the European Judicial Network (EJN) and CEPOL, taking into account input coming from international institutions, authorities worldwide and the private sector. Authorities can download the Model Forms on the **restricted SIRIUS platform**. Law enforcement officers and judicial authorities can find more information about how to register on SIRIUS at **https://www.europol.europa.eu/sirius**.

- ***In law enforcement agencies where not yet established, create Single Points of Contact for electronic evidence requests to OSPs under voluntary cooperation***

The digital environment is constantly evolving and changes are frequent both in the way platforms are abused by criminals and in the way OSPs operate. The establishment of

SPoCs for centralization of requests or for knowledge-sharing can largely contribute to enhanced capacity in dealing with electronic evidence, also leading to more effective and faster investigations. This is the same recommendation included in the previous report, given the growing relevance of SPoCs, as reported also this year by OSPs and law enforcement authorities. In the EU, 15 Member States have established SPoC units.

Established SPoCs are invited to join the restricted SIRIUS SPoC Network page, which aims at facilitating the exchange of best practices among these specialized units. For more information contact the SIRIUS Team at Europol via e-mail to **sirius@europol.europa.eu**.

B. For European Union Judicial Agencies

- ***Stimulate national capacity building initiatives on the available instruments and processes to request and obtain electronic data from other jurisdictions***

Having regard to the diversity of national legal frameworks, different approaches to acquisition of electronic data, policy developments at national and international level and the relentlessly evolving digital landscape, which significantly is and will continue to impact all spheres of EU citizens' lives, it is fundamental for the EU judicial community to have capacity to properly identify and rely on investigative and prosecutorial solutions that match specific needs. As indicated by the direct feedback received for this report, the judicial authorities often referred to the absence of legal clarity in their respective national legislations as well as difficulty in identifying correct methods and channels to request and obtain data disclosure. Therefore, in such a fast-evolving technological, legal and policy landscape, investing in the constant capacity building of EU judicial authorities would substantially contribute to filling the gaps and to increasing their efficiency and effectiveness.

In this regard, the EU judicial authorities are encouraged to reach out to the SIRIUS team at Eurojust via e-mail to **sirius.eurojust@eurojust.europa.eu**, indicating their specific training needs in the field of the electronic evidence. Adhering to those needs, the SIRIUS team will dedicate its efforts to support the practitioners with the tailor- made capacity building activities.

- ***Enhance the interconnection, know-how and expertise exchange among EU judicial practitioners in the field of electronic evidence***

Acknowledging that in the field of electronic evidence, the EU judicial practitioners have to perform their functions in an increasingly global society in which international judicial cooperation as well as direct interaction with private sector are essential, it is of paramount importance to promote exchanges among judges and judicial authorities. Enhancing

interconnection as well as fostering exchange of knowledge and expertise including other relevant actors in the field of electronic evidence, would provide necessary know-how, expand understanding on legal systems of other countries as well as legal processes for cross-border data disclosure followed by private entities and strengthen mutual confidence at the benefit of all involved stakeholders.

In this regard, the SIRIUS restricted platform offers concrete means to the daily efforts of EU judicial authorities as well as promotes knowledge exchange via its dedicated forums. Striving to better adhere to the needs of the practitioners to be timely informed about the developments in the field of electronic evidence as well as updated about different expertise and angles from which electronic evidence can be approached, the EU judicial authorities are encouraged to provide an official contact point to the SIRIUS team at Eurojust via e-mail to **sirius.eurojust@eurojust.europa.eu** to enhance the outreach of the practitioners. Noting that some of the member states have established cybercrime networks, the judicial authorities are suggested to designate a contact point from such respective networks.

C. For Online Service Providers

- ***Disseminate updates about policies and changes in processes to EU authorities also through SIRIUS***

The SIRIUS platform is designed to securely facilitate knowledge sharing in relation to cross-border access to electronic evidence amongst law enforcement and judicial authorities in the EU. Therefore, SIRIUS can play a key role in complementing the dissemination strategy of relevant information, leading to improved quality of request and avoiding unnecessary inquiries. Ultimately, this can contribute to faster and more effective data disclosure requests in criminal cases.

This is the same recommendation as in the previous report, since OSPs stated this year that disseminating updates and information to authorities remains one of their main challenges. OSPs may contact the SIRIUS Team at Europol via e-mail to **sirius@europol.europa.eu**.

- ***For small and medium OSPs that do not have yet established processes for engagement with law enforcement in the context of criminal investigations: join the SIRIUS Programme for OSPs***

SIRIUS has a structured programme dedicated to OSPs, mainly small and medium OSPs that do not have law enforcement response policies in place. The participation of OSPs takes place on a voluntary basis and the aim of the programme is to share relevant knowledge in relation to cross-border access to electronic evidence, in the context of criminal investigations. The

programme includes guidelines, templates and model forms, as well as meetings that are organised annually.

- ***For OSPs that already have established processes for engagement with law enforcement in the context of criminal investigations: take into account the perspectives of law enforcement and judicial authorities presented in this report when updating policies***

This report is based on information coming from EU authorities in all Member States, and presents the main issues encountered and the main challenges they face. We recommend considering this information when updating processes for disclosure of data in criminal investigations, with a view to render the process faster and more effective. For instance, clearly informing requesters about the reasons for refusal of requests or the partial disclosure of data may lead to higher quality requests in the future. Moreover, the focus on outreach activities towards authorities and engagement with existing SPoCs can facilitate the dissemination of information about processes and streamline communication in emergencies.

ENDNOTES

1 https://www.europol.europa.eu/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations

2 Extensive analysis of the impact of COVID-19, during and after its initial phase, in terms of crime areas and response from EU competent authorities is available on Eurojust's and Europol's websites. Some specific examples: "EXPLOITING ISOLATION: Offenders and victims of online child sexual abuse during the COVID-19 pandemic" (Europol, 19 Jun 2020); "How COVID-19-related crime infected Europe during 2020" (Europol, 11 Nov 2020); "The Impact of COVID-19 on Judicial Cooperation in Criminal Matters, Eurojust, Analysis of Eurojust Casework" (Eurojust, 17 May 2021).

3 Joint Report, "The impact of COVID-19 on judicial cooperation in criminal matters - Executive summary of information compiled by Eurojust and EJN", Council of the European Union, 16 July 2021; "The Impact of COVID-19 on Judicial Cooperation in Criminal Matters, Eurojust, Analysis of Eurojust Casework" Eurojust, 17 May 2021

4 Consisting of a Proposal for a Regulation of the European Parliament and the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD) and a Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD).

5 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

6 https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html

7 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

8 https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/

9 La Quadrature du Net and Others (Judgement of 6 October 2020 in Joined Cases C-511/18, C-512/18 and C-520/18) and Prokuratuur (Judgement of 2 October 2018 in Case C-207/16).

10 Report, "Cybercrime Judicial Monitor - Issue 6", Eurojust, May 2021

11 https://www.coe.int/en/web/portal/-/cybercrime-council-of-europe-strengthens-its-legal-arsenal

12 Automattic reported 19 requests from EU authorities in 2020, Cloudflare 9, Dropbox 28 and Reddit 56. Because these OSPs reported less than 100 requests in 2020, they have not been included in the analysis and graphs in this Report.

13 Austria, Belgium, Bulgaria, Croatia, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain and Sweden.

14 In general, textual feedbacks featuring this report were edited to ensure clarity, conceal sensitive data, or translated from different EU languages into English.

15 Report, "European Union Serious and Organised Crime Threat Assessment", Europol 12 April 2021 and Report, "How COVID-19-related crime infected Europe during 2020", Europol, 11 Nov 2020

16 Report, "EXPLOITING ISOLATION: Offenders and victims of online child sexual abuse during the COVID-19 pandemic", Europol, 19 Jun 2020

17 Including, for example, Airbnb, Facebook, Google, Microsoft, PayPal, Twitter, Uber and WhatsApp, among others.

18 SPoCs for centralization of requests are designated persons, units or institutions who centralize, review and submit requests (mostly those issued under voluntary cooperation) from governmental authorities to OSPs.

19 The Impact of COVID-19 on Judicial Cooperation in Criminal Matters, Analysis of Eurojust Casework, May 2021, available at: https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/2021_05_12_covid_19_report.pd

20 Indicated by the respondents of the survey

21 In general, textual feedbacks featuring this report were edited to ensure clarity, conceal sensitive data, or translated from different EU languages into English.

22 More information on the effects of COVID-19 pandemic on judicial cooperation is available at: The Impact of COVID-19 on Judicial Cooperation in Criminal Matters , Compilation of Replies - https://www.ejn-crimjust.europa.eu/ejn/EJN_RegistryDoc/EN/3223/108/0

23 It is worth noting however that the the Budapest Convention on Cybercrime refers to this category of data as "Subscriber information".

24 https://www.eurojust.europa.eu/sirius-eu-digital-evidence-situation-report

25 Including their provided services i.e. the mentioned options of Gmail and YouTube attributed to Google; Instagram and WhatsApp attributed to Facebook and Skype attributed to Microsoft.

26 Article 18 – Production order.

27 T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention) of 1 March 2017, available at www.coe.int.

28 http://www.irishstatutebook.ie/eli/2008/act/7/enacted/en/print.html

29 Code of Criminal procedure, https://www.legislationline.org/download/id/8697/file/Code_Criminal_Procedure_2003_am2020_en.pdf, Passed on 12 February 2003

30 Article 32 – Trans-border access to stored computer data with consent or where publicly available.

31 Internet & Jurisdiction Policy Network, We need to talk about data, https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf, 2021

32 La Quadrature du Net e.a. C-511/18, C-512/18 and C-520/18 of 6 October 2020

33 Privacy International C-623/17 of 6 October 2020

34 H.K. v Prokuratuur C-746/18 of 2 March 2021

35 https://www.eurojust.europa.eu/cybercrime-judicial-monitor-issue-6

36 https://www.eurojust.europa.eu/cybercrime-judicial-monitor-issue-6

37 https://www.eurojust.europa.eu/cybercrime-judicial-monitor-issue-6

38 In relation to U.S.-based OSPs, this is regulated by 18 U.S.C. §2706.

39 EU Commission's Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal

matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (SWD/2018/118 final), p. 282.

40 A useful selection of insightful analysis on the topic of encryption comes from: https://www.eurojust.europa.eu/third-report-observatory-function-encryption, https://www.europol.europa.eu/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

41 https://www.eurojust.europa.eu/observatory-report-encryption-presents-latest-developments-practitioners

42 As an example: "MI5 chief asks tech firms for 'exceptional access' to encrypted messages", The Guardian, 25 February 2020.

43 https://www.eurojust.europa.eu/observatory-report-encryption-presents-latest-developments-practitioners

44 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1.

45 Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 1.

46 Denmark and Ireland. See the Table on the Status of Implementation for the EIO Directive for additional information in the EJN website.

47 Article 18(1.b) Convention on Cybercrime of the Council of Europe (CETS No.185)

48 "Member States shall take the necessary measures to comply with this Directive by 22 May 2017", Article 36.1, Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1.

49 See Council document WK 13576 2018 INIT of 9 November 2018, "Conclusions of the EJN e-Evidence Working Group on the proposals for a Production and Preservation Order and Appointment of a legal representative" LIMITE and Council document 6649/19 of 22 February 2019, "Annexes to the Proposal for a Regulation on European Production and reservation Orders for electronic evidence in criminal matters - conclusions of the 2nd meeting of the EJN e-Evidence Working Group - comments on Annexes I-III", LIMITE.

50 53rd Plenary Meeting of the European Judicial Network under the Finnish Presidency 20-22 November 2019 and 56th Plenary Meeting of the European Judicial Network under the Portuguese Presidency 29 June 2021

51 See Chapter 'Perspective of Judicial Authorities', section c. 'Cross-border requests and data disclosure', subsection 'Principle of admissibility'

52 See Chapter 'Perspective of Judicial Authorities', section d. 'Challenges to EU judicial authorities', subsection 'The data retention regime'

53 According to the information provided by the Member States for the Fiches Belges on e-evidence - https://www.ejnforum.eu/cp/e-evidence-fiche/223/0

54 See Chapter 'Perspective of Judicial Authorities', section d. 'Challenges to EU judicial authorities'

55 Discussions during the 53rd and 56th Plenary Meetings of the European Judicial Network

56 Information provided in the EJN Fiches Belges for e-Evidence, EJN | e-Evidence Fiche Belge (ejnforum.eu)

57 Note that TikTok has no public data available regarding disclosure requests from governmental authorities received before 2019

58 https://www.facebook.com/safety/groups/law/guidelines/

59 TikTok has not been included in the analysis regarding Success Rate, because the company only publishes aggregated data for "Percentage of legal requests where data was produced" that includes "Legal Requests" and "Emergencies". Therefore, it is not possible to calculate the success rate only of non-emergency requests.

60 https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf

REFERENCES

All links were accessed in September 2021.

- Airbnb, Airbnb Law Enforcement Transparency Reports, https://www.airbnbcitizen.com/transparency
- Automattic, Transparency Report, https://transparency.automattic.com/
- Cloudflare, Transparency Report, https://www.cloudflare.com/transparency/
- Dropbox, Transparency Overview, https://www.dropbox.com/transparency
- Facebook, Government Requests for User Data, https://transparency.facebook.com/government-data-requests
- Google, Google Transparency Report, https://transparencyreport.google.com/
- LinkedIn, Government Requests Report, https://about.linkedin.com/transparency/government-requests-report
- Microsoft, Law Enforcement Requests Report, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
- Reddit, Transparency Report 2020, https://www.redditinc.com/policies/transparency-report-2020-1
- Snap Inc., Transparency Report, https://www.snap.com/en-US/privacy/transparency/
- TikTok, Transparency Report, https://www.tiktok.com/safety/resources/transparency-report
- Twitter, Information requests, https://transparency.twitter.com/en/information-requests.html
- Verizon Media, Government Data Requests, https://www.verizonmedia.com/transparency/reports/government-data-requests.html

ACRONYMS

- CSAM: Child Sexual Abuse Material
- CSEM: Child Sexual Exploitation Material
- EDR: Emergency Disclosure Request
- EIO: European Investigation Order
- EJN: European Judicial Network
- EU: European Union
- IP: Internet Protocol
- LEA: Law Enforcement Authority
- MLA: Mutual Legal Assistance
- NCMEC: National Center for Missing & Exploited Children
- OGP: Online Gaming Platform
- OSP: Online Service Provider
- SPoC: Single Point of Contact
- UK: United Kingdom