Council of the European Union

Brussels, 10 February 2023
(OR. en)

6013/23

LIMITE

CATS 2
COPEN 35
COSI 25
ENFOPOL 62
JAI 106

NOTE

From:	Presidency
To:	Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS)
Subject:	Going Dark: Justice perspectives on access to communications data for law enforcement purposes

Introduction

Access to data related to internet and electronic communications has become an essential part of most criminal investigations [1].

New digital services are continuously being made available, providing citizens, companies and organisations with efficient and secure ways to exchange and process information. This has meant that policymakers have had to deal with a double evolution.

[1] In its EU Security Union Strategy (COM(2020)605 final), the Commission observes that electronic evidence is needed in about 85 per cent of investigations concerning serious crime.

On the one hand, judicial authorities and investigators are able to use types of electronic data that did not exist before to identify individual behaviours, delivering key evidence in concrete cases. The amount of data available is growing every day as more and more aspects of the life of citizens are digitalised. On the other hand, this digitalisation has meant that judicial authorities and investigators are losing access to other types of information and evidence because an increasingly important part of the commission or preparation of offences does not require movements or contacts in the physical world. Digital services are increasingly abused by criminals to commit crimes such as child sexual abuse, online rape, fraud, ransomware attacks or attacks on critical infrastructure. It is easy for criminals to 'go dark' under these circumstances. In other words, criminals can commit crimes in ways that law enforcement cannot detect and intercept.

This "going dark" phenomenon is caused by changes which reduce the possibilities for law enforcement and judicial authorities to access existing electronic data. This includes, in particular, the massive switch to internet-based communications (OTT services), coupled with the expanding use of end-to-end encryption and with the difficulties to obtain cooperation of providers located abroad. Another key evolution is the Court of Justice case law on data retention. Other factors include for example the impact of EU data protection legislation on access to Whois data, etc.

At operational level, the successful ANOM, EncroChat and SKY ECC related operations are cases in point, and not only with regard to how necessary access to communications data and the sharing of data can be in effectively fighting organised crime. They also offer a glimpse of how easy it has become for criminals to contact each other to commit violent crimes, drug or arms trafficking, etc. The results of these operations have also highlighted a small fraction of the extensive ongoing criminal activities in the dark, that thrive on remaining undetected, and at the same time have a direct impact on the security of our societies.

The Swedish Presidency is committed to tackling the "going dark" phenomenon, to make sure that judicial and law enforcement authorities have the necessary means to investigate and prosecute crime and to ensure a high level of protection of fundamental rights. The debate around proportionality on issues related to access to communications data for law enforcement purposes is a difficult one. Prosecutors, judges and national and EU legislators have had to cope with these issues for the past 20 years. It has implied difficult decisions on what the existing legal framework means in relation to new – and rapidly evolving – technologies and on what is the balance that new legislation should achieve. In the Presidency's view, the protection of fundamental rights must include the ability to provide security for our citizens, effective means of investigating and prosecuting crime, and protecting and providing justice to victims of crime. These complex issues highlight the need to discuss access to communications data as a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences, as well as the protection of victims of crime and threats to public security.

As a first step in this conversation, Ministers of Home Affairs discussed these issues during their informal meeting in Stockholm on 26 January. Ministers of Justice were informed of the outcome of the discussions the next day.

The sector of access to electronic and internet communications must be approached as a whole

A key factor in successfully tackling the challenges at hand is to approach the sector of access to communications data as a whole. The Council and its preparatory bodies have already worked on many related issues, including data retention, end-to-end encryption, e-evidence and access to Whois data. However, the discussions have been mostly fragmented, focusing on each issue separately.

Approaching these issues more globally from a policy making perspective is necessary to highlight the trend of "going dark" and to take it into account in policy choices to be made. For example, understanding the impact of limitations to data retention requires to be aware of the loss of data resulting also from end-to-end encryption of internet-based communications.

Additionally, a more global approach can help in developing a better narrative in public debate and during the negotiations of specific legislative instruments. With a view to allowing a better and more complete narrative to develop, it is important to highlight the complexity of the issue and the need for a nuanced analysis based on a global overview, rather than a sterile opposition between privacy and security.

Approaching the sector of access to communications data as a whole could also help the Council to take the appropriate position, and in negotiating with the Parliament, on legislative files which are not handled in the JHA structure but have an important impact on law enforcement and criminal proceedings. This is the case for the e-Privacy Regulation and for the Media Freedom Act, for which excellent coordination within Member States will be essential to make sure that the result is satisfactory also from the point of view of criminal justice.

The sector of access to electronic and internet communications has a strong criminal justice dimension

Many challenges arising from the "going dark" evolution require solutions in terms of technological tools, mutualisation of resources, specialisation of law enforcement authorities, forensic capacity, dialogue between law enforcement authorities and the private sector, etc. Together with national police authorities, Europol's Cybercrime Center and Innovation Lab plays a key role in this regard. The work of ENLETS (European Network of Law Enforcement Technology Services) should also be highlighted. When it comes to the Council's preparatory bodies, COSI will tackle these aspects.

Other aspects are related to criminal law and judicial cooperation in criminal matters. This is particularly the case in several well identified files.

Extensive work on data retention has been done and continues in COPEN including analysis and exchange of views on ECJ case law, exchange of information on national evolutions, reflexions on possible solutions at the EU level, etc.

The process on the so-called "e-evidence" file (which covers direct transmission to the service provider of national decisions to access data related to internet communications in the course of criminal proceedings) has required intensive efforts. More than seven years after the issue was raised in Council, the legislative framework is now being finalised. The Presidency is of the view that it will be important to maintain a close look at upcoming efforts to make sure that the new instruments work in practice.

Regarding the international framework, COPEN will be consulted by the Commission with regard to the negotiation of the EU-US agreement on e-evidence and the ongoing Cybercrime Convention negotiations in the United Nations. COPEN had the same role for the negotiation of the Second Additional Protocol to the Budapest Convention.

More generally, a number of horizontal criminal law issues common to the sector of access to communications data have arisen across various files. This includes procedural safeguards (such as the need or not for a decision by a judge to access data), the need for and the wording of exclusion or derogation clauses in EU legal instruments so as to avoid a negative impact on the prosecution of criminal offences, jurisdiction and territoriality issues, etc.

It is also clear that the Court of Justice is more and more involved in the field of access to communications data and that its case law is likely to cover more and more aspects of criminal procedure. This is apparent already from the case law on data retention. In that regard, it is interesting to note that, in the absence of specific secondary legislation the ECJ is entering more and more into the compatibility of specific aspects of procedural criminal law (including on the independence of judicial authorities or admissibility of evidence) with the Charter based on a Directive adopted as part of the development of the internal market.

The recent request for a preliminary ruling (C-670/22) brought to the ECJ on the basis of the interpretation of the Directive on the European Investigation Order concerning EncroChat also demonstrates the expanding involvement of the Court in issues related to access to communications data.

Further, access to communications data is an essential part of the work of the European Judicial Cybercrime Network (EJCN). Eurojust is also very active in the field. Prosecutors in the EJCN and at Eurojust play a key role not only in making judicial cooperation in relation to access to communications data work in practice, but also in identifying new common challenges arising at national level and sharing best practices.

Next steps

At the informal meeting of Ministers of Home Affairs in Stockholm, the idea of establishing a new forum, gathering all relevant actors, to jointly take the issue of access to data forward, received broad support. The task of defining the continuation of the work was subsequently given to COSI. Discussions will proceed at the COSI meeting on 22 February.

With this said, it seems clear that, if the "going dark" challenge is to be approached as a whole, aspects related to judicial cooperation in criminal matters and issues within the competence of CATS need to be taken into account. More specifically, it would be necessary to assess the remaining or newly emerging challenges that arise when it comes to access to data. In the view of the Presidency, it therefore seems appropriate to have a discussion on the issue of access to communications data for law enforcement purposes in CATS. The outcome of this discussion will be useful for the next steps, including the coming discussions in COSI.

QUESTIONS:

- **Do you share the view that, as part of a necessary multidisciplinary approach, CATS should participate in identifying challenges and possible opportunities, in particular when it comes to access to communications data? Do you agree that CATS should keep a horizontal view focusing on aspects related to criminal justice?**

- **Do you see aspects of access to communications data which should already be identified as requiring attention from a criminal justice point of view, other than those already mentioned throughout the document (such as data retention, e-evidence, end-to-end encryption and lawful interception, derogation clauses, territoriality issues, etc) to be addressed in future discussions related to this "going dark" challenge ?**