PRESIDENCIA
ESPAÑOLA
CONSEJO DE LA
UNIÓN EUROPEA

Discussion paper

Working lunch. Police access to electronic communications and digital data as a premise for law enforcement: The need for a respectful and effective legal framework

Informal JHA ministerial meeting – Home Affairs
20-21 July 2023
Logroño

Discussion paper

Working lunch. Police access to electronic communications and digital data as a premise for law enforcement: The need for a respectful and effective legal framework.

European context

Fundamental rights can only be enjoyed in a context of security and public order. The challenge is finding an acceptable balance between all of the rights concerned in a model of a peaceful and democratic society. The police and other law enforcement agencies are key actors in the practical implementation of concrete measures that contribute to this goal: to guarantee the desired level of security. The legal and operational tools necessary to investigate and prosecute crime must always be used in full compliance with fundamental rights.

In this regard, particularly sensitive and far-reaching issues arise when considering the matter of law enforcement access to data related to the use of electronic communications.

How can we ensure that the protection of rights and freedoms does not place police services in a position of technological inferiority in the investigation of criminals who are increasingly taking advantage of the tools available to them in the digital environment? What limits can/should be placed on the fulfilment of fundamental rights and freedoms while duly respecting the principles of necessity and proportionality? What kind of legal framework can reconcile all legitimate interests, and should it be adopted nationally by each Member State, or is there a need to regulate at European level?

We have already been discussing for a long time whether solutions can be found to maintain adequate levels of police and judicial effectiveness without undermining rights and freedoms. However, the vast majority of European citizens do not question that law enforcement agencies act with full respect for their rights when tackling serious threats to their security.

To understand the scale of the challenge/problem we face, it is necessary to know some facts. Electronic evidence is relevant in about 85 % of criminal investigations. At least 65 % of investigations where electronic evidence is relevant require a cross-border request. It is not only a question of being able to access – increasingly diverse – categories of electronic data that previously had to be retained, but also of being able to do so in the context of cross-border investigations.

When the preparatory work for the adoption of the 2006 Data Retention Directive began, a detailed study was carried out to support the need for the provision of data and its use. However, the objective scope of this study has become obsolete. Since then, new challenges have emerged and intensified, such as the increasing prevalence of end-to-end encryption, and access to

connection ports rather than just IP addresses, which have complicated the scope to be regulated and the process of reaching an agreement on the legal framework.

At the same time, investigations into serious and organised crime are almost always cross-border investigations, given the nature of the criminal organisations involved. This often means that mechanisms for international cooperation must be used, either through the traditional methods of mutual legal assistance or through the possibilities offered by agencies such as Europol and Eurojust. However, even with these institutions facilitating – and therefore accelerating – the process of requesting and exchanging relevant information, these procedures take time. If data are not retained for a reasonable period of time, requests for access are not viable.

The European Police Chiefs, meeting in Lisbon on 30 March 2023, expressed their concerns in a joint declaration on the impact of a lack of an EU data retention regime for traffic and location data.

Almost 10 years after the CJEU invalidated the Data Retention Directive[1], a solution is needed. However, there seems to be no clear idea of how to proceed, either at European level or at the level of the individual Member States, given the limits imposed by the Court. Apart from some clarifications on the scope and limits of data retention, the only movement has been the confirmation and consolidation of the CJEU's case-law established in 2014 and 2016.

Bringing some light into the darkness

On this basis, we must push for the necessary measures to change the situation and bring some light into the darkness in which criminals operate and which our police and other law enforcement agencies face. The recently adopted initiative to set up a high-level group on access to data for effective law enforcement, co-chaired by the Commission and the rotating Presidency, is a good starting point. It will allow those involved to identify the main problems and to work together on possible solutions on all related dossiers in a holistic manner. It is important that the group's work results in clear, solid and achievable proposals, which the Commission can consider as the basis for a proposal on concrete technical and/or legislative initiatives.

Once the most appropriate solution has been chosen, it should be precisely designed and provided with all the necessary safeguards to make it future-proof. The solution should be resilient, including against legal proceedings that may be brought before the CJEU or any national court (by guaranteeing its full compliance with fundamental rights), and adaptable to technological developments likely to occur in today's societies. It is a complex task, but it is possible.

In this package of future measures, consideration should be given to the adoption of legislation at EU level establishing a new system for the retention of electronic communications metadata[2]. This could cover all the legitimate purposes of retention on which the CJEU has ruled, or be limited to only some of them, taking into account the specificities of national security.

[1] 2014 case (Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, C-293/12 and C-594/12)

[2] Electronic communications metadata includes traffic and location data (as well as subscription data), but does not include the content of the communication.

Harmonising data retention rules would also represent a strong political commitment to what is seen as the right balance – and the benefits are clear.

Law enforcement authorities are asking us to ensure not only that they maintain their access to data, but also that the data provided by service providers is clear and usable. They are also asking us to provide access to other types of data held by service providers that are not currently available to law enforcement, but which are essential, such as connection port or network event information. Law enforcement authorities also must adapt to ever-changing technological developments.

In addition to technical solutions and the innovation and investment they require, a new legal framework is needed to provide legal certainty for law enforcement, judicial authorities and service providers. To this end, we must highlight the importance of moving towards a European solution: it no longer seems feasible to legislate or act in isolation in this area, as in so many others that fall within our remit as guarantors of citizens' security.

Questions for delegations

1. Do ministers agree that a basis should be laid for a new proposal for European rules on retention of and access to electronic communications metadata, overcoming the current situation resulting from the invalidation of the 2006 Directive? If so, with respect to the competences of Justice in this area, what main elements do ministers consider that that basis should comprise from an internal security/law enforcement perspective?

2. The information available to traditional service providers is becoming less relevant compared to that available to new and non-traditional service providers[3]. Do ministers agree on the general need to engage with industry and, in particular, to encourage cooperation and joint work with industry to promote not only privacy by design, but also the development of capabilities to enable legal access to information, where necessary for law enforcement purposes, on a case-by-case basis and with due respect for the fundamental rights of citizens?

[3] An example of one of these new service providers is over-the-top (OTT) platforms, which offer media and communication services via the internet without the involvement of traditional operators in the control or distribution of the content.