Council of the European Union

Brussels, 17 February 2023
(OR. en)

5607/23

LIMITE

COSI 22
CRIMORG 13
ENFOPOL 61
IXIM 26
CT 20
CATS 8
CYBER 29
TELECOM 36
DATAPROTECT 37
COPEN 34
JAI 151

NOTE

From:	Presidency
To:	Delegations
Subject:	Digital files - state of play

The Presidency wishes to underline the importance to internal security of several ongoing discussions and legislative negotiations on digital files. Technological development and digitalisation are game changers for our societies across all sectors. Retaining and accessing relevant information, analysing it and acting upon it within legally prescribed powers is the very essence of law enforcement work. It is central to ensuring the capacity of criminal justice systems and law enforcement agencies to access data in a digital environment, including encrypted communications data and electronic evidence. The situation is exacerbated by the limitless exploitation of technological development in the criminal underworld. Whilst there is a general tendency for more and more legislative proposals to be addressed horizontally and thus viewed in terms of their overall impact, the direct effects of each proposal will be felt - though not necessarily negotiated - in our sector. General digital policy developments need also to benefit the JHA sector while addressing and minimising the associated risks. This, in turn, requires a high degree of coordination across a wide range of policies, including the internal market, telecoms and data protection.

COSI should continue to monitor and discuss relevant concepts and updates on the different initiatives. These efforts should also facilitate creating a positive narrative and consolidating views on the justice and internal security needs related to technological development and digitalisation. National coordination processes, and the consolidation of national positions between sometimes differing views, play a key role and should ensure that internal security sector considerations are channelled into the working fora leading the negotiations on the various legislative proposals.

The following provides an overview on the current status of certain digital files relevant to internal security/law enforcement interests.

AI Act

On 6 December 2022, the Council adopted its general approach on the Artificial Intelligence Act (14954/22). The Council is now waiting for the Parliament's position, expected in the first quarter of 2023, in order to start the trilogues. Though the JHA communities have been involved, to some extent, in the negotiations on the AI Act due to the significant consequences for the JHA sector (especially for law enforcement authorities), it remains crucial to closely follow this file, especially during the trilogue phase. It is likely that the European Parliament's position will diverge significantly from the Council mandate on a range of issues, including crucial ones (e.g. Article 5 on the ban of real-time remote biometric identification).

Regulation to prevent and combat child sexual abuse (CSA)

The Commission presented its proposal for a Regulation on laying down rules to prevent and combat CSA (9068/22) in May 2022. The Czech Presidency organised eight meetings of the LEWP-Police to examine the proposal in its entirety and to table compromise texts on three chapters. The examination of the proposal continued in meetings of the LEWP-Police during the Swedish Presidency. The meetings in January were devoted to horizontal issues linked to detection orders and fundamental rights (inclusion of audio communications, options for voluntary detection to continue, detection in interpersonal communications and impact on end-to-end encryption), as well as other categories of orders. The presentation of its Joint Opinion 4/2022 by the European Data Protection Supervisor in LEWP-Police on 19 January was followed by a Q&A session with delegations. Following those exchanges of views and delegations' written contributions, the Presidency tabled compromise proposals concerning removal orders, blocking orders and delisting orders.

Work in the European Parliament has not formally started yet but the lead committee (LIBE) and the rapporteur (Zarzalejos, EPP/ES) have been appointed.

E-evidence

A political compromise on the e-evidence package, consisting of a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, was reached in December 2022, and was formally confirmed by Coreper and in Parliament in January 2023. The legal instruments are expected to be formally adopted in early spring 2023.

Negotiations were time-consuming and challenging but the final result should give law enforcement and judicial authorities an important tool to fight crime more effectively.

ePrivacy and lawful access to electronic evidence, including data retention

The proposal for a Regulation on the respect for private life and the protection of personal data in electronic communications (proposal for e-Privacy Regulation) was published on 10 January 2017.

It will replace Directive 2002/58/EC (e-Privacy Directive) and specify the General Data Protection Regulation (GDPR). The objective is to reinforce trust, security and confidentiality of the communications in the Digital Single Market (including content and metadata, e.g. sender, time, location of a communication), while providing flexible regulatory tools to enable innovation, defining clearer rules on tracking technologies such as cookies (including more friendly ways for users to express consent) as well as on spam. It applies both to natural and legal persons and includes in its scope also market-players using the internet (e.g. 'Over-the-Top communication services', as instant messaging apps and web-based e-mail services), with the aim of ensuring a level playing field for companies.

The file is negotiated in the Telecom Working Party. On 10 February 2021, Coreper adopted a negotiating mandate on this legislative proposal. As far as JAI is concerned, the Council mandate includes important access to electronic evidence and data retention aspects (Article 2(2)(d) - Scope: Article 6(1)(d) - Opening for data processing for law enforcement and public security purposes; Article 7(4) -An explicit provision on data retention; Article 11 -Exceptions to the obligations and rights provided for in the instrument).

Trilogues started in May 2021, with one trilogue taking place per Presidency (Portuguese, Slovenian, French). The first technical meeting under the Czech Presidency was held on 14 September 2022, including some of the provisions related to data retention. At this stage, the Rapporteur requested to limit the references to data processing for law enforcement and public security purposes and data retention to the provision dealing with exceptions (Article 11) and to leave all the discussions on those matters to the end of the trilogue process. However, upon the Member States request, the EP agreed to discuss these articles in a technical meeting on 10 November 2022, where it confirmed its position. The Council reitarted its position and no compromise is found to date.The two other technical meetings foreseen under the Czech Presidency (22 and 24 November 2022) did not take place. At present the negotiations are on standby.

Media Freedom Act:

On 16 September 2022, the Commission presented a proposal for a Regulation establishing a common framework for media services in the internal market (European Media Freedom Act, EMFA). The proposal aims at improving the internal media market. From a law enforcement perspective, the proposal provides for a list of criminal offences covered by the notion of "serious crimes", with reference to some of the criminal offences listed in Article 2 (2) of the Council Framework Decision 2002/584/JHA. In addition, Article 4(2)(c) also provides for a prohibition to deploy spyware on device used by media service providers, unless certain conditions are met (e.g. justified on grounds of national security or in the case of serious crimes investigations).

In the Council, the negotiations take place in the Audiovisual and Media Working Party (AVMWP).

At this stage, the Parliament has not yet confirmed the lead Committee, nor appointed a Rapporteur.

European Digital Identity (revision of the eIDAS Regulation)

On 6 December 2022, the Council adopted its general approach regarding the framework for a European Digital Identity. The revised Regulation aims to ensure universal access for people and businesses to secure and trustworthy electronic identification and authentication by means of a personal digital wallet on a mobile phone. The general approach introduces changes to the Commission's proposal, on how the wallet functions to ensure that the person claiming an identity is the actual holder. It also makes sure that the text is in line with other EU laws, such as the cyber security legislation. Finally, the Council ensured that the wallet should not cost anything for individuals, but businesses may incur cost for authentication with the wallet.

At the Parliament the file has been assigned to the Industry, Research and Energy Committee (ITRE). Rapporteur is Romana Jerković (S&D, Croatia), to which the European Commission presented the legislative proposal on 17 June 2021. MEPs welcomed the proposal while raising some concerns on the digital divide and inclusion for those citizens less digitally literate and the need to guarantee security and data protection in the solutions. Three committees have been asked for an opinion, namely the Committee on the Internal Market and Consumer Protection (IMCO), the Committee on Legal Affairs (JURI) and the Committee on Civil Liberties, Justice and Home Affairs (LIBE).

The ITRE committee draft report, published on 31 May 2022, focuses on four areas: cybersecurity, governance, data protection (data minimisation and use of a single identifier) and digitalisation of public services. It amends the definition of European digital identity wallet and modifies its structure. The wallet could be issued not only by Member States or under a mandate of Member States but also by organisations established in the EU. The draft report expands the use of the wallet, by enabling citizens not only to prove their identity and share documents but also to verify companies and other citizens' identities and documents. The draft report also includes an explicit requirement for the design of the wallet to ensure cybersecurity and privacy by design. Furthermore, the draft report includes a new chapter on European Digital Identity Board that would have advisory and coordination tasks as well as a role in supporting the application of the regulation. Finally, the draft report encourages the 'once only principle' (i.e. not having to provide the same data to public authorities more than once). The ITRE committee is planning to vote on the draft report on 9 February 2023.