Council of the European Union

Brussels, 28 September 2021
(OR. en)

12060/21

LIMITE

COSI 176
ENFOPOL 336
CYBER 245
CRIMORG 82
JAI 1030

NOTE

From:	Presidency
To:	Delegations
Subject:	The digital dimension of investigating child sexual abuse: challenges and way forward

Virtually all criminal activity, ranging from terrorism and serious forms of organised crime to petty crime, now features a strong digital dimension. Despite continued law enforcement efforts, it is still often easier, less risky and more efficient to perpetrate crime online than offline, whether it is selling firearms and drugs and communicating on the dark web, or spreading online content that can be used to radicalise vulnerable targets for violent purposes.

Child sexual abuse is no exception. It involves both online aspects (e.g. forcing a child to engage in sexual activities via live streaming or distributing child sexual abuse material online) and offline aspects (e.g. engaging in sexual activities with a child or causing a child to participate in child prostitution), which are often used in combination by perpetrators of these crimes.[1] It is estimated[2] that the COVID-19 pandemic has led both to children becoming more active and connected online, often unsupervised, and to an increase in the number of criminal activities relating to child sexual abuse on both the web and dark web. An increasing number of children have thus become vulnerable to those who wish to exploit this growing online presence for the most abhorrent purposes.

[1] EU strategy for a more effective fight against child sexual abuse, COM(2020) 607 final, 24.7.2020

[2] See 'Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic', Europol, 19 June 2020, and European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021, Europol, 12 April 2021. According to Europol, online child sexual abuse likely remains highly underreported and many victims remain unidentified and their abusers undetected.

Countering child sexual abuse is one of the main priorities of the Slovenian Presidency of the Council of the EU. To fight child sexual abuse effectively, it is essential to focus on the digital dimension of this criminal phenomenon. Central to this effort is ensuring and preserving the ability of law enforcement and judicial authorities to exercise their powers, as prescribed and authorised by law, both offline and online.

The current situation, however, poses various challenges as regards competent authorities' access to data in their daily work, a prerequisite for their activities and central to the performance of their tasks. In particular, a number of recent cases have shown the critical importance of proactive information from social media platforms, hosting providers and electronic communications providers. Often, child sexual abuse is only detected because of their reports, especially because the content is usually shared in closed networks and not publicly disseminated, giving visibility to providers alone. As a result, a number of Member States are currently reflecting on ways to strengthen the framework for the proactive detection and reporting of child sexual abuse online. The European Commission has announced a legislative proposal to be put forward in December which could include the creation of an EU centre to prevent and combat child sexual abuse. Furthermore, the Council recently held a debate on the Digital Services Act and its implications for the Justice and Home Affairs field. A possible next step could be a discussion on the role of proactive measures – extending above and beyond what is provided for in the Digital Services Act proposal – in addressing the specific phenomenon of child sexual abuse online.

Several other ongoing or future legislative files feature aspects that are critical as regards how law enforcement can access data to detect, prevent, investigate and prosecute criminal offences, a prime example being child sexual abuse. These include e-evidence, e-privacy, data retention, including the development of CJEU case law, the introduction of 5G, and encryption, including its links with the NIS 2 proposal.

In addition, during investigations law enforcement is often challenged by the significant volume of data that has to be analysed, as well as by the accessibility of information used as evidence. For example, the introduction of end-to-end encryption, which in itself is a major tool for ensuring privacy and security of communications, facilitates perpetrators' access to secure channels. They can hide their criminal activities from law enforcement and continue trading illegal material and grooming children, abusing the very tools created to safeguard the privacy of citizens and to protect their data.

The rules regarding law enforcement access to data are being defined in individual pieces of legislation which are often horizontal in nature, and handled in diverse fora. Robust coordination and a comprehensive approach are crucial to ensure that there are no gaps in the law. For example, the entry into force of the European Electronic Communications Code in December 2020 created a situation where certain online communication services, such as webmail or messaging services, would fall under the scope of the e-Privacy Directive. However, the Directive notably did not contain an explicit legal basis to continue the voluntary measures for the detection and reporting of child sexual abuse online, and the removal of such material. The Commission had to urgently introduce an interim Regulation[3] so as not to jeopardise the continued application of the voluntary measures.[4]

It is therefore important to have a broad policy discussion at the highest political level on the challenges and way forward in relation to the underlying question: what is required, in concrete terms, in order to ensure an operationally *sufficient* level of access to data for authorities that are responsible for public/internal security, including to safeguard the most vulnerable members of our societies. The latter aspect is clearly illustrated by the need to address the digital dimension when investigating child sexual abuse, and the challenges this involves.

[3] COM(2020) 568 final

[4] The European Commission is expected to introduce a new overall package on countering child sexual abuse at the end of 2021.

Questions for ministers:

What are the most immediate objectives and how can access to data for competent authorities be guaranteed in order to effectively counter the exploitation of the digital dimension to commit crimes, especially against children?

How can the role of social media, hosting services and electronic communications services be strengthened to protect children and to prevent the circulation of child sexual abuse content via their services? What should be the role of proactive measures in addressing the specific phenomenon of child sexual abuse online?