Webinar

26th June 2023 (11:00 -13.00 CET)

EU Jurisprudence on admissibility of evidence obtained from SKY ECC and EncroChat phone networks

-

Encryption is an essential tool that helps protect data, communications, devices, and infrastructure from cyber threats and contributes to user privacy. On one side, strong encryption is considered cornerstone of contemporary digitalised democracies because it protects the privacy of citizens, the intellectual property of companies and the freedom of the press and fosters the development of digital economies.

On the other hand, rapidly growing use of robust encryption in everyday devices, such as products and services with encryption that can only be decrypted by the end user or customer, means that criminals—including drug dealers, child predators, and terrorists—use encryption to shield their illicit activities from authorities. This way encryption is standing in the way of successful investigations and prosecutions.

Legal and practical challenges on this field hamper the state and its authorities in exercising one of their primary obligation – to safeguard the security and the fundamental rights of citizens. The modern paradox, when the same technology protects and directly or indirectly harms the most important values of our society.

Until we find balanced solution that ensures privacy and safety for all, judicial and law enforcement authorities will obviously be in stressful position of constant search for new ways of obtaining legally admissible evidence for criminal proceedings. It seems that enhanced international cooperation, sharing knowledge and expertise, along with joint actions are key points to success.

Looking back to past joint operations, such as EncroChat and Sky ECC, there are effective ways to tackle this phenomenon. However, depending on different national frameworks, without uniform and clear legal provisions, in most cases it is impossible to predict the outcome of the criminal proceedings regarding this topic. The most challenging issues on the topic are related to the admissibility of LEA actions and gathered digital evidence.

In this webinar, participants will have a chance to obtain more information on state of play and key findings on lawful access to encrypted digital evidence, jurisprudence, admissibility and best practices with a focus on Encrochat, Sky ECC, Anom Encrypted Networks.

Agenda

	Time	Item	Speaker
1.	11:00	Introduction by Claudia Pina, Investigating Judge (JLD), SNE, Operations Department – Casework Unit, Coordinator EJCN Support Team, Eurojust	
2.	11:05	Presentation by Xavier Laurent, Deputy Prosecutor, National Counter Terrorist Public Prosecutor's Office, France	
3.	11:25	Joint presentation by Philippe Van Linthout, Investigating Judge, Co-President of the association of Investigating Judges and Jan Kerkhofs, Federal Magistrate, Belgium	
4.	12:25	Presentation by Sofia Mirandola, Judicial Cooperation Advisor, Operations Department – Casework Unit, Eurojust	
5.	12:40	Q&A session	
6.	13:00	End of the webinar	

The webinar will be in English with **simultaneous interpretation** in Albanian, Macedonian and Serbian languages.

During the **Q&A session**, participants will be able to ask questions to the speakers **in English** via the chat. If you would like to ask **questions in other languages** please send them to project team before the webinar: wbcrimjust@eurojust.europa.eu. We will translate and communicate them to the speakers.

How to participate?

1. You are invited to register **your participation** via following the link by 21/06/023:

https://eu.eventsforce.net/eurojusteu/384/home

Access Code: LA017

Registration deadline: 21/06/2023 (23:59)

2. Once registered, you will receive **the connection details** to access the webinar and instructions to use the Pexip platform

3. On 26th of June, you can connect to the webinar from your computer using any browser via the connection link received by email.