Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Second Additional Protocol

2021/0383(NLE) - 25/11/2021

PURPOSE: to authorise Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence.

PROPOSED ACT: Council Decision.

ROLE OF THE EUROPEAN PARLIAMENT: Council may adopt the act only if Parliament has given its consent to the act.

BACKGROUND: cybercrime continues to represent a considerable challenge to society. Notwithstanding the efforts of law enforcement and judicial authorities, cyberattacks, including ransomware attacks, are increasing and are becoming more complex. The borderless nature of the internet makes cybercrime investigations almost always cross-border in nature, thus requiring close cooperation between authorities in different countries.

The Commission estimates that **law enforcement and judicial authorities currently need access to electronic evidence in 85% of criminal investigations**, including cybercrime. As evidence of criminal offences is increasingly held in electronic form by service providers on the territory of foreign jurisdictions, the Commission considers it necessary to obtain such evidence by appropriate measures to uphold the rule of law.

The Council of Europe's **Budapest Convention on Cybercrime** aims to facilitate the fight against criminal offences committed through computer networks. 66 countries are currently party to the Convention, including 26 EU Member States. The Convention does not provide for the European Union to accede to the Convention. However, the EU supports the Budapest Convention, which remains the main multilateral convention for combating cybercrime.

On 9 June 2019, the Council authorised the Commission to participate, on behalf of the Union, in the negotiations for the **Second Additional Protocol** to the Council of Europe Budapest Convention on Cybercrime. The text of the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted by the Council of Europe Committee of Ministers on 17 November 2021 and is envisaged to be opened for signature in March 2022.

It is important that EU Member States take the necessary steps to **implement and ratify rapidly the Protocol**, as the Protocol:

- will ensure that law enforcement and judicial authorities are better equipped to obtain electronic evidence necessary for criminal investigations;

- will ensure that such measures to obtain access to electronic evidence will be used in a manner that allow Member States to respect fundamental rights, including criminal procedural rights, the right to privacy and the right to the protection of personal data;

- will resolve and prevent conflicts of law, affecting both authorities and private sector service providers and other entities, by providing compatible rules at international level for cross-border access to electronic evidence.

CONTENT: this proposal concerns the Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Council of Europe's Budapest Convention on Cybercrime, on enhanced co-operation and disclosure of electronic evidence.

The purpose of the Protocol is to establish common rules at international level to **enhance cooperation in relation to cybercrime and the gathering of evidence in electronic form** for criminal investigations or proceedings.

The Protocol recognises the need for **greater cooperation between States and the private sector** and for greater legal certainty for service providers and other entities regarding the circumstances in which they may respond to requests for disclosure of electronic evidence from criminal justice authorities in other parties.

The Protocol provides a basis:

- for the direct cooperation between competent authorities in one Party and entities providing domain name registration services in another Party, for the disclosure of domain name registration data;

- for the direct cooperation between competent authorities in one Party and service providers in another Party for the disclosure of subscriber data;

- for enhanced cooperation between authorities for the disclosure of computer data and cooperation between authorities for the disclosure of computer data in emergency situations;

- for mutual legal assistance in emergency situations, cooperation by videoconference and for joint investigations and joint investigation teams.

The Protocol requires the parties to ensure that powers and procedures are subject to an adequate level of protection of fundamental rights.