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

2021/0383(NLE) - 06/04/2022 - Legislative proposal

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 co-operation 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 our society. The borderless nature of the internet makes cybercrime investigations almost always cross-border in nature, thus requiring close cooperation between authorities in different countries.

As evidence of criminal offences is increasingly held in electronic form by service providers in the territory of foreign jurisdictions, and to enable an effective criminal justice response, it is necessary to obtain such evidence by appropriate measures in order to uphold the rule of law.

On 6 June 2019, the Council authorised the Commission to participate, on behalf of the Union, in the negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185) (the Convention on Cybercrime).

The Budapest Convention on Cybercrime aims to facilitate the fight against criminal offences committed through computer networks. The Convention:

- contains provisions harmonising domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;

- provides for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or where the evidence is in electronic form;

- aims to set up a fast and effective regime of international cooperation.

The Commission is committed to ensuring a swift conclusion of the negotiations on the Protocol. In participating in the negotiations on the Protocol, the Commission has ensured its compatibility with the relevant common rules of the Union. The European Parliament also recognised the need to conclude work on the Protocol in its 2021 resolution on the EU cybersecurity strategy for the digital decade.

The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted by the Committee of Ministers of the Council of Europe on 17 November 2021 and is envisaged to be opened for signature on 12 May 2022.

The provisions of the Protocol fall within an area covered to a large extent by common rules within the meaning of Article 3(2) of the Treaty on the Functioning of the European Union (TFEU), including instruments facilitating judicial cooperation in criminal matters, ensuring minimum standards of procedural rights as well as data protection and privacy safeguards.

CONTENT: the purpose of the draft Council Decision is to authorise Member States to ratify, in the interest of the European Union, the **Second Additional Protocol to the Convention on Cybercrime**, on enhancing cooperation and the provision of electronic evidence.

The aim of the Protocol is to **enhance co-operation on cybercrime** and the collection of evidence in electronic form of a criminal offence for the purpose of specific criminal investigations or proceedings.

The Protocol recognises the need for increased and more efficient co-operation between States and with the private sector, and for greater clarity and legal certainty for service providers and other entities regarding the circumstances in which they may respond to requests from criminal justice authorities in other Parties for the **disclosure of electronic evidence**.

The Protocol also recognises that effective cross-border cooperation for criminal justice purposes, including between public sector authorities and private sector entities, requires effective conditions and strong safeguards for the protection of fundamental rights.

The Protocol:

- applies to specific criminal investigations or proceedings concerning criminal offences related to computer data and systems and to the collection of evidence in electronic form of a criminal offence;

- determines the languages in which the parties must submit orders, requests or notifications under the Protocol;

- provides for the widest possible mutual cooperation between the parties and provides for **swift procedures that improve cross-border access to electronic evidence** and a high level of safeguards. Its entry into force will contribute to the fight against cybercrime by facilitating cooperation between Member States party to the Protocol and third countries party to the Protocol, ensure a high level of protection for individuals and resolve conflicts of law.

The Protocol provides a basis for:

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

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

- enhanced cooperation between authorities for the disclosure of computer data;

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

- mutual legal assistance in emergency cases;

- cooperation by videoconference;

- joint investigations and joint investigation teams.

The entry into force of the Protocol will help promote EU data protection standards at global level, facilitate data flows between Member State Parties and third-country Parties, and ensure compliance of Member State Parties with their obligations under Union data protection rules.