

DECISIONS

COUNCIL DECISION (EU) 2022/895

of 24 May 2022

authorising the opening of negotiations on behalf of the European Union for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 82(1) and (2), and Article 83(1), in conjunction with Article 218(3) and (4) thereof,

Having regard to the recommendation from the European Commission,

Whereas:

- (1) On 27 December 2019, the United Nations General Assembly adopted Resolution 74/247 on countering the use of information and communications technologies for criminal purposes, deciding to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.
- (2) The Union has already adopted rules that cover some, but not all, of the elements that are likely to be considered for inclusion in the comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Those rules include in particular instruments on substantive criminal law ⁽¹⁾, on police and judicial cooperation in criminal matters ⁽²⁾ and on minimum standards of

⁽¹⁾ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1); Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8); Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (OJ L 123, 10.5.2019, p. 18).

⁽²⁾ Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 1); Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (OJ L 295, 21.11.2018, p. 138); Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53); Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams (OJ L 162, 20.6.2002, p. 1); Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJ L 328, 15.12.2009, p. 42); Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1).

procedural rights ⁽³⁾, as well as data protection and privacy safeguards ⁽⁴⁾. In addition, as legislative proposals have already been made and discussed in additional associated domains, those proposals should also be taken into account to the extent that they aim to reinforce the effectiveness of the Union legal framework.

- (3) Therefore, a comprehensive international convention on countering the use of information and communications technologies for criminal purposes may affect certain Union rules or alter their scope.
- (4) In order to protect the integrity of Union law and to ensure that the rules of international law and Union law remain consistent, it is necessary that the Commission participate, alongside Member States, for matters falling within the Union competence, as defined by the Treaties, and in respect of which the Union has adopted rules, in the negotiations on a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.
- (5) On 22 March 2021, the Council adopted conclusions on the EU cybersecurity strategy for the digital decade. Therein, the Council recalled that several aspects of the negotiations on a comprehensive international convention on countering the use of information and communications technologies for criminal purposes could relate to the Common Foreign and Security Policy, by stressing that it 'supports and promotes the Budapest Convention on Cybercrime and the ongoing work on the Second Additional Protocol to this Convention. Furthermore, it continues to engage in multilateral exchanges on cybercrime, including in processes related to the Council of Europe, the United Nations Office on Drugs and Crime (UNODC) and the Commission on Crime Prevention and Criminal Justice (CCPCJ), to ensure an enhanced international cooperation to counter cybercrime, including the exchange of best practices and technical knowledge and support for capacity building, while respecting, promoting and protecting human rights and fundamental freedoms'.
- (6) This Decision should be without prejudice to the division of competences between the Union and its Member States as defined by the Treaties, to the participation of Member States in the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes and to any subsequent decision to conclude, sign or ratify such a convention.
- (7) The negotiating directives set out in the addendum to this Decision are addressed to the Commission and may be revised and further developed if appropriate depending on the evolution of the negotiations.
- (8) In accordance with the principle of sincere cooperation, the Commission and the Member States should cooperate closely during the negotiation process, including through regular contacts with the Member States' experts and representatives in New York and Vienna.

⁽³⁾ Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings (OJ L 280, 26.10.2010, p. 1); Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (OJ L 142, 1.6.2012, p. 1); Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294, 6.11.2013, p. 1); Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297, 4.11.2016, p. 1); Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132, 21.5.2016, p. 1); Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (OJ L 65, 11.3.2016, p. 1).

⁽⁴⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1); Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89); Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ L 337, 18.12.2009, p. 11).

- (9) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on 18 May 2022 ^(?).
- (10) In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union (TEU) and to the Treaty on the Functioning of the European Union (TFEU), and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Decision and is not bound by it or subject to its application.
- (11) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Decision and is not bound by it or subject to its application.

HAS ADOPTED THIS DECISION:

Article 1

1. The Commission is hereby authorised to open negotiations, on behalf of the Union, as regards matters falling within the Union's competence, as defined by the Treaties, and in respect of which the Union has adopted rules, for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

2. The negotiations shall be conducted on the basis of the negotiating directives of the Council set out in the addendum to this Decision which may be revised and further developed as appropriate depending on the evolution of the negotiations.

Article 2

The negotiations shall be conducted in consultation with the Working Party on Judicial Cooperation in Criminal Matters, which is hereby designated as the special committee within the meaning of Article 218(4) TFEU.

The Commission shall regularly report to the special committee referred to in the first subparagraph on the steps undertaken pursuant to this Decision and consult it on a regular basis.

Whenever so requested by the Council, the Commission shall report to it on the conduct and the outcome of the negotiations, including in writing.

To the extent that the subject matter of the negotiations falls within the competences of both the Union and its Member States, the Commission and the Member States shall cooperate closely during the negotiating process, with a view to ensuring unity in the international representation of the Union and its Member States.

Article 3

This Decision and its addendum shall be made public immediately after their adoption.

Article 4

This Decision is addressed to the Commission.

^(?) Opinion of 18 May 2022 (not yet published in the Official Journal).

Done at Brussels, 24 May 2022.

For the Council
The President
B. LE MAIRE

ADDENDUM

DIRECTIVES FOR THE NEGOTIATION OF A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

Regarding the process of the negotiations, the Union should aim to achieve that:

- (1) The negotiation process is open, inclusive and transparent, and based on cooperation in good faith.
- (2) The negotiation process enables participation in a meaningful way of all relevant stakeholders, including representatives of civil society, the private sector, academia and non-governmental organisations.
- (3) Inputs received from all the United Nations Members are considered on an equal basis to ensure an inclusive process.
- (4) The negotiation process is based on an effective and realistic work programme.

Regarding the general objectives for the negotiations, the Union should aim to achieve that:

- (5) Whilst ensuring a high level of protection of human rights and fundamental freedoms, the Convention serves as an effective instrument for law enforcement and judicial authorities in the global fight against cybercrime, with the aim to promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively, to also promote and facilitate international cooperation, to ensure a high level of protection of victims' rights, and to support capacity building and technical assistance in the fight against cybercrime.
- (6) The existing framework of tried-and-tested international and regional instruments and efforts as reflected in United Nations General Assembly Resolutions 74/247 and 75/282 is taken into full consideration. Accordingly, the Convention is compatible with existing international instruments, in particular the 2000 United Nations Convention against Transnational Organized Crime and its protocols, the 2003 United Nations Convention against Corruption, the 2001 Council of Europe Budapest Convention on Cybercrime and its protocols, but also other relevant international and regional instruments, in particular relating to the protection of human rights and fundamental freedoms. The Convention avoids any impact on their application or the further accession of any country to these existing instruments and, to the extent possible, avoid unnecessary duplication.
- (7) The work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime as agreed by United Nations General Assembly Resolution 75/282 are taken into full consideration.
- (8) The provisions of the Convention achieve the highest possible protection of human rights and fundamental freedoms. EU Member States should be able to comply with international and EU law, including the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter of Fundamental Rights. The provisions of the Convention should also be compatible with the EU's and its Member States' international trade obligations.

Regarding the substance of the negotiations, the Union should aim to achieve that:

- (9) The Convention provides for definitions of offences that can only be committed using computer systems.
- (10) Provided that sufficient conditions and safeguards and an adequate protection of human rights and fundamental freedoms are guaranteed, as an exception to the principle set out in paragraph 9, the Convention could provide for definitions of offences that can be committed without using computer systems but that can be enabled by the use of computer systems in certain circumstances, but only in cases where the involvement of computer systems substantially changes the characteristics or impact of the offences.
- (11) The offences are clearly and narrowly defined in a technology neutral manner. The definitions are compatible with those in other relevant international or regional conventions in particular in the area of cybercrime, and with international human rights standards and fundamental freedoms.

- (12) The Convention provides for rules on aiding and abetting and, where appropriate, on the attempt of such offences, on the liability of both natural and legal persons for such offences, for rules on the establishment of jurisdiction over such offences, and on effective, proportionate and dissuasive sanctions and measures in relation to such offences that are compatible with other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and with international human rights standards.
- (13) The Convention provides for procedural criminal measures that allow authorities to investigate cybercrimes effectively, which could, providing that sufficient safeguards are provided for, include measures to preserve or obtain electronic evidence of any criminal offence as part of a criminal investigation or proceeding and, where there is, in addition, a demonstrated need and added value, measures to freeze and confiscate proceeds of such crimes, taking due account of the proportionality, legality and necessity principles, the protection of the rights concerning the respect for privacy and the protection of personal data.
- (14) Those procedural criminal measures do not contradict other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and are compatible with such conventions and with international human rights standards and fundamental freedoms.
- (15) Procedural measures to preserve or obtain electronic evidence contain a clear and narrow definition of the type of data covered. Procedural measures for cooperation with private sector entities ensure that the burden on such entities is proportionate and that private sector entities fully respect laws protecting human rights of their users. The Convention provides legal clarity for online service providers (e.g., Internet service providers) in their interactions with law enforcement authorities of the State Parties to the Convention. Procedural measures for the removal of illegal content only relate to illegal content that is sufficiently specific and narrowly defined in the Convention.
- (16) The Convention provides for cooperation measures that allow authorities in different States that are party to the instrument to cooperate effectively through mutual legal assistance, including by the establishment of contact points, for the purpose of criminal investigations or proceedings concerning offences defined in the instrument. It could also provide for such cooperation measures for the purpose of preserving or obtaining electronic evidence of any criminal offence as part of a criminal investigation or proceeding, provided that these measures are subject to sufficient conditions and safeguards under States' domestic law, which shall provide for the adequate protection of human rights and fundamental freedoms.
- (17) Those cooperation measures are compatible with other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and do not contradict such conventions, international human rights standards and fundamental freedoms.
- (18) Cooperation measures are subject to the conditions provided for by the law of the requested Party and provide for broad grounds for refusal such as to ensure the protection of fundamental rights, including the right to the protection of personal data, including in the context of personal data transfers, and the existence of double criminality.
- (19) The Convention provides for strict conditions and strong safeguards to ensure that EU Member States can respect and protect fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter of Fundamental Rights, including, in particular, the principles of proportionality, legality and necessity of criminal offences and penalties, procedural guarantees and rights, the right to effective judicial redress, the presumption of innocence, the right to a fair trial, and the rights of defence of persons subject to criminal proceedings, the right not be tried or punished twice in criminal proceedings for the same criminal offence, as well as the right to privacy, the right to the protection of personal data and of electronic communications data when such data is processed, including for transfers to authorities in countries outside the European Union, and the right to freedom of expression and information. The Convention ensures in particular that EU Member States are able to comply with requirements for the international transfers of personal data within the meaning of Directive (EU) 2016/680, Regulation (EU) 2016/679 and Directive 2002/58/EC. The conditions and safeguards also ensure the protection of human rights and fundamental freedoms in line with international human rights standards. This applies to the entire Convention, including procedural measures and cooperation measures, including those that may significantly interfere with individuals' rights.

- (20) The Convention provides a basis for voluntary capacity building measures to support countries in their ability to conduct effective cybercrime investigations and proceedings and to obtain electronic evidence for investigations and proceedings of other offences, including by means of technical assistance and training. The UNODC has a clearly described role for the implementation of such measures.
- (21) The Convention ensures that victims of cybercrime receive appropriate assistance, support, protection and access to compensation.
- (22) The Convention provides a basis for practical measures for the prevention of cybercrime that are clearly defined and strictly limited and distinct from criminal procedural measures that could interfere with the rights and freedoms of individuals or legal persons.

Regarding the functioning of the Convention, the Union should aim to achieve that:

- (23) The Convention preserves existing global and regional instruments and ongoing international cooperation in the global fight against cybercrime. In particular, the European Union Member States, in their mutual relations, are able to continue to apply the rules of the European Union.
- (24) The Convention provides for an appropriate mechanism to ensure its implementation and provide for final provisions, including on the settlement of disputes, signature, ratification, acceptance, approval and accession, entry into force, amendment, suspension, denunciation and depositary and languages that are modelled where possible and appropriate along the provisions of other relevant international or regional conventions in particular in the area of organised crime or cybercrime.
- (25) The Convention allows for the European Union to become a party to it.

Overall, the procedure for negotiation shall be as follows :

- (26) The Commission should endeavour to ensure that the Convention is consistent with relevant Union legislation and policies, as well as the Union's commitments under other relevant multilateral agreements.
 - (27) The Commission should conduct negotiations on behalf of the Union, for matters falling within its competence, in accordance with the Treaties, and in respect of which the Union has adopted rules.
 - (28) The negotiations, including each negotiation round, must be prepared well in advance. To this end, the Commission shall inform the Council of the schedule anticipated and the issues to be negotiated and shall share the relevant information as early as possible.
 - (29) In accordance with the principle of sincere cooperation, the Commission and the Member States should cooperate closely during the negotiation process, including through regular contacts with the Member States' experts and representatives in Vienna and New York.
 - (30) The negotiating sessions shall be preceded by a meeting of the Working Party on Judicial Cooperation in Criminal Matters in order to identify the key issues, formulate opinions and provide guidance, including formulating declarations and reservations, as appropriate.
 - (31) The Commission shall report to the Working Party on Judicial Cooperation in Criminal Matters on the outcome of the negotiations after each negotiating session, including in writing.
 - (32) The Commission shall inform the Council and consult the Working Party on Judicial Cooperation in Criminal Matters on any important issue that may arise during the negotiations.
-