European Parliament
2024-2029

Committee on Petitions

24.6.2024

NOTICE TO MEMBERS

Subject: Petition No 0760/2023 by B. O. (German) on the banning of encryption in the EU

1. Summary of petition

The petitioner claims that the Council of the European Union's current plan to ban encryption for all EU citizens, except for businesspeople, is a disproportionate measure. According to the petitioner, this would lead to 99.98 % of EU citizens having their fundamental rights restricted. The petitioner asks the European Parliament to continue rejecting the measures set out in the 'Draft Council Declaration on Encryption - Security through encryption and security despite encryption' (12143/20). The petitioner also urges the Commission to initiate infringement proceedings against the Member States on the grounds that breaches of Article 67(1) TFEU, in conjunction with Articles 6 to 8 of the EU Charter of Fundamental Rights, have been taking place for decades.

2. Admissibility

Declared admissible on 17 November 2023. Information requested from Commission under Rule 227(5), New Rule 233(5).

3. **Commission reply**, received on 24 June 2024

The Commission would like to stress that the fundamental rights to privacy and confidentiality of electronic communications and the right to data protection are guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

Directive 2002/58/EC[1] ('ePrivacy Directive') ensures the protection of the right to confidentiality of electronic communications and the users' terminal equipment. Also, the Commission proposal for a Regulation on Privacy and Electronic Communications[2] — which, if approved, will replace the ePrivacy Directive — ensures harmonisation and a high level of protection of confidentiality of electronic communications, and is currently negotiated by the co-legislators. In addition, Regulation 2016/679[3] ('GDPR') provides a comprehensive framework for the processing of personal data of individuals in the EU.

Directive 2016/680[4] (the 'Law Enforcement Directive or LED) complements this framework by setting out the data protection rules applicable to law enforcement authorities processing personal data, such as accessing personal data stored in a user's device, for the purpose of prevention, investigation and prosecution of criminal offenses.

Encryption plays a fundamental role for strong cybersecurity and the effective protection of fundamental rights, such as privacy and data protection. The GDPR and the LED explicitly mention encryption as an effective measure to guarantee the security of the processing of personal data[5]. The Article 29 Data Protection Working Party has even qualified encryption as a "*a necessity in the modern digital world*" given that it "*contribute*[s] *in an irreplaceable way to our privacy and to the secure and safe functioning of our societies*"[6]. However, the use of encryption should be without prejudice to the powers of competent authorities to safeguard national security and to prevent, investigate, detect and prosecute criminal offences, in accordance with the procedures, conditions and safeguards set forth by law. A. In that sense, a balance must be struck between the various rights and interests at stake, notably protection of privacy of users and security of communications in general, and the need to prevent and tackle the undetected grooming of a vulnerable group of users (i.e. children) and the dissemination of material concerning the abuse of children. All these rights are not absolute and can be subject to limitations where necessary and proportionate.
Also, Directive 2018/1972 ('EECC')[7] in recital 97 refers to the use of encryption for example, end-to-end encryption where appropriate, should be promoted, and where necessary be mandatory in accordance with the principles of security and privacy by default and by design, without prejudice to the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences.

The Commission has contributed to the discussions in the Council leading to the adoption of

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.
[2] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).
[3] Regulation 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).
[4] Directive 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.
[5] General Data Protection Regulation, Article 32(1)(a); Law Enforcement Directive, recital 60.
[6] Statement of the Article 29 Data Protection Working Party on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, p 3.
[7] Directive 2018/1972 of the European Parliament and of the Council of 12 December 2018 establishing the European Electronic Communications Code (recast).

the Council Resolution on encryption, calling for a discussion with the industry and the development of an appropriate regulatory framework that would allow national authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communications.[8]

Conclusion

The Commission agrees that encryption plays a fundamental role for strong cybersecurity and the effective protection of fundamental rights, including freedom of expression, privacy and data protection.

The Commission contributed to the discussions leading to the adoption of the Council Resolution on encryption, calling for a discussion with the industry and the development of an appropriate regulatory framework that would allow national authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communications.

The Security Union Strategy[9] provided that encryption plays a fundamental role in ensuring strong cybersecurity and the effective protection of fundamental rights, such as privacy, including the confidentiality of communications, and protection of personal data. At the same time, a substantial part of investigations against all forms of crime and terrorism involve encrypted information as criminals are using it to mask their identity and to hide the content of their communications. The Commission will explore and support balanced technical, operational and legal solutions to the challenges and promote an approach which both protect privacy and security of communications, while providing an effective response to crime and terrorism.

[8] Council Resolution on Encryption - Security through encryption and security despite encryption, 13084/1/20 REV 1, 24.11.2020.

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605