To the Portuguese Presidency of the Council of the European Union in 2021
Dear Prime Minister, António Costa,

We write to share our concerns about the consequences that may result from what appears to be a new European Union guideline on the use of digital cryptography for civilian purposes, both in terms of citizens' rights and guarantees, and in the erosion of progress made towards a digital transition.

Using the argument that it is important to fight against organized crime and the terrorist threat, the Council of the European Union, in its note of 24.11.2020, as well as the European Commission, its communiqué of 9.12.2020, affirm the intention to regulate the use of cryptography in digital communications with the aim that, when mandated by the courts, police authorities can “read” encrypted communications. It is important to bear in mind the following facts when considering this intention:

1. The cryptographic primitives available today do not allow meeting the objectives mentioned by the EC without jeopardizing the guarantees of secure communications that the current methods offer.

2. Without new (and improbable) cryptographic primitives, the only way to satisfy the goals expressed by the EC, would be to weaken existing encryption systems. It is unreasonable to expect that such a voluntary weakening of encryption would not lead to security breaches that would be used by ill-intentioned parties, thus facilitating an increase in criminal actions. This would dramatically undermine public confidence in the use of the digital communication network, which could have dramatic consequences for an economy which is strongly based on digital transactions.

3. It is not enough that posit that there may be encryption systems that have such chimeric characteristics (which we believe is not the case), it would also be necessary to prohibit the use of current systems which provide strong encryption. This will only affect the common citizen, without reducing criminal practices.

4. Any “solution” that involves changing the behavior of software component to achive the ultimate goal (the creation of “backdoors”) will result in even greater vulnerabilities and even worse results for the security of the systems and, consequently, will decrease users' confidence in digital media.

5. Our legal system does not allow certain communications to be scrutinized, even under a court order (for example, with some exceptions, attorney-client communications). Thus some communications would be exempted from the proposed new cryptographic order. Consequently, it would be necessary to distinguish citizens who could legally use strong cryptography from others who would have to commit a crime to do so. This is manifestly unfeasible: determined criminals would simply organize their communications to fall into the exempt category.

The signatories of this letter fear that, if this line of regulating and limiting the use of cryptography by weakening it is pursued:

- The fight against the crimes referred to above will not be more effective: it is not possible to prevent the use of existing strong cryptography.

- It is not feasible to criminalize of a wide range of actions hitherto taken as legitimate and justified.

- There would be a strong reduction in public confidence in digital communications as well as its widespread use, putting at risk the continued growth of a digital economy whose importance today is considerable.

- There would be a dramatic reduction in the guarantees given to ordinary citizens about their right to privacy and secrecy of communications (e.g. with their banks, financial institutions, legal advisors).

- It might promote a situation that can be a fertile ground for the development of regimes of strong control over the populations to the detriment of their democratic freedoms, hinder efforts to encourage the global adoption of the human rights enshrined in the European Convention on Human Rights, and be used as an argument (albeit spurions) to lend legitimacy to efforts of autocratic regimes to ignore those human rights.

The signatories,

Deutschland Chapter of the Internet Society (ISOC DE)
France Chapter of the Internet Society (ISOC FR)
Netherlands Chapter of the Internet Society (ISOC NL)
Portugal Chapter of the Internet Society (ISOC PT)
Switzerland Chapter of the Internet Society (ISOC CH)
…..