COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CDDH(2023)R99 Addendum 1
28/11/2023

STEERING COMMITTEE FOR HUMAN RIGHTS
(CDDH)

_____

COMMENTS ADOPTED BY THE CDDH ON RECOMMENDATIONS OF THE PARLIAMENTARY ASSEMBLY

Recommendation 2258 (2023)
"Pegasus and similar spyware and secret state surveillance"

PACE Recommendation 2258 (2023) - "Pegasus and similar spyware and secret state surveillance"

1. The Parliamentary Assembly refers to Resolution 2513 (2023) "Pegasus and similar spyware and secret state surveillance" and recommends that the Committee of Ministers:

1.1 adopt a recommendation to member States of the Council of Europe on secret surveillance and human rights, particularly in the light of the threats posed by new surveillance technologies and spyware, taking due account of the highest international standards, the case law of the European Court of Human Rights and Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223, "Convention 108+"). The recommendation should focus on:

1.1.1 the conditions for the acquisition of spyware by member States' government bodies and agencies;

1.1.2 the conditions for the use of spyware technologies for law enforcement and national security purposes;

1.1.3 the conditions for the sale and export of spyware technologies to third countries;

1.1.4 authorisation procedures, judicial supervision and oversight mechanisms, notification mechanisms and remedies applicable to the use of spyware by State authorities;

1.1.5 accountability mechanisms in cases of unlawful use of spyware;

1.1.6 human rights due diligence standards for spyware companies;

1.1.7 the transnational aspect of digital surveillance and the use of spyware;

1.1.8 the role of national parliaments;

1.2 examine the feasibility of a Council of Europe Convention on the acquisition, use, sale and export of spyware;

1.3 co-ordinate its efforts with other international organisations, including the European Union and the United Nations, in the areas of data protection, targeted surveillance and spyware, for the purposes of standard-setting and co-operation.

CDDH COMMENTS

1. The CDDH takes note of Parliamentary Assembly Recommendation 2258 (2023) "Pegasus and similar spyware and secret state surveillance". It shares the Assembly's concern at the deeply intrusive nature of such tools, given the role played by mobile phones in collecting, storing, and processing large amounts of highly sensitive personal data, and at the resulting risk of serious violations of the right to private and family life, as protected by Article 8 of the European Convention on Human Rights (the Convention).

2. The CDDH recalls the caselaw of the European Court of Human Rights (the Court) concerning secret surveillance and Article 8. The Court has recognised that even very extensive and/ or intrusive surveillance measures may exceptionally be required in a democratic society and thereby permitted under Article 8. In doing so, however, the Court has underlined the requirements and safeguards set out in the Convention, although it has not yet

given judgment in a case concerning Pegasus or similar spyware. Any such judgments may give rise to further developments in the Court's jurisprudence.

3. As regards the Convention's requirement that surveillance measures must pursue a "legitimate aim," the Court has affirmed that in the case of targeted surveillance measures, there must be an objectively reasonable suspicion based on factual indications for suspecting the person concerned of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures. Furthermore, surveillance measures must be "in accordance with the law" – they must have a basis in domestic law and be compatible with the rule of law. This implies foreseeability, namely that the law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to such measures.

4. The Court has indicated that for surveillance measures to be "necessary in a democratic society," as required by the Convention, there must be adequate and effective guarantees against arbitrariness and the risk of abuse. The Court has clarified the minimum requirements that should be set out in law to avoid abuses: (i) definition of the nature of offences which may give rise to an interception order; (ii) definition of the categories of people liable to have their communications intercepted; (iii) limitation of the duration of interception; (iv) a procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed.

5. Finally, the Court has stated that there should be review and supervision of secret surveillance measures when first ordered, while being carried out, and after having been terminated.

6. The CDDH further recalls the standards of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its amending Protocol (CETS No. 223).

7. The CDDH notes in particular the Parliamentary Assembly's proposal that the Committee of Ministers adopt a recommendation to member States on secret surveillance and human rights. The CDDH considers that the preparation of a non-binding instrument would be feasible and have genuine added value, bearing in mind the gravity of the threat to individuals' right to private life posed by potential abuse of Pegasus and similar spyware. Such an instrument could be a recommendation, but it could also be, for example, guidelines applying principles from the Court's jurisprudence to the case of spyware, along with examples of existing good national practice.

8. Recalling its preparation of the 2002 Committee of Ministers' Guidelines on human rights and the fight against terrorism, which touched upon the collection and processing of personal data and measures that interfere with privacy, the CDDH would be ready to contribute to work on any new non-binding instrument, taking into account subsequent developments in the Court's caselaw and the adoption of the amending protocol to Convention ETS No. 108.

9. As regards the Parliamentary Assembly's proposal that the Committee of Ministers examine the feasibility of a Council of Europe convention on the acquisition, use, sale and export of spyware, the CDDH considers that these aspects could be examined in the context of follow-up to Committee of Ministers Recommendation CM/Rec(2016)3 on human rights and business.