EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

The Director-General

Brussels
JUST.C.3/CS/ks(2022)9917600

Dear Ambassador,

Following reports on the use of spyware in or by Member States, the European Commission intends to do a mapping of the situation in Member States and examine the interplay with EU law. For that purpose, we are requesting information from all Member States about the use of spyware[1] by national authorities and the legal framework governing such use.

In this context, I would appreciate it if you could provide us with information in reply to the questions set out in this letter. For each of these questions, it would be important to clearly indicate the relevant national legal provisions.

1. For what purpose is the use of spyware permitted under national law:
   a. criminal law enforcement?
   b. national security?
   c. any other purpose (please specify)?

2. Please list all authorities which are permitted by national law to use or authorise the use of spyware.

(1) For the purposes of this exercise, spyware is understood to mean "*any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting or analysing data from such products or from the natural or legal persons using such products, in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data or tracking activities across multiple end-user devices, without the natural or legal person concerned being made aware in a specific manner and having given their express specific consent in that regard*" (Article 2 of the Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU, COM/2022/457 final).

HE Mr Lars DANIELSSON
Ambassador Extraordinary and Plenipotentiary
Permanent Representative of Sweden
Square de Meeûs 30/De Meeûssquare 30
1000 Bruxelles/Brussel
representationen.bryssel@gov.se

3. If your reply to question 1 b) is affirmative, please specify:
   a. the definition of national security or the criteria used to define the scope of national security;
   b. the relevant legislation that governs the processing of data for national security purposes;
   c. which bodies supervise the use of spyware by public authorities (e.g. internal oversight within national security authorities; external oversight by administrative bodies, independent authorities, courts or the national parliament, etc.).

4. What are the conditions for the use of spyware under question 1 a), 1 b) and 1 c)? Please explain the type of safeguards that exist under national law (e.g. whether there is a limit on what data can be accessed, on the duration of the measure, on the personal scope, etc.).

5. Please specify if the use of spyware for purposes under question 1 a), 1 b) and 1 c) requires prior authorisation by a court or an independent administrative authority. If yes, please explain:
   a. the circumstances where prior authorisation is required and any criteria allowing the authorisation to be issued;
   b. which court or independent administrative authority provides the authorisation;
   c. whether the court or the independent administrative authority has access to all information relating to the request for prior authorisation.

6. Are there any transparency requirements with respect to the use of spyware (e.g. reporting obligations to Parliament or oversight bodies on the use of spyware, public reporting on statistics, etc.)? Please specify the transparency requirements under question 1 a), 1 b) and 1 c).

7. Please specify:
   a. whether there is any requirement to notify the concerned individual(s), once there is no longer a risk to national security;
   b. what remedies are available to an individual who was subject to surveillance by means of spyware (e.g. judicial redress, administrative redress such as lodging a complaint to ombudspersons or oversight bodies);
   c. whether the administrative or judicial remedy examines the lawfulness of such a measure including whether the purposes specified in question 1 were invoked legitimately.

I would appreciate receiving your reply by 31 January 2023. Thank you for your cooperation.

Yours faithfully,

Ana GALLEGO