



Council of the European Union
General Secretariat

Brussels, 26 October 2021

**DOCUMENT PARTIALLY
ACCESSIBLE TO THE PUBLIC
(03.10.2022)**

WK 12803/2021 INIT

LIMITE

**COMER
CONOP
CFSP/PESC
ECO
UD
ATO
COARM
CYBER**


This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

| | |
|----------|---|
| From: | Presidency |
| To: | Working Party on Dual-Use Goods |
| Subject: | Regulation of export of cybersurveillance items |

Following the Dual Use meeting of October 25 under agenda item 2b, delegations will find the presentation given by a representative of the Institute for Information Law.

Regulation of export of cybersurveillance items

, Institute for Information Law

25 October 2021

Introduction and main question

- ▶ New DuRe introduces new framework for CS items
- ▶ Dutch MinFA engaged IViR to research implications
- ▶ Main question:
 - ▶ what is the scope of CS items?
 - ▶ how should the authorisation requirement be applied to CS framework?

Approach

- ▶ Individual interviews with industry, NGOs, authorities, experts
- ▶ Two roundtables where interviewees could comment on draft
- ▶ Written by [REDACTED], [REDACTED], [REDACTED] and me

Old framework: non-listed items and HR considerations

- ▶ Basic rules, already present under old DuRe:
 - ▶ authorisation required if listed item (Art. 3);
 - ▶ MS may require authorisation for non-listed item for HR considerations (Art. 9(1)).

New framework: authorisation and transparency

- ▶ Authorisation also required if (Art. 5):
 - (i) non-listed CS item; and
 - (ii) exporter has been informed that item may be used to infringe human rights; or
 - (iii) exporter is aware b/c due diligence that it may be used for this, and CA requires authorisation.
- ▶ Transparency and co-ordination required:
 - ▶ if MS requires authorisation for CS item, it must inform other MS and EC;
 - ▶ EC publishes list of identical exports (Art. 5(4)); and
 - ▶ EC publishes dedicated information on authorisations for CS items, including application per item, MS, destination and decision.
- ▶ And MS may adopt legislation requiring authorisation for non-listed CS items, if the exporter has grounds for suspecting that those items are or may be intended, in their entirety or in part, for any of the uses referred to in paragraph 1 of this Article.

Authorisation in case of HR infringements

- ▶ items which are or may be intended for use in connection with
- ▶ internal repression and/or
- ▶ the commission of serious violations of human rights and
- ▶ international humanitarian law.
- ▶ Council Common Position should be guiding

So what are cybersurveillance items?

- ▶ Art. 2(20) DuRe:
 - ▶ dual-use items specially designed
 - ▶ to enable the covert surveillance of natural persons
 - ▶ by monitoring, extracting, collecting or analysing data
 - ▶ from information and telecommunication systems
- ▶ Starting point: intended to protect human rights

So what are cybersurveillance items? (cont'd)

- ▶ “to enable the covert surveillance of natural persons”
- ▶ “covert”: if that person does not know whether *and how* information on her is being used to target her specifically
- ▶ “surveillance”: surveillance as used by the ECHR and the CJEU, which is very broad, can be both private and public

So what are cybersurveillance items? (cont'd)

- ▶ “by monitoring, extracting, collecting or analysing data”
- ▶ should be read broadly, includes all kinds of processing of data
- ▶ but does not include the destruction/manipulation of data

So what are cybersurveillance items? (cont'd)

- ▶ “from information and telecommunication systems”
- ▶ should be read broadly, includes computers and networks
- ▶ but “from” means that collecting “offline” data does not fall within the scope

So what are cybersurveillance items? (cont'd)

- ▶ “specially designed”
- ▶ WA 1996: “any object whose design includes particular features to achieve some particular purpose”
- ▶ WA 2007/2008: unknown
- ▶ this criterion has gained in importance due to open-ended nature of definition
- ▶ therefore we suggest to harmonize this concept in guidelines
- ▶ but what are “particular features” to achieve surveillance?

Specially designed for surveillance: ECHR and CJEU considerations

- ▶ ECHR and CJEU criteria for problematic surveillance are:
 - ▶ nature of data
 - ▶ nature of derived information
 - ▶ scale of surveillance
 - ▶ way data is processed
 - ▶ way data is accessed
 - ▶ security of the data

Application to certain technologies

This includes:

- ▶ Communications interception technologies (listed)
- ▶ Intrusion software (listed)
- ▶ Extraction software (listed)
- ▶ Cryptanalysis software (listed)

Application to certain technologies (cont'd)

But this does not include:

- ▶ Jamming equipment (listed) (not processing of data)
- ▶ Intrusion software modifying a system (listed) (not processing of data)
- ▶ Laser acoustic detection equipment (listed) (not “from”)

Application to certain technologies (cont'd)

And may include:

- ▶ AI for emotion and facial recognition
- ▶ Location tracking devices
- ▶ Open source intelligence software

Suggestions for clarification:

- ▶ Role of domestic laws (EU laws on biometric AI)
- ▶ Where the data comes from (only cameras - is that an information system, what about other sources?)

Grey area: obligation to do due diligence

- ▶ We argue that where it is unclear whether something is a CS item
- ▶ Organisations should perform due diligence to determine the capability of human rights infringement
- ▶ We suggest to provide harmonized guidelines for this as well

Summing up

- ▶ We suggest to clarify:
 - ▶ the term “specially designed”
 - ▶ that “surveillance” should be read in light of HR case law
 - ▶ that “covert” should be interpreted subjectively
 - ▶ that “from an information system” includes camera systems
 - ▶ the role of domestic laws in determining whether something is a CS item
 - ▶ that the CCP should be applied when determining HR infringements

Thank you!

[REDACTED] [REDACTED] [REDACTED]@uva.nl