Export control of cybersurveillance items in the new dual-use regulation

The challenges of applying human rights logic to export control

van Daalen, O.L.; van Hoboken, J.V.J.; Rucz, M.

DOI
10.1016/j.clsr.2022.105789

Publication date
2023

Document Version
Final published version

Published in
Computer Law & Security Review

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

Export control of cybersurveillance items in the new dual-use regulation: The challenges of applying human rights logic to export control

O.L. van Daalen, J.V.J. van Hoboken, M. Rucz*

Institute for Information Law, Roeterseilandcampus, Building A, 5th floor, Nieuwe Achtergracht 166, 1018 WV Amsterdam, the Netherlands

ARTICLE INFO

Keywords:
Export control
Cybersurveillance
Human rights
Location tracking
Facial recognition
Open source intelligence

ABSTRACT

In 2021, the Recast Dual-Use Regulation entered into force. The regulation includes a heavily debated new provision on the export control of so-called cybersurveillance items. This provision departs from the traditional logic of export control rules in multiple ways. Most importantly, it positions human rights considerations as an important factor in the export control of a flexible range of technologies. This article explores the operation, implications and challenges of this new human rights-orientated approach to export control of digital surveillance technologies. Taking the definition of cybersurveillance items as a starting point of the analysis, the article draws on surveillance-related case law of the European Court of Human Rights and the Court of Justice of the European Union, to define the potential scope of application of the open-ended cybersurveillance concept of the Regulation. By exploring how this concept maps to technologies often connected with human rights infringements, such as facial recognition, location tracking and open-source intelligence, the article highlights the challenges of applying this new approach and underscores the need for its further development in practice.

1. Introduction

In the summer of 2021, Amnesty International and Forbidden Stories revealed that hundreds of journalists, opposition politicians and human rights defenders in at least 20 different countries were targeted with Pegasus spyware, hacking software developed by the Israeli NSO Group.[1] Although this kind of software may have a legitimate use for law enforcement, the revelations highlighted once again that advanced digital surveillance capabilities can be used to commit serious human rights violations. The fact that NSO Group sold its services to regimes well-known for their repressive track record illustrated once again the weaknesses in attempts to regulate the international trade in these technologies - a trade which has created a lucrative market for high tech equipment, with

* Corresponding author: O.L. van Daalen Institute for Information Law, Roeterseilandcampus, Building A, 5th floor, Nieuwe Achtergracht 166, 1018 WV Amsterdam, the Netherlands.
E-mail address: o.l.vandaalen@uva.nl (O.L. van Daalen).

[1] Forbidden Stories, 'The Pegasus Project' https://forbiddenstories.org/case/the-pegasus-project/ accessed 1 April 2022; Stephanie Kirchgaessner accessed 1 April 2022.

https://doi.org/10.1016/j.clsr.2022.105789
0267-3649/

authoritarian regimes as eager customers. The revelations of the Pegasus Project led to renewed calls to tighten the governmental grip on the private surveillance industry.[2]

The timing of these calls coincided with the adoption of a legal instrument which was, in fact, aimed precisely at curbing the export of these kinds of tools. In 2021, the European Union (EU) amended its regulatory framework on export control, the Dual-Use Regulation.[3] In it, a new category of items is defined, "cyber-surveillance items", for which a new regulatory framework applies. In this new framework, human rights considerations play an important role. Export control rules traditionally focus on items which are described in a detailed, technical manner, enumerated in so-called control lists. This new category of cyber-surveillance items, however, is defined partly in non-technical terms – emphasising the capability for "surveillance", a concept strongly related to human rights. Moreover, while export control regimes have historically been aimed at mitigating military risks, the EU's new rules on export of surveillance technologies take human rights considerations as a primary justification for control, marking a shift in its normative grounding as well.[4]

This new, human rights-focused approach to export control will now have to be applied in the EU by the member states. It might also serve as inspiration for other countries, including those countries from which there currently is an active trade in surveillance tools like Pegasus. This is particularly pressing, because stories on export of surveillance tools to authoritarian regimes continue to be revealed, such as, relatively recently, a story on Nokia's technology internet surveillance technology being exported to Russia.[5] While academic literature has previously analysed how the integration of human rights considerations in the EU's export control regime raises normative tensions and exposes the difficulties of reconciling a free trade logic with a human rights logic, it remains underexplored how the EU's new cyber-surveillance export framework could operate in practice.[6] So, it is relevant to consider what the practical implications and challenges of the EU export control framework are, and what lessons we can draw for the development and application of similar rules at the international level.

We focus on these questions in this article.[7] We argue that while export control frameworks traditionally assess the need for export control based on the end-use and end-user of exported items, the new rules under the EU's Recast Dual-Use Regulation essentially introduce an additional relevant consideration, namely the *human rights infringing potential of a technology*. In this article, we unpack this new consideration. We identify criteria based on which such human rights infringing potential can be assessed. And we critically analyse how this would play out in practice, by applying this new consideration to three surveillance technologies that often receive scrutiny for their impact on human rights (facial and emotion recognition software, location tracking technologies and open-source intelligence software).

We start by discussing the background and genesis of the EU's new export control rules on cybersurveillance items in Section 2. Here, we trace the development of the new framework, starting from the multilateral Wassenaar Arrangement, through the making of the EU's Dual-Use Regulation, eventually leading to the adoption of tailor-made rules for the export control of cybersurveillance items. Section 3 zooms in on the definition of cybersurveillance items, as stipulated in Article 2(20) of the Recast Dual-Use Regulation, which is the essence of the new export control rules for surveillance technologies. We draw on surveillance-related human rights case law of European courts to define the scope of application of this provision. Section 4 then takes this definition and explores its application to three technologies which are not subject to international export control: facial and emotion recognition software, location tracking devices and open-source intelligence software. Based on this analysis, we subsequently highlight

[2] See e.g.: UN Office for the High Commissioner for Human Rights, 'Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech' (12 August 2021) https://www.ohchr.org/en/press-releases/2017/07/mexico-un-experts-call-independent-and-impartial-investigation-use-spyware?LangID=E&NewsID=21892 Accessed 1 April 2022; MENA Rights Group, 'Pegasus Project: End export of surveillance technology to MENA autocratic governments' (26 July 2021) http://menarights.org/en/articles/pegasus-project-end-export-surveillance-technology-mena-autocratic-governments Accessed 1 April 2022; Article 19, 'EU: Action needed to tackle spyware abuses after Pegasus revelations' (15 September 2021) https://www.article19.org/resources/eu-action-needed-to-tackle-spyware-abuses-after-pegasus-revelations/ Accessed 1 April 2022; Human Rights Watch, Access Now, Amnesty International, Committee to Protect Journalists and Reporters Without Borders, 'EU: Robustly Implement New Export Rules for Surveillance Tech' (8 September 2021) https://www.hrw.org/news/2021/09/08/eu-robustly-implement-new-export-rules-surveillance-tech accessed 1 April 2022.

[3] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast).

[4] See further: Machiko Kanetake, 'The EU's dual-use export control and human rights risks: the case of cyber surveillance technology' (2019) 3(1) Europe and the World: A law review.

[5] A. Satariano, P. Mozur, A. Krolik, "When Nokia Pulled Out of Russia, a Vast Surveillance System Remained", *New York Times* 28 March 2022.

[6] See e.g.: Machiko Kanetake, 'Dual-Use Export Control: Security and Human Rights Challenges to Multilateralism' (2021) 11 European Yearbook of International Economic Law 265; Machiko Kanetake, 'Converging Dual-Use Export Control with Human Rights Norms: The EU's Responses to Digital Surveillance Exports' in Elaine Fahey (ed.), Framing Convergence with the Global Legal Order (Hart Publishing 2020); Machiko Kanetake, 'The EU's dual-use export control and human rights risks: the case of cyber surveillance technology' (2019) 3(1) Europe and the World: A law review; Machiko Kanetake, 'The EU's export control of cyber surveillance technology: human rights approaches' (2019) 4(1) Business and Human Rights Journal 155; Fabian Bohnenberger, 'The proliferation of cyber surveillance technologies: Challenges and prospects for strengthened export controls' (2017) 4 Strategic Trade Review 81; Kim Heejin, 'Global export controls of cyber surveillance technology and the disrupted triangular dialogue' (2021) 70(2) International & Comparative Law Quarterly 379.

[7] This article is based on a study we performed for the Dutch Ministry of Foreign Affairs on export control of cybersurveillance items: O.L. van Daalen, J.V.J. van Hoboken, M. Koot and M. Rucz, "The new rules for exportcontrol of cyber-surveillance items in the EU", IViR 2021.

shortcomings of the EU's human-rights orientated approach and provide suggestions for future policy development.

2. The road to the EU's human rights-orientated export control of surveillance technologies

The latest update to the EU's Dual-Use Regulation came into force in September 2021, introducing a special export control framework for cybersurveillance items. The EU's Dual-Use Regulation finds its origins in the Wassenaar Arrangement, which predominantly aims at mitigating military risks, preventing the proliferation of weapons of mass destruction and maintaining international security. Throughout the last decade, calls to extend export control to surveillance technologies, not for military reasons but out of human rights considerations, grew louder, particularly bolstered by the abuse of surveillance technologies during the Arab Spring uprisings.[8] This eventually culminated in the recasting of the EU's Dual-Use Regulation. This section summarises these developments and provides the backdrop against which the new regulatory framework for cybersurveillance exports was later adopted.

2.1. *Wassenaar arrangement*

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA), serves as a basis for the EU's export control framework. It is the most important contemporary multilateral export control instrument (with currently over 40 participating states). Participants to the WA agree to control the export of specific items, which are described in an attachment to the WA, called the "control lists" - one for military items (the Munitions List), and one for items which can be used for military and non-military, or "civil" purposes (the Dual-Use List). The control lists to the WA contain detailed descriptions of items which the participating countries are obliged to place under export control via their national legislation. These lists are usually copied verbatim by the participating states in their relevant legislation. In the EU, the Munitions List is transposed nationally, and the Dual-Use List is transposed on the EU level.

2.2. *The dual-use regulation and its revision*

In the EU, the export control of dual-use items is regulated through the so-called Dual-Use Regulation. The Council already agreed in 1994 on EU-wide rules relating to the trade in dual-use items, even though the EU as such is not a participating entity to the WA (most of its member states are). These rules have since been updated and eventually resulted in the Dual-Use Regulation. The Regulation at a minimum transposes the lists under the WA. The European Union may, however, also provide for additional rules relating to the export of certain dual-use items. It did so with regard to the topic of this article – the export control of cybersurveillance items – in the Recast Dual-Use Regulation.

This amended regulation is the outcome of a decade-long revision process, with corresponding political debates largely revolving around whether and how to tighten restrictions on exports of surveillance technologies. After lengthy trialogue negotiations between the European Commission, the Council and the European Parliament, an agreement was reached in 2021. The Recast Regulation defines a new category of items, cybersurveillance items, and introduces a new regulatory framework for the export of these items. This definition is the focus of this article. Before we get to that, though, it is useful to provide an overview of the new framework which regulates these items, because this also clarifies what the role of the concept of cybersurveillance items plays in the new regulation.

2.3. *A new regulatory framework for export control of cybersurveillance items*

A first important distinction can be made between listed and non-listed cybersurveillance items under the Recast Dual-Use Regulation. Under the regulation, cybersurveillance items that have already been added to the control list in accordance with the WA, *listed items*, require an authorisation prior to export. The new regulatory framework, however, also applies to *non-listed* cybersurveillance items. These are items which fall within the scope of the term "cybersurveillance item" under the regulation, but are not on the list of specific items which require prior authorisation for export. Non-listed cybersurveillance items may be subject to an authorisation requirement in three scenarios.

First, non-listed cybersurveillance items are subject to such a requirement if the exporter is informed by the competent national authorities that the items in question "are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law."[9] Second, the Regulation imposes an obligation on exporters to notify national authorities if, on the basis of their own due diligence findings, they are aware that non-listed cybersurveillance items are or may be intended for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law.[10] The national authority shall then determine whether the export needs to be subject to authorisation. Third and finally, the Recast Regulation also grants member states the competence to adopt national legislation that triggers the authorisation requirement when the exporter has grounds for suspecting that an item may be used for these purposes.[11] What all these scenarios have in common, is that the application is very much contingent on

[8] See for example European Parliament Directorate-General for External Policies, 'After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy' (July 2012).

[9] Recast Dual-Use Regulation, Art. 5(1).

[10] Ibid., Art. 5(2).

[11] Ibid. Art. 5(3). When a member state imposes an authorisation requirement pursuant to any of these provisions, other member states and the European Commission shall be notified. If member states are notifying essentially identical transactions to each other, the Commission shall publish in the Official Journal of the

human rights considerations, as we will discuss in more detail below.

3. What is cybersurveillance?

This primarily follows from the scope of the definition of "cybersurveillance items" - a term defined in the new Dual-Use Regulation. Unfortunately, the text of the definition does not provide many clues, and as a result, many kinds of technologies are potentially subject to this new framework.

3.1. *Link between human rights and cybersurveillance in the dual-use regulation*

According to the Regulation, cybersurveillance items are "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".[12] Recital 8 specifies that the definition includes items "specially designed to enable the covert intrusion or deep packet inspection into information and telecommunications systems in order to conduct covert surveillance of natural persons by monitoring, extracting, collecting or analysing data, including biometrics data, from these systems".[13] Items, on the other hand, which are "used for purely commercial applications such as billing, marketing, quality services, user satisfaction, network security etc." are considered to generally not fall within the scope of the rules.[14]

Still, these explanations leave much room for interpretation, because some of the terms used in these recitals, such as "information and telecommunications systems" and "monitoring, extracting, collecting or analysing data", are also used in the definition itself. So we need to look at what clues the definition provides.

The definition contains four elements which are relevant for determining its scope. Two of these will not be discussed further here. These are the terms "covert" and "monitoring, extracting, collecting or analysing". We conclude in a report to the Dutch Ministry of Foreign Affairs on these new rules, that these two elements should be interpreted broadly, also in view of the intention to protect human rights with these new rules.[15] Surveillance should be considered "covert" with regard to a person, if that person does not know whether and how information on her is being used to target her specifically.[16] And the terms "monitoring, extracting, collecting or analysing" encompass a broad range of activities related to the collection and use of data on persons from certain systems.[17]

We argue that the two other elements read together, the terms "surveillance" and "specially designed", introduce a kind of export control which hinges on the *potential of the technology* for human rights abuse. Export control frameworks traditionally focus on the *end use* and the *end user*. Under the new framework for cybersurveillance items, the end use and end user remain relevant, but we argue that they are complemented by a new consideration: whether the items are specially designed for surveillance which interferes with human rights – in other words, the human rights infringing potential of a technology becomes relevant for the assessment. As an example: facial recognition cameras are not a listed item, which means authorisation for export is not automatically required. But as we demonstrate in our analysis below, the potential for human rights infringing surveillance of this technology implies that export might still be subject to authorisation under the new framework for cybersurveillance items.

3.1.1. *Interpretation of the term "surveillance"*

The term surveillance is not defined in the Dual-Use Regulation and has no commonly accepted meaning. Merriam-Webster defines it as: keeping a close watch over someone or something (as by a detective).[18] The Cambridge Dictionary defines it as: the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected.[19] In one book on surveillance studies, it is defined as "regard or attendance to others (whether a person, a group, or an aggregate as with a national census) or to factors presumed to be associated with these", where a "central feature is gathering some form of data connectable to individuals (whether as uniquely identified or as a member of a category".[20] And even "surveillance capitalism" is a thing now, referring to an economy which is based on the pervasive monitoring and manipulation of consumers through data.[21]

Because the new regulatory framework is aimed at protecting human rights, we suggest that for the Dual-Use Regulation, this term should be understood with reference to European human rights case law on surveillance.[22] For the European Union, the two most relevant instruments protecting human rights in that context are the European Convention for Human Rights (the Convention) and the Charter of Fundamental Rights (the Charter). And under those instruments, the rights to privacy and communications freedom are the most likely candidates for interference as a result of surveillance. Under the Convention, the right to privacy is protected (Article 8). Under the Charter, the right to privacy and the right to data protection are protected separately (Articles 7 and 8). Both instruments also protect the right to freedom of expression (Articles

European Union information regarding these cyber-surveillance items, to ensure a uniform application. Art. 5(6).

[12] Ibid., Art. 2(20).

[13] Ibid., Rec. 8.

[14] Ibid.

[15] Ot van Daalen, Joris van Hoboken, Matthijs Koot and Melinda Rucz, 'The new rules for export control ofcyber-surveillance items in the EU' (Report commissioned by the Dutch Ministry of Foreign Affairs, 2021) https://www.ivir.nl/publicaties/download/Report-on-cybersurveillance-items.pdf accessed 1 April 2022.

[16] Ibid., 18.

[17] Ibid., 18-19.

[18] Merriam Webster, 'Surveillance' https://www.merriam-webster.com/dictionary/surveillance accessed 1 April 2022.

[19] Cambridge Dictionary, 'Surveillance' https://dictionary.cambridge.org/dictionary/english/surveillance accessed 1 April 2022.

[20] Gary T. Marx, 'Surveillance Studies' (2015) 23 International Encyclopedia of the Social & Behavioral Sciences, 2nd ed.

[21] Shoshana Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (Profile Books 2019).

[22] The Dual-Use Regulation also speaks of surveillance of "natural persons", which further underlines that it the new rules are intended to protect human rights.

10 and 11 respectively). There are also other rights which are likely to be affected as a result of surveillance, such as the prohibition of discrimination (Articles 14 and 21 respectively), and the right to freedom of assembly (Articles 11 and 12 respectively). The analysis for those rights, however, will be more or less the same, so we will not focus on those rights.

The European courts have over the past decades used the term surveillance in a variety of settings. The European Court of Human Rights in the seminal *Klass* case reviewed certain German "surveillance measures", which allowed the government to open and inspect mail and post, read telegraphic messages, and listen to and record telephone conversations – communications surveillance, in other words.[23] Since then, the Court has repeatedly used the term to review various types of privacy-infringing measures. In *Leander*, it considered the classification of someone as a security risk in a register as a form of surveillance.[24] Similarly, in *Rotaru*, the Court assessed the maintenance of a secret register on someone, under the framework it developed for secret surveillance, specifically classifying the gathering and keeping of personal information as a form of surveillance.[25] The Court has further referred to posting at someone's house as a form of "visual" surveillance, and evaluated the installation of a listening device on a suspect's premises under its surveillance review framework.[26] More recently, in *Uzun*, it has considered location tracking with a GPS-device a form of surveillance (but concluded that the strict framework for reviewing communications surveillance was not appropriate for covert location tracking).[27] It has also reviewed surveillance by private entities, for example assessing the monitoring by an employer of the communications of an employee under the framework first developed in *Klass*.[28] And it has even provided guidance on the review of legislation of the use of "video"-surveillance by employers and in detainees' cells.[29] The European Court of Justice has not had the chance to rule on a similar number of cases on this topic, but where it did, it uses the term "surveillance" also in a broad way.[30]

It can therefore be concluded that the term "surveillance" in the Dual-Use Regulation, when read in light of European human rights law, refers to a broad range of activities related to the gathering and processing of information on individuals. It can from the result of government activities, but also of private actors, or a combination of both. This is particularly relevant because in the past, it has been difficult to assess who is behind the use of a certain tool: there are various examples of surveillance tools being used by private organisations, where it is not always clear whether there is a link with a government.[31] And to be clear: surveillance in this context is not necessarily *unlawful*. It could be that surveillance with a certain tool, when applied by a particular end user, should be considered lawful, while the export of the tool is nevertheless subject to export control. It would merely mean that the item is subject to the regulatory framework set out above.

Now, not only is the term "surveillance" very much connected to human rights – it must be read in conjunction with the other term, "specially designed". And as it turns out, human rights are also important for interpretation of that term.

3.1.2. *Interpretation of the term "specially designed"*

The term "specially designed' is not a new term in export control. In the WA and its predecessors, it is used abundantly.[32] These terms have been explicitly defined in the Guidelines for the Drafting of Lists under the WA in 1996, which was later revised in 2007/2008.[33] Under the 1996 Guidelines, "specially designed" means "any object whose design includes particular features to achieve some particular purpose. This will typically involve extensive research and development activity." This is juxtaposed to the term "designed", which means "any object whose design is general in nature to achieve some particular purpose. Typically extensive research and development will not be involved." There are also more recent Guidelines from 2007/2008, but these have not been made publicly available.

It is unfortunate that there is no further guidance on the term "specially designed". The term was already important for the interpretation of listed items, but will gain even more significance in the context of the new rules on cyber-surveillance items. This is because traditionally, items on control lists have been defined in a detailed, technical way: export control lists provide precise specifications of the kinds of technologies which are subject to regulation. For those kinds of items, there is only a limited role to play for the design-criterion to distinguish between controlled and non-controlled items.

But, as noted above, the definition of cyber-surveillance items under the Dual Use-Regulation is open-ended, focusing on the *function* of these tools (surveillance), not their specifications. This increases the importance of the design-criterion, in order to distinguish between technologies which *in theory* can be used for surveillance, and those which have actually been built with that goal in mind. This underscores the importance of understanding the scope of this term.

[23] *Klass v Germany* App no 5029/71 (ECtHR, 6 September 1978), para. 17.

[24] *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987), para. 60.

[25] *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000), paras. 47, 57. See later: *Segerstedt-Wiberg v Sweden* App no 62332/00 (ECtHR, 6 June 2006).

[26] *P.G. and J.H. v the United Kingdom* App no 44787/98 (ECtHR, 25 September 2001), para. 37; *Khan v the United Kingdom* App no 35394/97 (ECtHR, 12 May 2000), para. 22.

[27] *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010), para. 66; *Ben Faiza v France* App no 31446/12 (ECtHR, 8 Februari 2018).

[28] *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017), para. 120.

[29] *López Ribalda and others v Spain* App no 1874/13 and 8567/13 (ECtHR, 17 October 2019); *Gorlov and others v Russia* App no 27057/06 and 2 others (ECtHR, 2 July 2019).

[30] C-623/17 *Privacy International* (CJEU, 6 October 2020), para. 71; C-203/15 and C-698/15 *Tele2* (CJEU, 21 December 2016), para. 100; C-293/12 and C-594/12 *Digital Rights Ireland* (CJEU, 8 April 2014), para. 34.

[31] See for example the investigations of CitizenLab into the use of intrusion software in Mexico: Citizen Lab, 'Posts tagged "Mexico"' https://citizenlab.ca/tag/mexico/ accessed 1 April 2022.

[32] See the Revised List of Goods Subject to Embargo 1958: https://www.scribd.com/document/19647281/CoCom-Lists-1958 accessed 1 April 2022.

[33] Reproduced in Appendix G. See: https://core.ac.uk/download/pdf/288283595.pdf accessed 1 April 2022.

Assuming the WA Guidelines have not changed since 1996, this would mean that items which are "specially designed" to enable the covert surveillance of natural persons, are items whose design includes "particular features to achieve" such surveillance. And given that "surveillance" should be interpreted in light of European human rights case law, we argue that these "particular features" in this case must be reviewed against the rights to privacy and communications freedom. But of course, this still leaves much room for debate – so what design factors can be considered relevant in this assessment? That is the topic of the next section.

3.2. *Towards design criteria of cyber-surveillance technologies*

As noted above, the Convention case law on surveillance goes back decades, starting with the *Klass* case of 1978. The Court in this case outlined two basic principles which have since become the bedrock of European fundamental rights case law on surveillance. First, it is not only the application of these measures to individual persons which affects the rights to privacy and communications freedom, but also the "menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services".[34] And second, the Court noted that secret surveillance is allowed under certain circumstances, but, "being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".[35] Central to the assessment what measures are "appropriate", the Court requires that "whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse".[36]

Since then, this starting point has been worked out in numerous decisions (see also the cases mentioned in the section above). The most relevant decision of the European Court of Human Rights is *Zakharov*, in which the Court summarised its earlier body of case law on surveillance measures.[37] In short, the resulting assessment firstly tests whether the measures are set out in sufficient detail.[38] The Court secondly tests whether the measures are necessary in a democratic society and proportionate to the legitimate aim pursued, which depend on all the circumstances of the case, such as the nature of the measures and the oversight in place.[39] Around the same time, the European Court of Justice also started issuing decisions on surveillance measures.[40]

Together, these courts have in the past decades developed a number of criteria relevant to proportionality assessment of these measures.[41] For our purposes, those criteria which have a potential bearing on the technology are most relevant. Other criteria for the assessment of human rights violations developed by the Courts, such as whether surveillance powers are sufficiently circumscribed and their application is supervised by a court, have more to do with the rules in place, and less with the technology being used. These criteria relating to technology obviously depend on the context – for example, different criteria may be relevant for bulk surveillance of communications than for targeted location surveillance. Still, we argue that it is possible to derive a non-exhaustive list of relevant criteria from the case law of the European Court of Justice and the European Court of Human Rights (cited above and below), which would include the following considerations.[42]

First, the nature of the data collected is relevant. Although the processing of all types of personal data triggers the protection of the right to privacy, the more sensitive the data that is collected, the more serious the interference is considered to be under the Charter and Convention.[43] And when it comes to the collection of special categories of data as defined in Article 9 of the General Data Protection Regulation, such as data relating to racial or ethnic origin or genetic data, this will be considered very problematic very quickly. In respect of the nature of the data collected in the case of communications surveillance, both courts also distinguished between surveillance of the content of communications and surveillance of communications metadata. The surveillance of the content of communications has in the past been considered more problematic than the monitoring of communications metadata. However, this does not mean that surveillance of communications metadata is necessarily harmless. When metadata such as location data, Internet browsing activity and communication patterns are systematically monitored, the interference may

[34] *Klass v Germany* App no 5029/71 (ECtHR, 6 September 1978), para. 41.
[35] Ibid., para. 49.
[36] Ibid., para. 50.
[37] *Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015). See for other relevant decisions for example *Big Brother Watch* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021); *Centrum för Rättvisa v. Sweden* App nos 35252/08 (ECtHR, 25 May 2021); *S. and Marper v United Kingdom* App nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008);
[38] Ibid., para. 231.
[39] Ibid., para. 232.
[40] See for example CJEU 8 April 2014, Cases C-293/12 and C-594/12 (*Digital Rights Ireland*); CJEU 26 July 2017, Opinion 1/15 (*PNR data*); CJEU 16 July 2020, Case C-311/18 (*Schrems II*); CJEU 6 October 2020, Cases C-511/18, C-512/18 and C-520/18 (*La* Quadrature); CJEU 6 October 2020, Case C-623/17 (*Privacy International v. United Kingdom*); CJEU 21 June 2022, Case C-817/19 (*Belgian PNR data*).
[41] See also the case law under Section 3.1.1.
[42] Two other criteria - the way the data is accessed and how it is secured – depend strongly on the implementation of the technology. It can be assumed that many of the items which fall in these categories are set up in such a way that access is relatively circumscribed. In addition, given the context of these technologies, it can be assumed that many of these technologies must adhere to strict security requirements. These factors will, in other words, not be useful in distinguishing between items which are subject to the new framework, and those that are not.
[43] See for example for the CJEU the considerations in *Digital Rights Ireland, Schrems I, Schrems II* and *Opinion 1/15*, and for the ECHR the considerations in *Zakharov, Big Brother Watch, S. and Marper* and *Uzun* discussed above.

even be more serious than when content of communications is the target of surveillance.[44]

Second, the nature of the information derived from the data collected is relevant. When the data collected is not sensitive itself, but there is a potential that sensitive information can be inferred from it, the interference with the right to privacy will furthermore be considered more serious. In this respect, the European Court of Human Rights for example emphasised that when there is a possibility to draw inferences as to ethnic origin, the surveillance practice will be considered particularly problematic.[45]

Third, the scale of surveillance should be considered relevant. The greater the scale of a surveillance practice, and thus the more personal data collected, the more problematic it is from a privacy perspective, and the more pressing the need for adequate guarantees safeguarding against abuse.[46] Indiscriminate, bulk surveillance has been considered a particularly serious interference. For example, the European Court of Justice considers the untargeted retention of communications data for the purpose of fighting crime to be disproportionate.[47] Targeted data retention for fighting crime can on the other hand be compatible with the Charter if the authority is sufficiently clear and there are sufficient safeguards against abuse.[48] And indiscriminate data retention can be ordered for a limited period of time to protect national security.[49] Targeted surveillance, however, does not necessarily constitute a less serious interference and its necessity and proportionality need to be assessed along the other criteria.

Finally, the automated processing of data is a relevant criterion. A surveillance practice is considered more serious when the collected data is processed through automated means. Because automated processing allows authorities to go "well beyond neutral identification" and make inferences that would otherwise not be possible, it has been asserted by both courts that the implementation of adequate safeguards is particularly important when automated processing is used to analyse the collected information.[50]

We argue that these criteria which have historically been important in determining whether surveillance should be considered proportionate, are also relevant in determining whether certain technology should be considered "specially designed" for surveillance within the meaning of the Recast Dual-Use Regulation. The reason for this conclusion, as set out above, is that the prevention of human rights infringements play an important role in the export control of cybersurveillance technologies. Now, just to be clear, simply because some technology should be considered specially designed for surveillance, its export must not necessarily be prohibited. The consequence of something being considered a cybersurveillance item under the Dual Use Regulation is that the special regulatory framework for export control applies, which also means that under circumstances an authorisation for export is required.

So, how does this theory of applying the "specially designed" criterion through the lens of the proportionality assessment in human rights case law work in practice? That is the topic of the next section, in which we assess whether a number of potential surveillance tools fall within the scope of the new cyber-surveillance rules of the Dual Use Regulation. Doing so also allows us to highlight a number of challenges in its application.

4. Challenges of export control of cybersurveillance technologies

We will now discuss three non-listed technologies which may be subject to the new regulatory framework, depending on whether they should be considered cybersurveillance items: facial and emotion recognition technologies, location tracking devices and open source intelligence software. These three types of technologies have been selected for analysis because they represent a diverse range of surveillance tools and there have been calls to curtail their export for human rights reasons. At the same time, this small selection already allows us to illustrate the complexities in applying the new rules - in particular under which circumstances these technologies should be considered to be "specially designed" for surveillance under the definition of cybersurveillance items under the Dual Use Regulation.

4.1. *Potential cybersurveillance technologies*

4.1.1. *Facial and emotion recognition technologies*

Facial and emotion recognition technologies analyse images of faces, sometimes collected with cameras in the system, trying to detect the identity and emotions of the persons whose images are captured. These technologies have advanced quite rapidly in the past years, and now allow for the rapid detection of people within large datasets. Some of applications of these technologies do not interfere with human rights: you can for example use facial recognition technology to unlock your phone. But others are a more serious candidate for being considered cybersurveillance items.

The use of these technologies in China demonstrates their human rights-infringing potential. As reported by the New York Times, facial recognition technology has been deployed on a mass scale to identify and track individuals belonging to the Uighur minority in certain parts of China.[51] The purpose of the use of facial recognition is to try identify "unsafe"

[44] *Big Brother Watch* App no 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018), para. 356; *Digital Rights Ireland*, paras. 26-27.

[45] *S. and Marper v the United Kingdom* App no 30562/04 and 30566/04 (ECtHR, 4 December 2008), para. 76.

[46] *M. M. v the United Kingdom* App no 24029/07 (ECtHR, 13 November 2012), paras. 199-200.

[47] *Digital Rights Ireland*, *Tele2*.

[48] *Tele2*, para. 109.

[49] C-511/18, C-512/18 and C-520/18 *La Quadrature* (CJEU, 6 October 2020).

[50] *Privacy International*, par. 68; *La Quadrature du Net*, par. 132; *Marper*, para. 75; *Digital Rights Ireland*, para. 55; *Opinion 1/15* (CJEU, 26 July 2017), para. 141.

[51] Paul Mozur, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority' (New York Times, 14 April 2019) https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html accessed 1 April 2022.

actors who are then potentially sent to detention centres.[52] Thus, facial recognition applied to footage in public spaces has the potential to lead to mass surveillance and ethnic profiling, resulting in serious interferences with the right to privacy (due to the indiscriminate nature of surveillance and the highly sensitive nature of ethnic data). It can also pave the way for unlawful discrimination and subsequent human rights abuses (such as unlawful detention).

Emotion recognition technologies can raise further human rights concerns. This kind of technology was deployed for migration control under the EU's iBorderCTRL project between 2016 and 2019. Under this project, people entering a country (Greece, Hungary and Poland took part in the project) were asked certain questions with a camera recording their face while answering. The recording was then analysed with emotion recognition software, with the apparent aim of assessing whether the relevant subjects were deceitful or not. The project has been widely criticised for its lack of accuracy and its potential to lead to unlawful discrimination.[53] A more fundamental concern is that deception detection may be at odds with the right to non-self-incrimination.

The use of such technologies, especially in public spaces, may raise significant human rights concerns due to their indiscriminate nature, and these concerns are only amplified by the sensitive nature of facial biometric data. We discuss later in this section how the "specially designed" criterion applies to these kinds of technologies.

4.1.2. *Location tracking devices*

Another technology which is a good candidate to be considered a non-listed cybersurveillance item are location tracking devices. These allow tracking of the physical location of a device over time. While facial and emotion recognition technologies may be relatively recent inventions, location tracking technologies have already been in use for quite some time by law enforcement and intelligence agencies: attaching a beacon to a vehicle is for example already being done for decades. However, as smartphones have become ubiquitous and tracking technologies have become more advanced, this has become much easier to do, also at scale. There are various ways of tracking your location – with your phone, through cellphone towers and via wifi routers for example. Location is a sensitive category of data to collect, as it reveals a lot about behaviour, and, similar to your face and expression, cannot be easily faked.

Non-problematic uses of location are finding a lost device, as Apple for example offers, tracking your pet and navigation software. But given the information which can be gleaned from this data, governments and companies also take a keen interest in this information and their ability and capabilities to collect it. In fact, even Apple's functionality of finding things with an AirTag has been demonstrated to be used to stalk people.[54] Law enforcement agencies use it to collect evidence in the course of an investigation. This will generally be targeted. And intelligence agencies also use it to track suspects and to reveal links between different persons in the same location. The NSA reportedly collected 5 billion phone records daily, which included locations of devices – and hence users – based on cell-id's and identified links between users on the basis of that location.[55]

Companies also are known to use location tracking for commercial purposes. There are companies who use it to provide reports on aggregated movement patterns, for example in shopping streets. There are also companies which use the data for more targeted purposes. Employers use it to track their employees who are working off-site.[56] And location-based advertising is already being touted as the next innovation in marketing, allowing advertisers to present an advertisement for a certain clothing brand to a smartphone user when this person is at near a store of the brand.[57] One US-based firm even touts it can provide real-time locations of specific cars in nearly any country on Earth to its customers.[58]

Using location data for commercial or state purposes may also raise serious human rights concerns. Although there are situations where this can be considered proportionate, these must be surrounded by significant safeguards.

4.1.3. *Open-source intelligence software*

A final candidate technology which can be considered relevant is open-source intelligence software. Open-source intelligence (OSINT) refers to the domain of intelligence produced through the collection and analysis of information from sources that are freely accessible to any person or organization, either through paid (commercial) or unpaid channels. Most of the information in OSINT nowadays comes from digital sources, such as online social media, satellite imagery, real-time camera footage, and leaked, dumped or commercially

[52] Darren Byler, 'China's Hi-Tech War on its Muslim Minority' (The Guardian, 11 April 2019) https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition accessed 1 April 2022.

[53] Natasha Lomas, ''Orwellian' AI Lie Detector Project Challenged in EU Court' (Tech Crunch, 5 February 2021) https://techcrunch.com/2021/02/05/orwellian-ai-lie-detector-project-challenged-in-eu-court/ Accessed 1 April 2022; Umberto Bacchi, 'EU's lie-detecting virtual border guards face court scrutiny' (Reuters, 5 February 2021) https://www.reuters.com/article/europe-tech-court-idUSL8N2KB2GT Accessed 1 April 2022.

[54] A. Matei, "I was just really scared: Apple AirTags lead to stalking complaints", *The Guardian* 20 January 2022.

[55] See the NSA's Co-Traveler programme revealed by Snowden: Barton Gellman, 'NSA tracking cellphone locations worldwide' (The Washington Post, 4 December 2013) https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html accessed 1 April 2022.

[56] See the numerous articles on the "best" apps for employee tracking. See e.g.: Aigerim Berzinya, 'A Complete Guide to the Top Ten Employee GPS Tracking Systems' (Turtler, 1 September 2020) https://turtler.io/news/a-complete-guide-to-the-top-ten-employee-gps-tracking-systems accessed 1 April 2022.

[57] See e.g.: 'Complete Guide to Location-Based Advertising (LBA) in 2021 – Geo-Targeting, Geo-Fencing, Geo-Conquesting, Proximity Targeting' (Knorex, 2021) https://www.knorex.com/blog/articles/location-based-advertising-2 accessed 1 April 2022.

[58] Joseph Cox, 'Cars Have Your Location. This Spy Firm Wants to Sell It to the U.S. Military' (Vice, 17 March 2021) https://www.vice.com/en/article/k7adn9/car-location-data-telematics-us-military-ulysses-group accessed 1 April 2022.

available databases, including data brokers. And while much intelligence is still produced by persons manually browsing through online databases, since the information is in digital form, it has also become increasingly easy to conduct software-based automated collection and analysis of these sources, in real-time and at scale.

Given the broad range of data which can be harvested and analysed online, the potential for abuse is significant. Some of the use may be less problematic - not entirely unproblematic, though. For example, software for sentiment analysis is becoming increasingly popular as a tool for companies to understand their (potential) customers. This software may automatically analyse opinions and emotions on social media, such as Twitter on a broad scale. A company can then use this information to optimize its product or service and adapt its communication strategy. This application can already raise concerns, for example when a company uses the insight not to improve its offering but instead merely steers the online conversation away from its flaws.

Whensentiment analysis is used for political purposes, its use rapidly becomes problematic from a human rights perspective. A government can, for example, check public posts on Facebook and Twitter to quickly identify people organising protests against a regime and then arrest those people. It can also use posts as evidence of participation in protests and use it to prosecute protesters. This latter application will use facial recognition software as part of the analysis. One paper presents a system "to identify and characterise public safety related incidents from social media, and enrich the situational awareness that law enforcement entities have on potentially unreported activities happening in a city", demonstrating its "usefulness in detecting, from Twitter, public safety related incidents occurred in New York City during the Occupy Wall-Street protests".[59]

4.2. *Issues regulating cybersurveillance technologies*

Whether these technologies actually fall within the definition of cyber-surveillance items in the Recast Dual-Use Regulation, depends on a number of factors. One important question is whether their design includes particular features to achieve covert surveillance. The criteria we identified in Section 3.2. are particularly relevant for this assessment. We argue that the three technologies analysed above generally meet most identified criteria, and thus, will in most cases be considered cyber-surveillance items for the purposes of the Recast Dual-Use Regulation.

In all cases, the nature of the data collected or inferred from it is sensitive, if not highly sensitive. This goes for location data – which can reveal much about your life (where you live, where you work, who your social contacts are, etc.). It goes for facial data – this is considered biometric data under the General Data Protection Regulation (GDPR) and treated as highly sensitive, if only because it can identify you and you have no choice but to expose your face when in public.[60] Of course, this also applies to emotional data, which can reveal your inner emotional state, something which many will consider to be highly sensitive. Lastly, this arguably also applies to much of the data collected via open source intelligence software. Although this obviously is less sensitive because you will often have chosen intentionally to reveal the data in public, it is not always intended that this data is harvested at scale and repurposed. In addition, other, more sensitive conclusions may be inferred from this data.

This also touches on two other criteria we described above for determining whether an item is "specially designed" for surveillance: scale and automation. Often, these technologies are intended to be deployed at scale and via automated means. This goes particularly for open source intelligence software, which derives its value from harvesting large amounts of data from public sources and analysing this automatically. But this will generally also apply to location tracking technologies, which – depending on the kinds of technologies - are often used to track many people at once, not only particular individuals. Of course, one can imagine that particular technologies are simply impossible to apply at scale – think for example of Apple's Airtag tracking technology, which is designed to be used on particular objects. Facial and emotion recognition technology is also generally applied at scale and via automated means: in many cases, these are intended to be used in public spaces to identify and monitor many people simultaneously. Again, this may be different where the technology simply does not work this way: one can for example imagine that a technology can only be used at one person at a time.

So, in conclusion, the three kinds of technologies described above can arguably all be considered cybersurveillance items in specific cases. But it remains difficult to apply the new regulatory regime to these, and similar technologies. This is because the regulatory framework for cybersurveillance items focuses on the *function* of technologies, while digital technologies rarely have only one function.

First, many of these technologies are modular in nature. They consist of a combination of software and hardware from different vendors, with the components themselves often being relatively innocuous. Take emotion recognition systems: these are composed of cameras, storage devices, database software, processing units and analysis software. Most of these elements – except perhaps for the analysis software – are general-purpose: they can be used to assist the Chinese government in rounding up Uyghurs, but they can also be used to keep track of the development of a banana cake in your oven. And for the analysis element – even that element in itself can be used for different purposes – for lie detection of suspects, for example, or for checking the reaction of a person at a consumer panel with consent.

So, when do you consider something a cybersurveillance item, when all elements in isolation are not? This, again, boils

[59] Michele Berlingerio, Francesco Calabrese, Giusy Di Lorenzo, Xiaowen Dong, Yiannis Gkoufas and Dimitrios Mavroeidis, 'SaferCity: A System for Detecting and Analyzing Incidents from Social Media' (2013) 2013 IEEE 13th International Conference on Data Mining Workshops 1077.

[60] Regulation (EU) 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), Art. 9(1).

down to the "specially designed" requirement: does the design have particular features for performing surveillance? One could argue that only the analysis and user interface element of such a system can be considered to have those particular features, for example to target particular groups. This means that the other elements, if exported in isolation, are not subject to export control. This is not particularly problematic: general purpose technologies should not be subject to export control. But when devising and enforcing international regulations for surveillance technologies, it is something to remain aware of. One way to draw the distinction between regulated and non-regulated items could be to determine whether an element is "essential" to achieving the surveillance, or whether a similar item with different technological specifications could also be used. This still leaves a lot of room for debate on where to draw the line.

A second issue with regulating these kinds of technologies is their flexibility. As a software developer, you could for example build in measures to restrict the use of your software. Say you have facial recognition software which you only want to be used to automatically grant entry at a building, and not for rounding up Uyghurs. Then you could perhaps limit the number of matches which can be done per day. However, if a customer can easily increase this limit once the technology is in their hands, this really does not prevent the human rights-infringing use. The more fundamental question is whether a manufacture can take security measures to make sure that something is not "specially designed" for surveillance. We are sceptical, since security measures – for example in digital rights management – have been widely circumvented in the past. It would be good to also take this into consideration when devising an international regulation to this effect. We suggest that the concept of "effectiveness" of security measures is the most important factor here: a measure should be considered effective, where it makes it in practice impossible for the end-user to change the function.

5. Conclusion

As the European Parliament launched a committee of enquiry to investigate the Pegasus revelations in March 2022, the question of how to adequately address the international trade in intrusive cybersurveillance technologies remains high on policy agendas.[61] The new regulatory framework for export control of cybersurveillance items, introduced by the Recast Dual-Use Regulation, gains particular importance in this context, and may also serve as inspiration for similar export controls on an international level, primarily via the Wassenaar Arrangement. But if this were to happen, it is useful to clarify a number of things.

Firstly, we have argued this definition should be interpreted in line with human rights case law on surveillance. We have clarified on the basis of this case law that a number of factors can be relevant in determining whether an item can be considered "specially designed" for surveillance: the nature of the data which is processed and inferred, as well as the scale and automation are the most relevant factors.

At the same time, we have underlined two challenges which result from the new approach taken in the Recast Dual-Use Regulation. As mentioned above, the definition centres around the *function* of an item, not its technical specifications. Because cybersurveillance items consist of digital technologies, this *function* is not fixed.

Most technologies are, in essence, a computer with some software elements which can also be used for other purposes and which can be exported in isolation. We suggest that one way of dealing with this, is by introducing the concept of technologies which are "essential" to achieving the goal of surveillance. It should be clarified that only those technologies must be subject to export control, whereas non-essential technologies, such as CPUs or memory, will not be subject to export control.

Moreover, even if one were to restrict the use of a certain system to prevent human rights infringements – in other words, to limit its function - these measures can generally be easily circumvented. One way of dealing with this flexibility is by assessing whether the security measures taken to restrict the functionality are "effective" - which means they are in practice impossible for the end user to circumvent.

Authorship conformation form

All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version. This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.

Declaration of Competing Interest

The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript.

Data Availability

No data was used for the research described in the article.

[61] European Parliament, 'Three new committees on Pegasus spyware, foreign interference and COVID-19' (European Parliament Press Room, 10 March 2022) https://www.europarl.europa.eu/news/en/press-room/20220304IPR24801/three-new-committees-on-pegasus-spyware-foreign-interference-and-covid-19 accessed 1 April 2022. See also: Zack Whittaker, 'European lawmakers launch investigation into use of Pegasus spyware by EU states' (Techcrunch, 11 March 2022) https://techcrunch.com/2022/03/11/europe-pegasus-investigation/ accessed 1 April 2022.