Recasting the Dual-Use Regulation – Digital Surveillance Technology, Human Rights, Due Diligence and Transparency

Trampert, J.

Publication date
2021

Document Version
Final published version

State responsibility **01.01.2021** **Joëlle Trampert**

Recasting the Dual-Use Regulation – Digital Surveillance Technology, Human Rights, Due Diligence and Transparency

Last November, the European Parliament and Council reached a provisional agreement on the final compromise text for the amendment of Council Regulation 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items ('Dual-Use Regulation'). Six years ago, the Parliament, Council and Commission published a joint statement, acknowledging 'the issues regarding the export of certain information and communication technologies (ICT) that can be used in connection with human rights violations (...)'. This blog post considers four noteworthy elements of the Recast Dual-Use Regulation, which has been endorsed by the Permanent Representatives Committee in November and will likely enter into force next spring.

I. The Problem – an Example

A recent report by Amnesty International on the export of digital surveillance technologies from EU Member States to the People's Republic of China ('PRC') has illustrated how China is using state of the art cyber surveillance equipment to keep track of and target certain members of the population, predominantly the Uighur, often resulting in egregious and systematic human rights abuses. Ms. Markéta Gregorová MEP explicitly highlighted the link between these abuses and the European digital surveillance tech industry in her speech at the EU's 2020 Export Control Forum on 11 December: under the current rules, European companies can sell digital surveillance technology to the PRC 'as if they are trading with New Zealand. When exposed and questioned, they deny knowing anything and do not fear any consequences.' This is obviously problematic.

The PRC's human rights track record with respect to the Uighur and other Turkic minority peoples has been a cause for concern for a considerable period of time. In 2018, the UN Committee on the Elimination of Racial Discrimination ('CERD') noted the '[n]umerous reports of the detention of large numbers of ethnic Uighurs and other Muslim minorities, held incommunicado and often for

long periods, without being charged or tried, under the pretext of countering religious extremism' [Concluding observations §40(a)]. The CERD also specifically voiced its alarm on the reported use of 'mass surveillance disproportionately targeting ethnic Uighurs, such as frequent baseless police stops and the scanning of mobile phones at police checkpoint stations (...) [and the] collection of extensive biometric data in [Xinjiang], including DNA samples and iris scans, of large groups of Uighur residents' [§40(b)]. China's use of digital surveillance technology to track and control the general population has expanded in recent years. Besides averting toilet paper theft in Beijing's public bathrooms, the PRC has further developed the surveillance network to prevent and even predict threats to national security. The Uighur population is viewed as such a threat, and under the guise of 'national security' and 'counter-terrorism', individuals belonging to this group are spirited away to secret camps where detainees are subjected to 're-education', sham trials and forced labour. Uighur people have allegedly been subjected to medical testing and forced sterilisation, and historic mosques in Xinjiang have been destroyed. Last year, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also paid specific attention to the PRC's use of surveillance cameras and facial recognition to track the Uighur population and record their every move [Report §12] and called for an immediate moratorium on the global sale and transfer of such items [§48-49]. Facial recognition technology, a type of artificial intelligence ('AI'), does what the name suggests: it detects a person's facial characteristics and identifies markers such as gender, age, and ethnicity. The focus on ethnicity is particularly disturbing here, as it enables racial profiling by the PRC government.

Modern technologies such as AI used by the PRC are, at best, exacerbating a climate of oppression, and, at worst, connected to crimes against humanity and genocide. Of course, many of these technologies are made in China, but recent studies have shown that other States are providing the PRC with these goods too. The issue is that under the current export control regime, this is not unlawful.

II. The Regulatory Gap

Amnesty International has identified several European companies which have exported digital surveillance technology to government agencies in the PRC for use in major indiscriminate mass surveillance projects, which, in turn, are connected to the repressive State policy described above. For those interested in the details, I refer to Amnesty International's report, but it is important to bear in mind that the companies exporting these technologies to the PRC – and to other repressive regimes for that matter – were under no binding legal obligation to apply for an export licence. Likewise, the States in question were under no binding legal obligation to review the export. The reason is fairly simple: the current Dual-Use Regulation defines 'dual-use items' as 'items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices' (Article 2(1)). This civil-military dichotomy means that items which are not used for activities which are strictly 'military' in nature, such as cyber technologies used to surveil the population for 'law enforcement' purposes, currently fall outside the scope of the Regulation. Article 4 of the 2009 Dual-Use Regulation provides a so-called 'catch-all clause', which dictates that *an authorisation shall be required* for the export of dual-use items not listed in Annex I if the exporter has been informed by a Member State's competent authorities that the items in question are or may be intended, in their entirety or in part, for use in connection with weapons of mass destruction; if

the purchasing country or country of destination is subject to an EU, OECE or UN arms embargo and if the exporter has been informed by the authorities that the items in question may be intended for a military end-use; or if the items in question may be intended for use as parts or components of military items that have previously been exported without or in violation of an authorisation prescribed by national legislation of that Member State. Outside of these three situations, Article 8(1) provides a final option: States *may prohibit or impose an authorisation requirement* on the export of dual-use items not listed in Annex I for reasons of public security or human rights considerations. As touched upon in a previous blog post, this is by no means sufficient, as there is little incentive for a State to impose trade restrictions on a highly profitable company domiciled within its jurisdiction. Applying the current framework to digital surveillance technology, it is not hard to see how such goods can flow from the EU to States such as the PRC where they are used in situations which infringe on human rights in a completely unregulated manner.

III. The Proposal and the Final Compromise Text

The Dual-Use Regulation was never meant to remain static or absolute (see Article 25, second paragraph, Dual-Use Regulation). In 2016, the European Commission submitted a proposal for a recast version ('Proposal') and last November, the European Parliament and Council published the provisional agreement on the final compromise text ('Compromise Text'). I have selected four points worth considering in more detail in relation to digital surveillance technology exports to the PRC: the definition of dual-use goods, the increased attention for human rights risk assessments, the notion of exporter due diligence and the push for greater transparency.

1. The definition of dual-use goods and the catch-all clause

The current Dual-Use Regulation stipulates that '[a]n authorisation shall be required for the export of the dual-use items listed in Annex I' (Article 3(1)). Recent technological developments, or the way they have been deployed, have exposed a major weakness here: even if certain goods are connected to human rights abuses, there is not a single export control requirement for goods not covered by Annex I, save the toothless clause in Article 8. In its Proposal, the Commission recognised that digital (NB: the EU uses the term 'cyber') surveillance technologies have been exported to repressive regimes and conflict areas, where they are used in violation of human rights. While accepting that these technologies can have legitimate law enforcement purposes, the Commission concluded that export 'poses a risk to the security of [dissidents and human rights activists] and to the protection of fundamental human rights, such as the right to privacy and the protection of personal data, freedom of expression, freedom of association, as well as, indirectly, freedom from arbitrary arrest and detention, or the right to life.' (see p. 6.)

In a laudable attempt to address the shortcomings of the civil-military dichotomy, the Proposal explicitly included 'cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law' in the definition of 'dual-use items' under Article 2(1)(b), thereby departing from the internationally accepted definition of 'dual-use' in the Wassenaar Arrangement (cf Annex I, under 'List of Dual-Use Items'). From the outset, the EU institutions have been aware of the negative impact stricter requirements may have on exporters. In comparison to the Proposal, a balance now seems to have been struck more favourably in the interest of free trade, as the Compromise Text has excluded digital surveillance technologies under Article 2's definition of 'dual-use items'. Even though the Commission's Article

2(21) definition of 'cyber-surveillance technology' has largely been retained, the removal of digital surveillance technology from the definition of 'dual-use items' means that digital surveillance technology is not included in the control list of Annex I.

2. Human rights as an explicit justification for export control

To make up for the lack of general export control requirements presented by the removal of digital surveillance technologies from the definition of dual-use items, the Compromise Text has added a new catch-all clause in Article 4a(1): 'An authorisation shall be required for the export of cyber-surveillance items not listed in Annex I if the exporter has been informed by the competent authority 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.'[1] From a human rights perspective, this mandatory language is encouraging, as is the inclusion of items which *may be intended* for use in connection with the commission serious violations of IHRL or IHL. The Proposal's Article 14 also contained a clear obligation to conduct a risk assessment before granting an export authorisation; under this provision, Member States were obliged ('shall') to take the following criteria into account in deciding whether or not to grant an export authorisation: 'respect for human rights in the country of final destination as well as respect by that country of international humanitarian law' (para. b); 'the internal situation in the country of final destination – competent authorities will not authorise exports that would provoke or prolong armed conflicts or aggravate existing tensions or conflicts in the country of final destination' (para. c); and 'preservation of regional peace, security and stability' (para. d). Especially the criterion of 'respect for human rights in the country of final destination' sought to bring the dual-use export regime more in line with the export regime for arms (see Council Common Position 2008/944/CFSP of 8 December 2008 Article 2(2)). These requirements have not made it into the Compromise Text's Article 14. Member States are now encouraged ('should') to consider the risk of internal repression or serious violations of human rights or humanitarian law in recitals (1a) and (3). A similar decision has been made with regard to the Proposal's addition to the existing catch-all clause in Article 4(d), namely that an authorisation for items not listed in Annex I 'shall be required' if the exporter has been informed by the competent authority that the items in question are or may be intended 'for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination'. While recital (5), which refers to this risk, has been retained, the Compromise Text has deleted this important provision from the Regulation's text.

3. Exporter due diligence

In addition to the extra catch-all clause, the Compromise Text has included the concept of exporter due diligence in Article 4a(2): 'If an exporter is aware according to its due diligence findings that cybersurveillance items which it proposes to export, not listed in Annex I, are intended, in their entirety or in part, for any of the uses referred to in paragraph 1, it shall notify the competent authority, which shall decide whether or not to make the export concerned subject to authorisation.' Recital (4a) and Article 2(22) tell us what is meant by 'due diligence': a risk assessment related to the export of items to end-users and end-uses. At first glance, Article 4a(2) is a major improvement when compared to the current Dual-Use Regulation, but the Council and Parliament have significantly watered down the initial concept of exporter due diligence in the Proposal's Article 4(2), which was phrased in less noncommittal terms: 'If an

exporter, under his obligation to exercise due diligence, is aware that dual-use items which he proposes to export, not listed in Annex I, are intended, in their entirety or in part, for any of the uses referred to in paragraphs 1.' It is hard to say what the Compromise Text's reference to 'due diligence findings' exactly means at the moment – the guidelines for businesses will be drafted in the following months. The EU is definitely increasing its efforts to include corporate due diligence obligations in its legislative arsenal (see here and here), but it is unlikely that vague references to due diligence with no clear penalties for infringement will incentivise businesses to flag an item intended for export and voluntarily subject themselves to export controls. There is also no way of knowing how businesses will conduct this enquiry, and how and if Member States' competent authorities will have some oversight mechanisms. This leads us to the final point.

4. Towards greater transparency

The 2009 Dual-Use Regulation makes no mention of the term 'transparency' at all, but recital (1a) of the Compromise Text and recital (25) of the Proposal and the Compromise Text stress that outreach to the private sector and transparency are 'essential elements for an effective export control regime'. Under the 2009 Dual-Use Regulation, the Commission was tasked to review the implementation of the Regulation every three years and present a report to the Parliament and Council, for which Member States were required to provide the Commission with 'all appropriate information' (see Article 25). The Compromise Text has retained this information requirement (Article 24(3)). Under the new rules, the Commission is to submit the report annually, and the report shall be public (Article 24(2)). The Compromise Text further adds that for digital surveillance items, 'the annual report shall include dedicated information on authorisations, in particular on the number of applications received by items, the issuing Member State and the destinations concerned by these applications, and on the decisions taken on these applications.' Sor far, so good. However, Article 24(2) also adds that the information in these annual reports 'shall be presented in accordance with the principles set out in paragraph 3', i.e. 'legal requirements concerning the protection of personal information, commercial sensitive information or protected defense, foreign policy or national security information.' (see also recital (25a) in the Compromise Text.) This new clause lays bare the broader problem with export controls. Naturally, protection of personal data, commercial confidentiality and national security concerns are all worthy goals, but one could question whether this provision leaves Member States with a dangerously large amount of discretion to withhold certain information based on either one or several of these three grounds. For example, the EU's Common Position on arms exports is perfectly clear and comprehensive, yet a lack of transparency allows States to keep details on licencing decisions secret by invoking national security interest and keep on arming foreign regimes which continue to commit war crimes.

IV. Final thoughts

As Ms. Markéta Gregorová concluded in her presentation at the Export Control Forum: there is no straightforward answer to the question whether export of AI to countries such as the PRC will now finally require a licence. For this reason, human rights NGOs remain critical, and following the EU's press release announcing the conclusion of the Compromise Text, Amnesty International and others called on the Council of the EU to reconsider the final draft, claiming it 'fails to meet basic human rights standards'. Indeed, the deletion of digital surveillance tech from the definition of dual-use and the general catch-all clause, the lack of an explicit human rights risk assessment in the authorisation decision, the vague notion of corporate due diligence findings, and the

multiple broad exceptions States can invoke in order to withhold information, still seem to provide both EU Member States and companies a lot of leeway to put business first. It is vital that the regulatory framework requires nothing less than a rigorous risk assessment, as even when such a legal requirement is in place, (former) EU Member States seem to find ample room to manoeuvre and choose to interpret the applicable law as they please. To end on a brighter note, the 2009 Dual-Use Regulation only makes reference to 'human rights considerations' once, namely in Article 8(1). The Proposal mentions 'human rights' twelve times, excluding the references in the explanatory memorandum. With seven references to 'human rights' in the actual text of the Regulation, the current Compromise Text seems to be just that – a compromise between the 2009 version and the Commission's Proposal.

1. Underlining in quoted passages is my emphasis.

State responsibility | Europe | Due diligence | China | Dual-use

Prev Next

Related articles

- The UK's Unlawful Grant of Export Licences for the Sale of Arms to Saudi Arabia
- Autonomous Weapons Systems and the Liability Gap, Part Two: Civil Liability and State Responsibility
- The Dam on the Gualcarque River
- Access to supply chain information: stopped at the border by customs?
- A clear risk of what? The Egyptian navy, the Dutch arms export policy and linguistic inconsistencies in the EU Common Position
- Civil liability in the EU proposal for a Corporate Sustainability Due Diligence Directive: a leap forward or stifling progress?

Tag cloud

accomplice liability 3 | Aiding and abetting 11 | Alien tort statute 3 | Arms export 9 | Autonomous Weapons 2 | banking and finances 1 | BNP Paribas 1 | Business and human rights 20 | bystander liability 1 | Canada 1 | Child slave labour 2 | China 2 | Civil law 9 | cobalt 1 | Command responsibility 1 | Consequentialism 1 | constructive knowlegde standard 1 | Corporate criminal liability 10 | crime of aggression 2 | Criminal law 25 | Criminal membership 2

DARS 3 | Data Protection Act 1 | death penalty 1 | Democratic Republic of Congo 1 | Doctrine of adoption 1 | Domestic law 9 | DPA 1 | Dual-use 1 | Due diligence 11 | ECHR 4 | Ecocide 2 | ECtHR 5 | Europe 8 | export licencing 2 | Facebook 1 | France 3 | Gemmeker 1 | Germany 1 | Guiding principles 4 | Holocaust 1 | ICC 6 | ICTY 1 | International Humanitarian Law 4 | JCE 1 | Jurisdiction 5 | Kant 1 | MLA 1 | Mutual legal assistance 1 | Myanmar 1 | Netslé 1 | OECD guidelines 1 | Parent company liability 4 | participation in a venture 1 | police brutality 1 | Private international law 1 | Public scrutiny 1 | Russia 5 | Social Media 3 | Soering liability 1 | South America 1 | State responsibility 10 | State-owned enterprise 1 | Strict liability 1 | Sudan 1 | Supply chain 7 | Syria 5 | Technology 2 | Terrorism 2 | The Netherlands 4 | Tort law 8 | U.S. Supreme Court 2 | Ukraine 4 | UNGPs 1 | United States 5 | Westerbork 1 | World War II 1