

Europe should not help dictators spy on their own citizens

- Exports of cyber-surveillance tools need to be authorised
- Civilians and human rights defenders should be protected
- Parliament ready for talks with EU ministers

EU export controls should be extended to cyber-surveillance tools to avoid human rights violations, MEPs said in a vote on Wednesday.

This now sets Parliament's position for negotiations with EU ministers.

The EU is currently updating its rules on the export control of *dual-use* items to keep up with new technologies and to prevent authoritarian regimes from spying on their own citizens with the help of European products.

Goods and technologies designed for use in peaceful, civilian circumstances, but that can also be used to build weapons of mass destruction or in terrorist attacks, are already under an [EU export control regime](#). The [new rules](#) would add certain cyber-surveillance tools to the list of items that need to be approved by national authorities before being exported. These include devices for intercepting mobile phones, hacking computers, circumventing passwords or identifying internet users, as [such dual-use items are widely used to suppress civilians](#), political opposition and activists around the world.

MEPs want to protect human rights more robustly and create a system that can rapidly deal with new technologies.

Their key suggestions include:

- protecting the right to privacy, data and freedom of assembly more thoroughly, by adding clear-cut criteria and definitions to the law,
- exporters of products not listed in the new law, but which could be used for human-rights violations, have to make sure that their goods will not fall into the wrong hands, by following OECD-based 'due-diligence' guidelines,
- the EU Commission must publish a handbook before the entry into force of the new rules, so that EU businesses know what they can and cannot do,
- new risks and technologies have to be swiftly included in the law,
- creating a level playing field among member states, by, for example, introducing similar penalties for non-compliance, along with greater transparency of national authorities' export control decisions, and

- removing encryption technologies from the list of cyber-surveillance products, as these are vital for the self-defence of human rights defenders.

The new rules were backed by 571 votes to 29, with 29 abstentions.

Quote

Parliament's rapporteur [Klaus Buchner \(Greens/EFA, DE\)](#) said: "Dictators spy on their citizens using EU cyber-surveillance. This must stop. The EU cannot contribute to the suffering of courageous activists, who often risk their lives for freedom and democracy. Trade should promote security, stability and human rights in the world. We are determined to close dangerous gaps in the export control of dual-use goods and call on member states to follow suit."

Next steps

MEPs have now set the Parliament's negotiating position. Talks can start as soon as EU member states have agreed on their own negotiating position.

Quick facts

Goods and technologies that can be used in peaceful civilian circumstances can also be used for building weapons of mass destruction, in terrorist attacks or to facilitate human rights violations. These include a broad range of products, from chemicals, toxins, electronic equipment, lasers and navigation technology, to nuclear power technology, robotics and software. The current system dates back to 2009; exports are inspected and authorised by national authorities. During the "Arab Spring", there was evidence that European technology was used by authoritarian regimes to oppress activists. The European Parliament, the Council and the Commission issued [a joint statement](#) in 2014 to review the export control system, and the European Parliament has also adopted [resolutions](#) calling for targeted changes.

Procedure: Co-decision

#dualuse #HumanRights

Further information

[The adopted text will be available here \(click on 17.01.2018.\)](#)

[Video recording of the debate \(click on 16.01.2018.\)](#)

[Press release on the committee vote \(23.11.2017\)](#)

[EuroparlTV video: Parliament calls for stricter export controls on spyware technology](#)

[EP Briefing: Review of dual-use export controls \(July, 2017\)](#)

[Dual-use control in a nutshell \(by the Commission\)](#)

[Cyber technology: preventing human rights abuses \(Article including a context video on Dual-use items\)](#)


[Procedure file](#)


[International Trade Committee](#)


Contacts

Bálint Péter LINDER

Press Officer

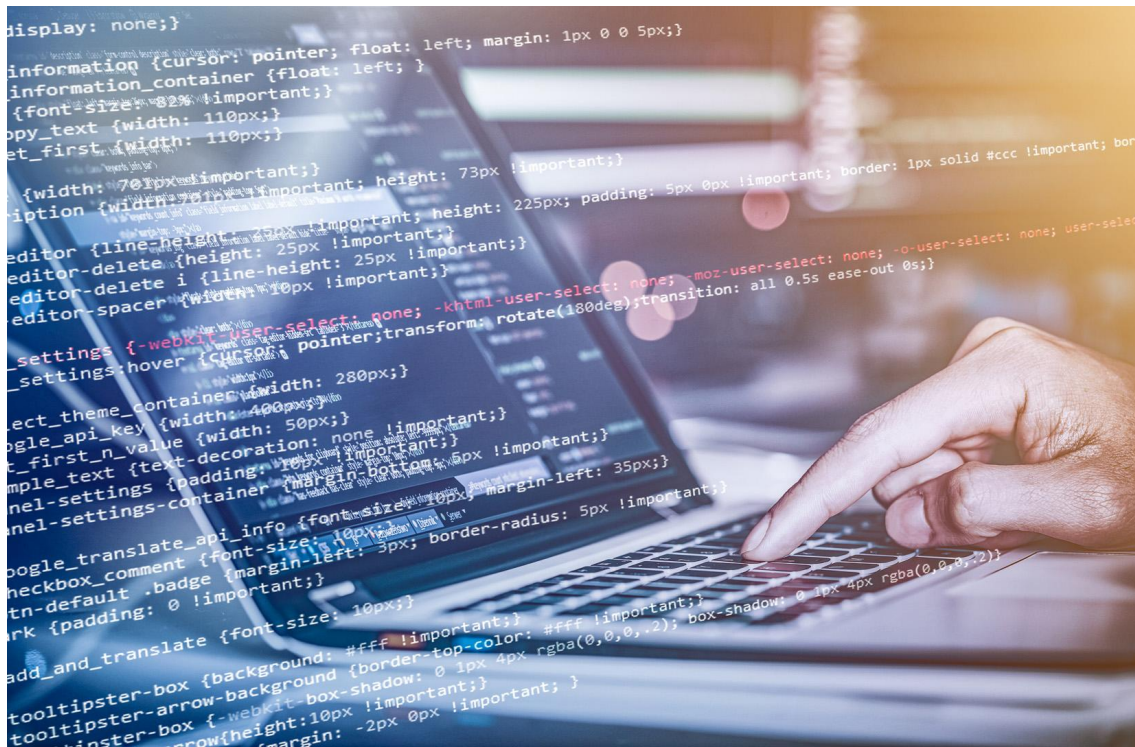
 (+32) 2 28 32584 (BXL)

 (+33) 3 881 73839 (STR)

 (+32) 470 88 08 77

 [@EP_Trade](https://twitter.com/EP_Trade)

 balint.linder@europarl.europa.eu



MEPs want to ensure that dictators don't spy on their citizens with EU products © AP Images/European Union-EP