

Preventing authoritarian regimes from spying on their own citizens

- Export of cyber-surveillance tools needs to be authorised
- Protection of civilians and human right defenders
- Handbook for exporters, level playing field for member states

EU export controls will be extended on goods and technologies designed for civilian use but possibly used for human rights violations, Trade Committee MEPs voted on Thursday.

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 for weapons of mass destruction or terrorist attacks, are already under an [EU export control regime](#). The [new rules](#) would enhance 'human security', by adding certain cyber-surveillance tools to the list of items that need the approval of 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.

Trade Committee MEPs want to strengthen the protection of human rights and create a "future-proof" system that can rapidly deal with new technologies.

Their key suggestions include:

- strengthening the protection of the right to privacy, data and, freedom of assembly, by adding clear-cut criteria and definitions to the regulation,
- exporters of products not listed in the regulation but which could be used for human-rights violations, have to make sure that their goods won't fall into the wrong hands, by following OECD-based 'due-diligence' guidelines,

- the 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 regulation, and
- 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.

MEPs also voted to delete encryption technologies from the list of cyber-surveillance products, as they consider these vital for the self-defence of human rights defenders.

The new rules were backed by 34 votes to 1, with 2 abstentions.

Quote

Parliament's rapporteur [Klaus Buchner \(Greens/EFA, DE\)](#) said: "With today's vote we extend effective control to cyber-surveillance technology. We close loopholes that otherwise result in innocent people across the world being imprisoned, tortured and killed. We make the protection of human rights a central aspect of dual-use export control. We add strong, new transparency measures and include civil society participation, whilst continuing to create value-based European trade policy."

Next steps

The full House will have to confirm the Parliament's negotiating mandate during the December plenary session in Strasbourg. Parliament can begin talks with ministers as soon as EU member states have agreed 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, terrorist attacks or facilitating human rights violations. These include a broad range of products from chemicals, toxins, electronic equipment, lasers,

navigation technology to nuclear power technology, robotics and software. The current system dates back to 2009, and 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 Parliament, the Council and the Commission issued [a joint statement](#) in 2014 to review the export control system, and the EP has also adopted [resolutions](#) calling for targeted changes.

Further information

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

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

[Procedure file](#)

[International Trade Committee](#)

Contacts

Bálint Péter LINDER

Press Officer

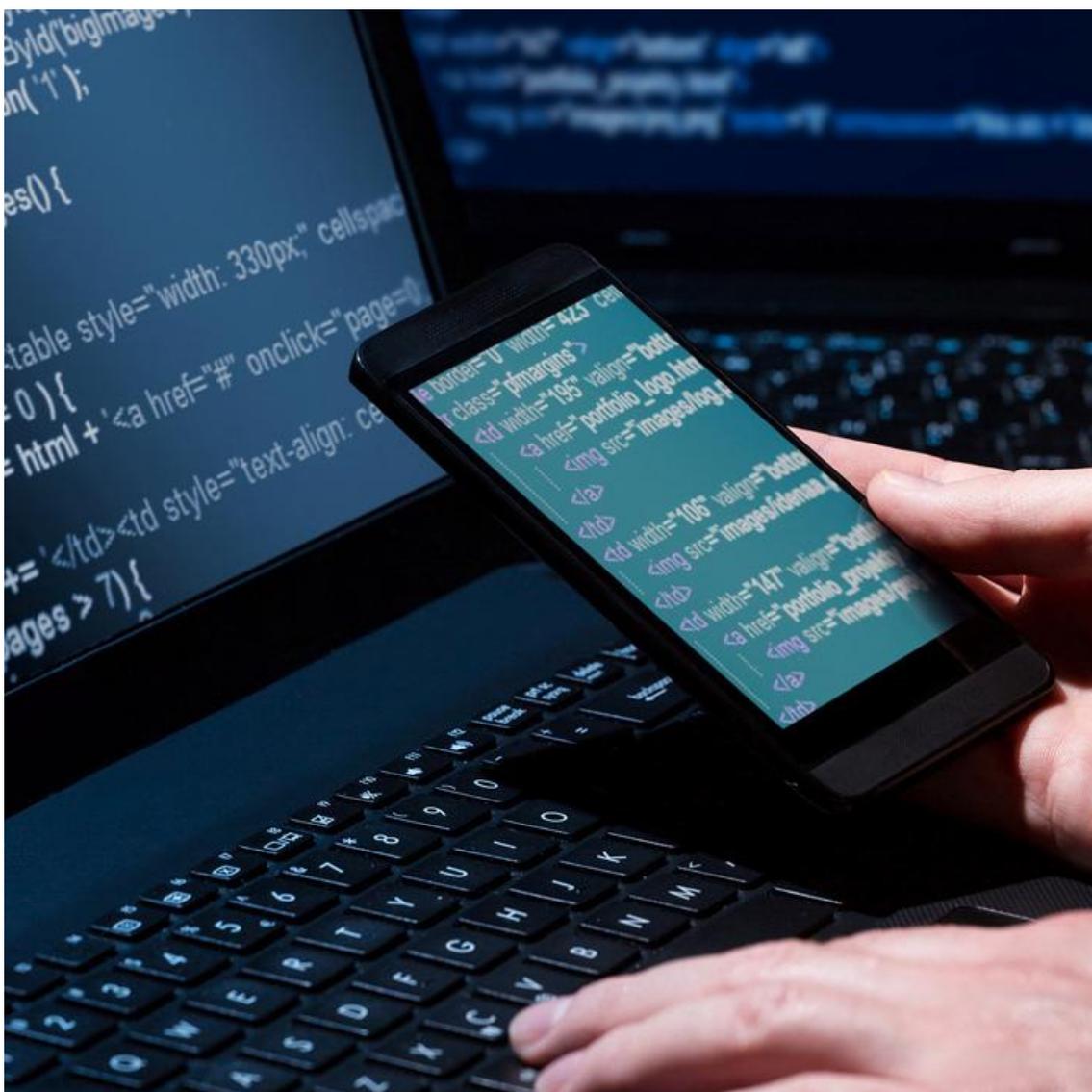
 (+32) 2 28 32584 (BXL)

 (+33) 3 881 73839 (STR)

 (+32) 470 88 08 77

 [@EP_Trade](#)

 balint.linder@europarl.europa.eu



Devices for intercepting mobile phones or hacking computers are used to suppress political opposition ©AP Images/European Union-EP