Council Conclusions on Cybersecurity of Connected Devices

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

On 2 December 2020, the Council approved conclusions on the cybersecurity of connected devices. The Council highlights that connected devices, including machines, sensors and networks that make up the Internet of Things (IoT) will not only play a key role in further shaping Europe's digital future, but also entail numerous security issues. The conclusions set out priorities to address risks related to privacy, information security and cybersecurity, and to boost the global competitiveness of the EU's IoT industry by ensuring the highest standards of resilience, safety and security. They, *inter alia*, highlight the importance of reinforcing resilient and secure infrastructures, products and services for building trust in the Digital Single Market and within the European society. The EU's core values must be preserved, in particular privacy, security, equality, human dignity, rule of law, and open internet. Priorities in the area of cybersecurity of connected devices should be:

- Assessing the need for a horizontal legislation that addresses all cybersecurity aspects and that will also serve as the basis for product placement on the market;
- Elaborating additional certification schemes for connected devices, which will also require the setting of cybersecurity norms, standards, and technical specifications;
- Supporting SMEs, which should be an essential building block of the European cybersecurity ecosystem, in particular if standardisations are developed.

The policy in cybersecurity comes along with the EU's efforts to the digital transformation. This is one of the key policy priorities of Commission President *Ursula van der Leyen* and is also backed by the EU leaders. At the Special European Council meeting on 1-2 October 2020, the heads of state and government confirmed the ambition for an acceleration of the digital transition and agreed that at least 20% of the funds under the Recovery and Resilience Facility would be made available for achieving objectives such as:

- Fostering the European development of the next generation of digital technologies, including supercomputers, quantum computing, blockchain and human-centric artificial intelligence;
- Accelerating the deployment of very high capacity and secure network infrastructures (e.g. 5G) all over the EU
- Enhancing the EU's ability to protect itself against cyber threats.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union