POLICY BRIEF NO. 3

ALL FUNDAMENTAL RIGHTS ARE RELEVANT FOR CYBERSECURITY

Cybersecurity regulation in the European Union

To understand the relevance of fundamental rights in the European Union (EU) cybersecurity domain, the following background information should be considered:

1. The EU can regulate cybersecurity issues only within the **boundaries of the Union's legislative competences**.

2. However, the EU's regulation competences in the field of cybersecurity are not well-defined.

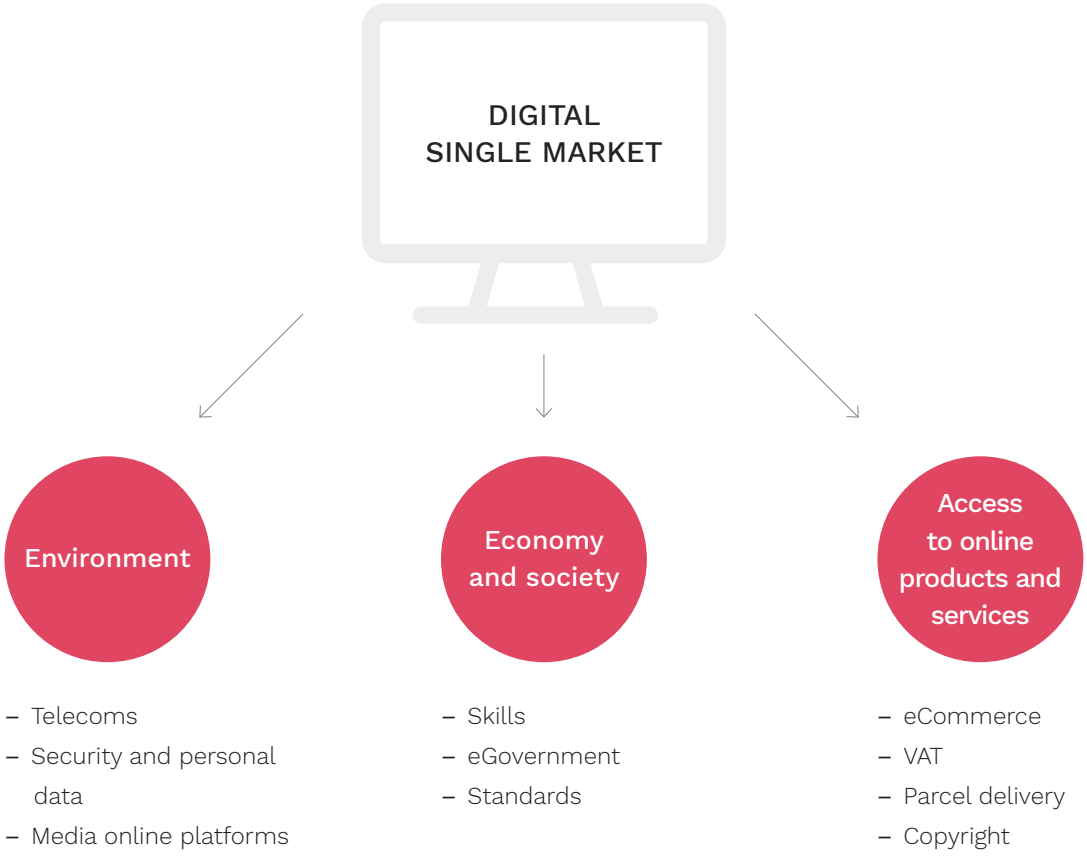
3. At the same time, EU policy makers can't avoid discussing cybersecurity, as daily **lives and economies become** increasingly **dependent on digital technologies** and **citizens** are **at risk of** becoming exposed to serious **cyber incidents**

4. It is an **emerging and complex policy area** concerned with the smooth functioning of the Digital Single Market.

The EU aims to ensure a fair, open, and secure digital environment

Relevant EU cybersecurity policy documents as well as legislative measures are found within frameworks addressing:

1. network and information security
2. electronic communications (including privacy and data protection issues)
3. cybercrime
4. cyber-defence



Guaranteeing the protection of fundamental rights

The EU digital economy could grow up to 4% of the EU's GDP, provided there are right framework conditions in place, including the appropriate legislative and policy measures.

EU Cybersecurity legislation affects a **wide range of fundamental rights** that are foreseen in the EU Charter of Fundamental Rights, such as freedom of expression, equality, rights of elderly, the right to conduct business.

Yet, impact assessments and discussions of legislative proposals tend to have an **unduly narrow focus** exclusively on the respect for private and family life and the right to the protection of personal data. A more in-depth, holistic analysis of the impact on the fundamental rights framework is needed.

The Charter of Fundamental Rights of the EU

Each legislative proposal put forward by the European Commission, including the ones concerning cybersecurity, must be compatible with rights and freedoms laid down in the Charter of Fundamental Rights of the EU.

Important facts:

- The Charter is based on the idea that fundamental rights protection is 'an indispensable prerequisite to the Union's legitimacy'.
- The initial proclamation was at the Nice Council in 2000, and it's legally binding as of the enforcement of the Lisbon Treaty in 2009.
- The Charter complements national human rights documents and the European Convention on Human Rights (ECHR).
- It provides the most recent codification of fundamental rights in Europe.

Values of the Charter of Fundamental Rights of the EU

Policy makers should consider a wider range of values and fundamental rights that are or may be affected by EU cybersecurity policies and regulatory measures, such as

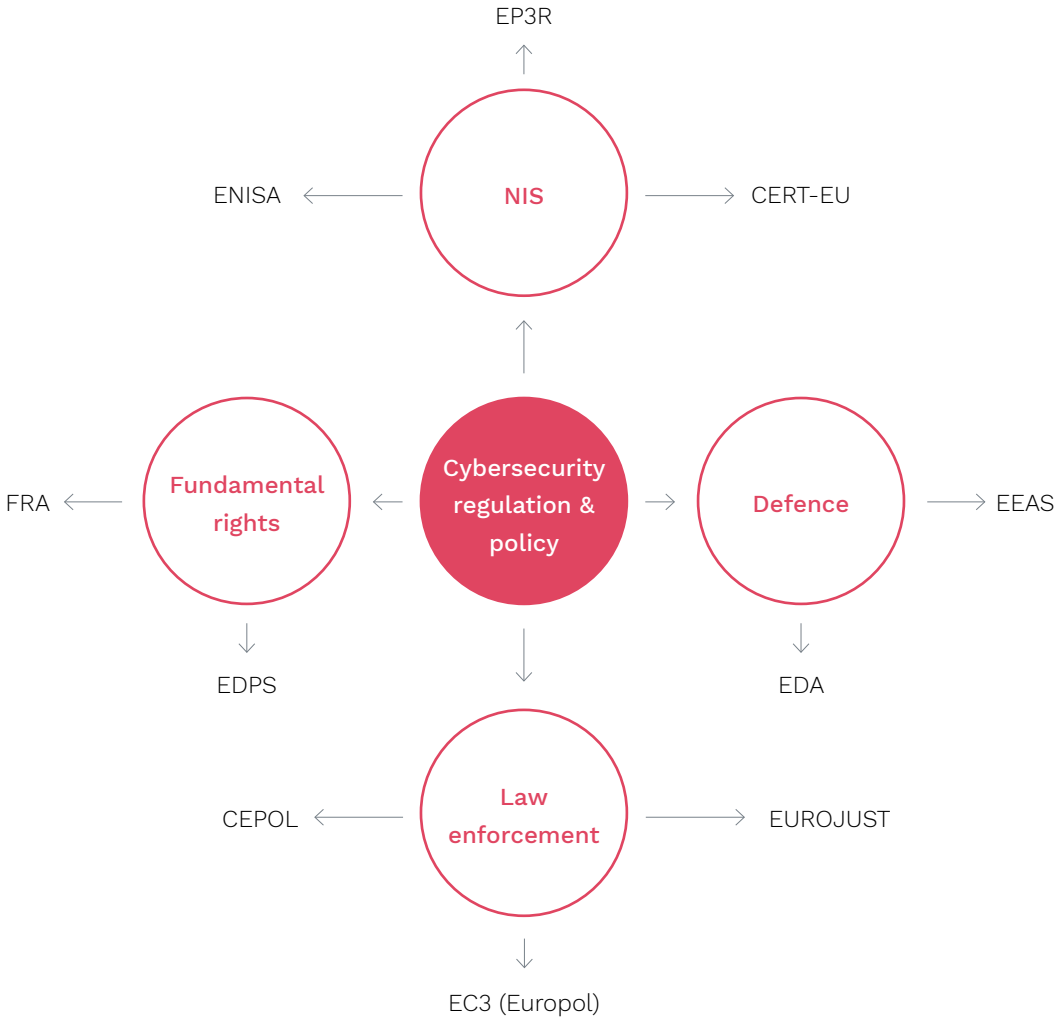
- Human dignity
- Freedom
- Equality
- Solidarity
- Democracy
- The rule of law
- Respecting the diversity of the cultures and traditions of the peoples of Europe (pluralism)
- Subsidiarity (respecting the organisation of their public authorities at national, regional and local levels)
- Balanced and sustainable development
- Free movement of persons, services, goods and capital, and the freedom of establishment

Opt-out countries:
UK, Poland and the Czech Republic.

An overview of specialised EU bodies involved in cybersecurity regulation and policy

All EU institutions (i.e. the European Commission, the Parliament, and the Council), agencies and bodies are bound by the Charter of Fundamental Rights of the EU.

The EU's cyber institutional arrangement is complex and multi-layered, crossing across an array of internal policy areas. The arrangement recognises that addressing cybersecurity issues requires the cooperation of multiple stakeholders with different expertise.



Despite these challenges, there are ways to embed EU values in legislative frameworks and policies

Challenges of cybersecurity regulation

It is important to recognise challenges of protecting fundamental rights on EU level in the digital environment. Such challenges are:

1. The cybersecurity domain is constantly evolving and it is comprised of highly fragmented legislative measures.

2. Cybersecurity is a horizontal problem and a common denominator of various new technologies connected to the internet.

3. Cooperation agreements among EU bodies and agencies could integrate aspects which concern fundamental rights protection.

Recommendation 1: Incentivise judicial review of EU legislative measures by the CJEU

There is a growing number of European Court of Justice case law concerning the compatibility of the EU Charter with the EU Data Retention Directive. This directive compelled ISPs and telecommunications service providers operating in the Union to collect and retain data about a subscriber‘s service usage.

Such case law undertakes consideration whether a proper balance is struck between the various interests, while it urges to take fundamental rights seriously from the very outset of the legislative process.

Examples:

Digital Rights Ireland judgement of 8 April 2014 (joined cases C-293/12 and C-594/12)

Opinion 1/15 concerning the agreement on Passenger Name Record data between the EU and Canada

Recommendation 2: Maintain a value-driven EU cybersecurity approach

Encourage the following actions

1. Conduct an impact assessment of the final text of a legislative measure. This would enhance compliance with values embedded in the EU Charter.

2. Involve diverse stakeholders throughout legislative deliberations, such as EU specialised bodies (e.g. EDPS, ENISA), NGOs and other relevant stakeholders.

3. Develop new legislative techniques, such as by the data protection by design principle, which further strengthens obligations stemming from the General Data Protection Regulation.

4. Aim for a more accentuated use of existing measures and principles (e.g. the implementation of appropriate security measures).

5. Cooperation agreements among EU bodies and agencies could integrate aspects which concern fundamental rights protection.

More information can be found

The slides are based on the research work done by the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity).

The objective of CANVAS is to bring together stakeholders from key areas of the European Digital Agenda to approach the challenge how cybersecurity can be aligned with European values and fundamental rights.

In particular, we provide the following CANVAS resources:

- Briefing packages
- CANVAS Reference Curriculum
- CANVAS MOOC
- Open Access Book
  'The Ethics of Cybersecurity'

The following slide directly points to those of our White Papers which address in detail the challenges of cybersecurity.

Bibliography: cybersecurity challenges (CANVAS White Papers)

Ethical challenges

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan, and Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” SSRN Scholarly Paper ID 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Legal challenges

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle, and Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” SSRN Scholarly Paper ID 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Technological challenges

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter, and Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” SSRN Scholarly Paper ID 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Project facts

Project coordination and contact:
PD Dr. sc. ETH Markus Christen
University of Zurich (UZH),
Digital Society Initiative
Rämistrasse 66, 8001 Zürich

Slidedocs version:
Version 2.0 October 2019

Project duration:
Sept. 2016 – Oct. 2019

Partners:
The CANVAS Consortium consists of 11 partners (9 academic institutions and 2 partners outside academia) located in 7 European countries.

Funding:
1.57 Mio. €, of which 1 Mio. € is funded by the European Commission and the remaining part emerges from the Swiss State Secretariat for Education, Research and Innovation.

Funding notice for CANVAS

Co-funded by the Horizon 2020 programme of the European Union

The CANVAS project (Constructing an Alliance for Value-driven Cybersecurity) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540. This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the EU and the Swiss Government