POLICY BRIEF NO. 3

ALL FUNDAMENTAL RIGHTS ARE RELEVANT FOR CYBERSECURITY

Maintaining a comprehensive approach to fundamental rights protection in EU cybersecurity

When the European Commission puts forward cybersecurity policy and regulation proposals, their evaluation is often focused on their compatibility with the right to protection of personal data and the right to respect for private and family life. Indeed, in the digital environment, the right to data protection and privacy are among the most relevant concerns. Yet, while still recognizing the significance of these two rights enshrined respectively in Articles 8 and 7 of the Charter of Fundamental Rights of the European Union (EU Charter), policy makers should consider a wider range of fundamental rights that are or may be affected by EU cybersecurity policies and regulatory measures.

Policy makers should consider a wider range of fundamental rights that ARE or may be affected by EU cybersecurity policies and regulatory measures.

European primary law proclaims protection of EU values and fundamental rights

According to Article 2 of the Treaty of the EU, '[t]he Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities'. These EU values are determined by the principles of pluralism, non-discrimination, tolerance, justice and equal treatment of men and women and they are further detailed in the EU Charter. Additionally, the EU Charter foresees a wide array of fundamental rights enjoyed by EU citizens and residents, including but not limited to the right to a fair trial, freedom of thought, freedom of expression and information, rights to property, education and to an effective remedy. These values and rights must be reflected in EU regulatory measures.

Step 1: Recognise challenges of protecting fundamental rights on EU level in the digital environment

EU policy documents and legislation in the cybersecurity domain recognise that any measures taken with respect to the protection of EU citizens, society as well as information systems and infrastructure, should be developed in accordance with the com-

mitment to respect fundamental human rights. For example, the NIS Directive in its Recital 75 notes that the 'Directive respects the fundamental rights, and observes the principles, recognised by the EU Charter, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard'. Thereby, the Directive should be implemented in accordance with those rights and principles.

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms, as enshrined in the Charter of Fundamental Rights of the European Union and in EU core values.

Despite recognition of the crucial role that fundamental rights play, their practical implementation remains difficult. The inherent complexity of the topic is furthered by EU governance arrangements - numerous bodies and institutions working on cybersecurity matters have delineated competencies. For example, the European Union Agency for Network and Information Security (ENISA) focuses on a high-level of network and information security. The European Defence Agency (EDA) plays a role in European military coordination, security and defence policy, while Europol contributes to Member State attempts to investigate cybercrime. Moreover, the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) takes care of securing the EU IT infrastructure.

While all these bodies have means of cooperation and information exchange, it is not entirely clear whether fundamental rights protection mechanisms are foreseen, and if so, whether they are sufficient.

Step 2: Incentivising judicial review of EU legislative measures

The Court of Justice of the EU (CJEU) interpreted EU law, including measures addressing cybersecurity. In its case law, the CJEU emphasised that '[t]he applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter'.

A model case of the CJEU judiciary declaring non-compliance with European fundamental rights would be the decision regarding Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive). This directive was annulled by the Grand Chamber of the Court on the grounds that the blanket collection of communication data, in particular traffic and location, by providers of communication providers was not proportionate (i.e., excessive). Therefore, this legislation constituted an infringement of the rights privacy and protection of personal data of individuals (enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU). However, the court decision did not automatically annul Member States' laws implementing the Data Retention Directive. This judgement is exemplary of a legislative measure to be overturned on the grounds of incompatibility with the rights set forth in the EU Charter.

The CJEU Opinion 1/15 concerning the draft agreement between the European Union and Canada on the transfer of Passenger Name Record is also an illustrative ex-ample highlighting the importance of adherence to the fundamental rights recognised by the EU. In this Opinion, the CJEU concluded that the envisaged agreement should not be concluded in its current form because rules governing the transfer of PNR data from the EU to Canada entail an interference with the fundamental rights to respect for private life and the protection of personal data.

These examples demonstrate that values stemming from the EU Charter play an important role in the EU regulatory approach in the cybersecurity domain, even though they are contested by the EU institutions. Nonetheless, such reviews of legislative measures are not conducted by default but rely on proactive EU institutions or judges at national courts.

Step 3: Maintaining a value-driven EU approach to cybersecurity

Only a strong emphasis on the protection of fundamental rights can contribute to a value-driven EU approach to cybersecurity. The 2013 Cybersecurity Strategy claims that: 'Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values.' Still, this approach is often challenged by EU institutions themselves (as seen in the previous section). In order to maintain this approach and adhere to the EU Charter, the EU needs to embed its values into the applicable regulatory framework. But putting this to practice is not a straightforward task when it comes to effective development and implementation of EU legislation or policies. The embedment process entails a comprehensive understanding of 'the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.' Additionally, a thorough understanding of the regulatory field is required while the best use of all-encompassing expertise can only be achieved by proactive involvement, action and collaboration of different stakeholders. The embedment of EU values enshrined in the EU Charter can take place both on an ex ante and an ex post basis (e.g., judicial review).

Ex ante basis: Impact assessments and stakeholder consultation

Those EU institutions exercising legislative power, namely the European Commission, the Council of EU, and the European Parliament, as well as EU agencies, in particular ENISA, can play an important role in this regard on an ex ante basis.[1] For example, the European Commission has developed good practices of carrying out compatibility checks and impact assessments of legislative proposals. It is believed that these practices mitigate the risk that proposed legislative measures violate fundamental rights. The knowledge generated during this process can then facilitate the decision-making process to ensure that the course of action that will best support the fulfilment of fundamental rights will be taken. Yet, the importance of these tools is often challenged during the legislative process. This is in particular done by amendments entailing considerable changes to a proposed text which originally related to the protection of fundamental rights.

In the domain of cybersecurity, consultations and contributions of the specialised EU bodies, such as EDPS, ENISA and the European Data Protection Board, proved to be useful and allowed overcoming the limitations of initial compatibility checks and impact assessments. At the same time, having an impact assessment of the final text of a legislative measure would be a welcome development. Additionally, the participatory dimension can also facilitate the integration of EU values into regulatory frameworks and policies. For example, during the drafting stage of legislative proposals, the European Commission usually launches a public consultation process in order to unveil the key issues faced by the concerned stakeholders. In fact, the European Commission carries a duty to conduct 'broad consultations with parties concerned in order to ensure that the Union's actions are coherent and transparent'.[2] Based on the inputs received during the public consultation process, the European Commission has to propose measures that would balance different interests of stakeholders. But these proposed measures would also need to be compatible with values enshrined in the EU Charter. The concerned stakeholders can remain active after closed consultations by providing comments on legislative proposals throughout different stages of legislative process. Some organisations, in particular, the ones representing civil society groups, often provide detailed analyses of how a future legislative measure could better implement provisions of the EU Charter. However, for these analyses to be taken into

account by legislators, the concerned stakeholders need to run costly lobbying campaigns. Consequently, business interest groups continue to be better represented.

Alternative ways of maintaining a European approach to cybersecurity regulation

Apart from compatibility checks, impact assessments of legislative proposals, and stakeholders' participation, legislators can choose emphasising certain values in the legislative text such as the principle of data protection by design in Article 25 (1) GDPR. It explicitly requires controllers of personal data processing activities to implement technical and organisational measures suitable to mitigate risks that may arise from the processing activities, thus affecting the rights and freedoms of individuals' whose data are being processed. These measures should ensure that the requirements and principles of the GDPR are embedded in the processing activity from its inception and are continuously reviewed throughout the data processing activity. In practice, this principle reinforces the obligations listed in Article 5 of the GDPR specifying the principles of personal data processing. Similar legislative techniques could be considered to maintain a value-based EU approach to cybersecurity, recognising the importance of fundamental rights in the digital environment.

Where more info can be found

This Policy Brief is based on the research work done by the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity). Detailed reports of this work have been published in four main White Papers:

1. Cybersecurity and Ethics
2. Cybersecurity and Law
3. Attitudes and Opinions Regarding Cybersecurity
4. Technological Challenges in Cybersecurity

All White Papers can be found on our website, along with all of our (downloadable and printable) Policy Briefs, short online explanations of the key cybersecurity issues, and commented literature lists for further reading:

canvas-project.eu

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 Swiss Government.

Objective of CANVAS:
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.

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

Version and date of publication:
Version 1.0, February 2019

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.

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

Project duration:
September 2016 – August 2019