POLICY BRIEF NR. 3

ALLE GRUNDRECHTE SIND FÜR DIE CYBER-SICHERHEIT RELEVANT

Die Regulierung der Cybersicherheit in der Europäischen Union

Um die Bedeutung von Grundrechten im Bereich der Cybersicherheit der Europäischen Union (EU) zu verstehen, sollten die folgenden Hintergrundinformationen berücksichtigt werden:

1. Die EU kann nur Cybersicherheitsfragen regeln die **innerhalb ihrer Gesetzgebungskompetenz** liegen.

2. Jedoch sind die regulatorischen Kompetenzen der EU im Cybersicherheitsbereich nicht klar definiert.

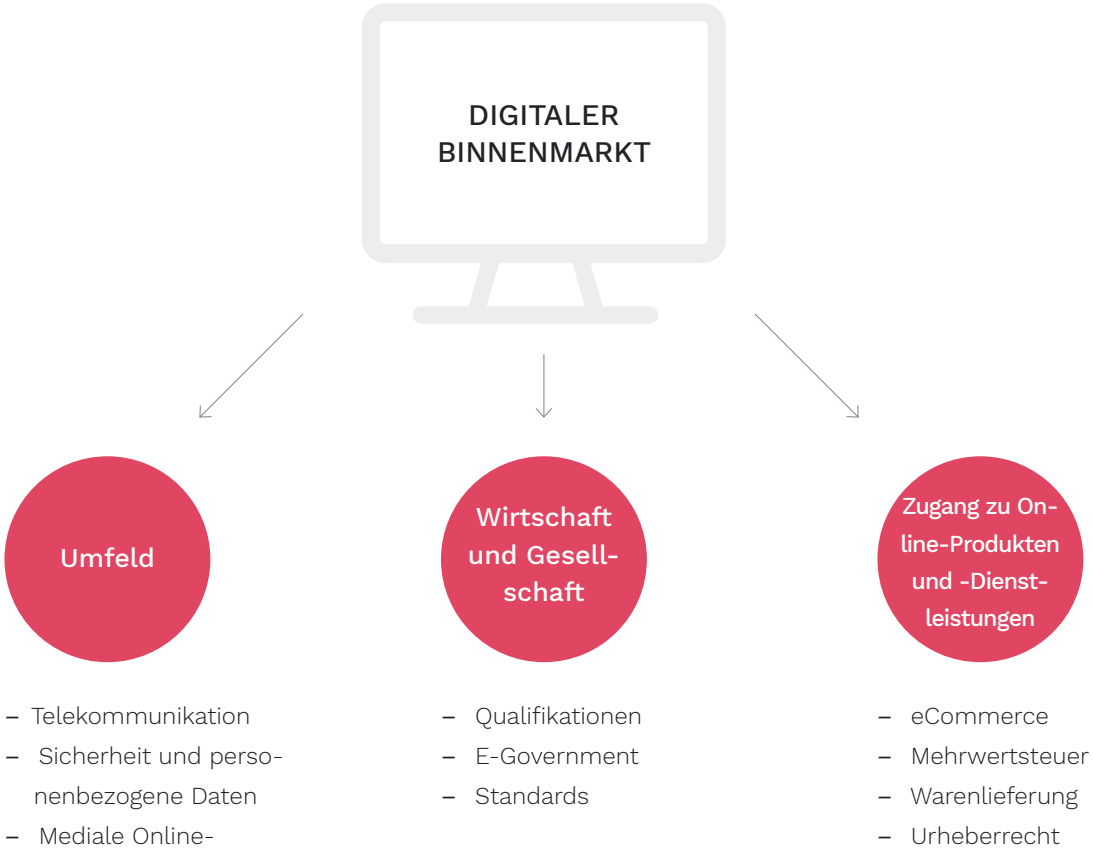
3. Gleichzeitig können europäische Gesetzgeber die Auseinandersetzung mit dem Thema Cybersicherheit nicht vermeiden, denn **im Alltag und in der Wirtschaft wird die Abhängigkeit von digitalen Technologien immer größer** und es besteht eine **Gefährdung von Bürgern durch schwerwiegende Cyber-Vorfälle.**

4. Es ist **ein sich entwickelnder und komplexer Problembereich**, der Auswirkungen auf das reibungslose Funktionieren des digitalen Binnenmarkts hat.

Die EU ist bestrebt, ein faires, offenes und sicheres digitales Umfeld zu gewährleisten

Relevante Dokumente der EU-Politik zur Cybersicherheit sowie legislative Maßnahmen finden sich, die innerhalb ihres Bezugsrahmens Folgendes addressieren:

1. Netzwerk- und Informationssicherheit
2. Elektronische Kommunikation (einschließlich Fragen der Privatsphäre und des Datenschutzes)
3. Cyberkriminalität
4. Cyber-Abwehr



Gewährleistung des Grundrechtsschutzes

Die digitale Wirtschaft der EU könnte um bis zu 4% ihres BIP wachsen sofern die richtigen Rahmenbedingungen, einschließlich der geeigneten legislativen und politischen Maßnahmen, vorhanden wären.

Die EU-Rechtsvorschriften zur Cybersicherheit **berühren ein breites Spektrum von Grundrechten**, die in der EU-Charta der Grundrechte vorgesehen sind, wie z.B. Meinungsfreiheit, Gleichberechtigung, Rechte älterer Menschen oder unternehmerische Freiheit.

Allerdings tendieren Folgenabschätzungen und Diskussionen über Gesetzesinitiativen dazu, **einen zu engen Fokus** nur auf die Achtung des Privat- und Familienlebens sowie das Recht auf den Schutz personenbezogener Daten zu haben. Eine eingehendere, ganzheitlichere Analyse der Auswirkungen auf die Gesamtheit der Grundrechte ist erforderlich.

Die Charta der Grundrechte der EU

Jeder Gesetzesvorschlag der Europäischen Kommission, einschließlich jener welche die Cybersicherheit betreffen müssen mit den festgelegten Rechten und Freiheiten vereinbar sein, die in der Charta der Grundrechte der EU niedergelegt sind.

Wichtige Fakten:

- Die Charta basiert auf der Idee, dass der Schutz von Grundrechten eine „unerlässliche Bedingung für die Legitimität der Union“ ist.
- Die erste Verkündung erfolgte auf dem Gipfel des Europäischen Rates in Nizza in 2000 und ist seit dem Inkrafttreten des Vertrags von Lissabon im Jahr 2009 rechtverbindlich.
- Die Charta ergänzt die nationalen Dokumente zu Menschenrechten sowie die Europäische Menschenrechtskonvention (EMRK).
- Sie enthält die jüngste Kodifizierung von Grundrechten in Europa.

Werte in der Charta der Grundrechte der EU

Gesetzgeber sollten ein breiteres Spektrum von Werten und Grundrechten in Betracht ziehen welche von EU-Cybersicherheitsgesetzen und Regulierungsmaßnahmen betroffen sind oder sein können, wie z.B.

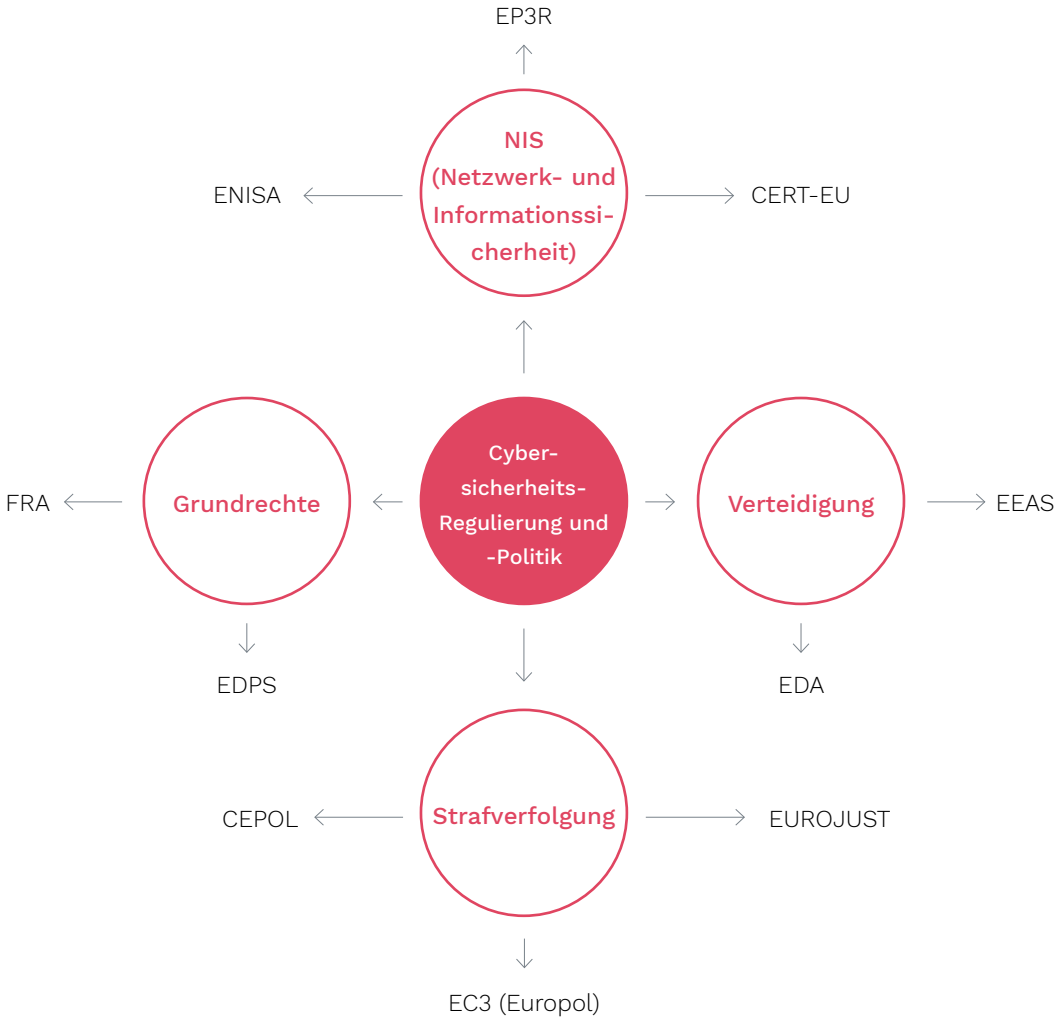
- Menschenwürde
- Freiheit
- Gleichstellung
- Solidarität
- Demokratie
- Rechtsstaatlichkeit
- Achtung der Vielfalt der Kulturen und Traditionen der Völker Europas (Pluralismus)
- Subsidiarität (unter Beachtung ihrer Behördenstruktur auf nationaler, regionaler und lokaler Ebene)
- Ausgewogene und nachhaltige Entwicklung
- Freier Personen-, Dienstleistungs-, Waren- und Kapitalverkehr sowie Niederlassungsfreiheit

Opt-out-Länder:
Großbritannien, Polen und die Tschechische Republik.

Ein Überblick über spezialisierte EU-Einrichtungen, welche an Regulierung und Politik der Cybersicherheit beteiligt sind.

Alle EU-Organe (d. h. die Europäische Kommission, das Parlament und der Rat), Agenturen und Einrichtungen sind durch die Charta der Grundrechte der EU gebunden.

Das cybersicherheitsbezogene institutionelle Gefüge der EU ist komplex und vielschichtig und erstreckt sich über eine Reihe von internen Politikbereichen. Es erkennt an, dass die Beantwortung von Cybersicherheitsfragen die Zusammenarbeit mehrerer Stakeholder mit unterschiedlichem Fachwissen erfordert.



Trotz dieser Herausforderungen gibt es Möglichkeiten, europäische Werte in den gesetzgeberischen Rahmen und in die Politik einzubetten.

Herausforderungen bei der Regulierung der Cybersicherheit

Es ist wichtig, die Herausforderungen beim Schutz der Grundrechte auf EU-Ebene im digitalen Umfeld zu erkennen. Solche Herausforderungen sind:

1. Der Bereich der Cybersicherheit entwickelt sich ständig weiter und besteht aus stark verstreuten Gesetzgebungsmaßnahmen.

2. Die Cybersicherheit ist ein Querschnittsthema und zugleich ein gemeinsamer Nenner verschiedener neuer Technologien, die mit dem Internet verbunden sind.

3. Kooperationsabkommen zwischen EU-Organen und -Agenturen könnten Aspekte umfassen, welche den Schutz der Grundrechte betreffen.

Empfehlung 1: Anreiz für die gerichtliche Überprüfung von EU-Rechtsvorschriften durch den EuGH

Es gibt eine zunehmende Rechtsprechung des Gerichtshofs in Bezug auf die Vereinbarkeit der EU-Charta mit der sog. EU Richtlinie zur Vorratsdatenspeicherung. Diese Richtlinie zwang Internetdienstanbieter (Internet Service Providers, ISPs) und Telekommunikationsunternehmen, welche in der Union tätig sind, die Nutzungsdaten ihrer Kunden zu erheben und auf Vorrat aufzubewahren.

Die Judikative prüfte, ob eine angemessene Abwägung zwischen den verschiedenen Interessen vorgenommen wurde, während sie dazu aufforderte, die Grundrechte schon von Beginn des gesetzgeberischen Prozesses an ernsthaft zu berücksichtigen.

Beispiele:

Urteil Digital Rights Ireland vom 8. April 2014 (verbundene Rechtssachen C-293/12 und C-594/12)

Stellungnahme 1/15 zum Abkommen über Fluggastdatensätze zwischen der EU und Kanada

Empfehlung 2: Beibehaltung eines wertorientierten EU-Cybersicherheitsansatzes

Förderung der folgenden Maßnahmen:

1. Durchführung einer Folgenabschätzung für die finale Fassung eines Gesetzestextes. Dies würde die Übereinstimmung mit den Werten, die in der EU-Charta verankert sind, verbessern.

2. Einbeziehung verschiedener Interessengruppen in die Gesetzeskonsultationen, wie z. B. spezialisierte EU-Einrichtungen (z. B. EDPS, ENISA), Nichtregierungsorganisationen und andere relevante Stakeholder.

3. Entwicklung neuer Legislativverfahren, wie z.B. beim Prinzip des Datenschutzes durch Technik (data protection by design), welche die Anforderungen aus der Datenschutzgrundverordnung zusätzlich stützen.

4. Trachten nach einer akzentuierteren Nutzung wbestehender Maßnahmen und Prinzipien (z. B. die Umsetzung geeigneter Sicherheitsmaßnahmen).

5. Kooperationsabkommen zwischen EU-Einrichtungen und -Institutionen können Aspekte integrieren, die den Schutz der Grundrechte addressieren.

Weitere Informationen finden Sie hier

Die Folien basieren auf der Forschungsarbeit des CANVAS-Projekts (Constructing an Alliance for Value-driven Cybersecurity).

Ziel von CANVAS ist es, Stakeholder aus Schlüsselbereichen der Europäischen Digitalen Agenda zusammenzubringen, um der Herausforderung zu begegnen, wie Cybersicherheit mit europäischen Werten und Grundrechten in Einklang gebracht werden kann.

Insbesondere stellen wir die folgenden CANVAS-Ressourcen zur Verfügung:

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

Die Folgefolie verweist direkt auf jene unserer White Paper, die sich ausführlich mit den Herausforderungen der Cybersicherheit befassen.

Bibliographie: Herausforderungen der Cybersicherheit (CANVAS White Papers)

Ethische Herausforderungen

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.

Rechtliche Herausforderungen

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.

Technische Herausforderungen

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.

Bibliographie

Vertrauen – generell – philosophisch

- Held, Virginia. 1968. “On the Meaning of Trust.” Ethics 78 (2): 156–59.
- Baier, Annette. 1986. “Trust and Antitrust.” Ethics 96 (2): 231–60.
- Pettit, Philip. 1995. “The Cunning of Trust.” Philosophy & Public Affairs 24 (3): 202–25.
- Becker, Lawrence C. 1996. “Trust as Noncognitive Security about Motives.” Ethics 107 (1): 43–61.

Vertrauen – generell – Sozialwissenschaften

- Frey, Bruno S. 1994. “How Intrinsic Motivation Is Crowded out and In.” Rationality and Society 6 (3): 334–52.
- Ostrom, Elinor. 2000. “Collective Action and the Evolution of Social Norms.” The Journal of Economic Perspectives 14 (3): 137–58.
- Frohlich, Norman, and Joe A. Oppenheimer. 1996. “Experiencing Impartiality to Invoke Fairness in the N-PD: Some Experimental Results.” Public Choice 86 (1): 117–35. https://doi.org/10.1007/BF00114878.

Vertrauen – online – digital

- Erlich, Yaniv, et al. 2014. “Redefining Genomic Privacy: Trust and Empowerment.” PLOS Biology 12 (11): e1001983.
- Etzioni, Amitai. 2017. “Cyber Trust.” Journal of Business Ethics, July. https://doi.org/10.1007/s10551-017-3627-y.
- Chakravorti, B., Bhalla, A., Chaturvedi, R.S., 2018. The 4 Dimensions of Digital Trust, Charted Across 42 Countries. Harvard Business Review.

Fakten zum Projekt

Projektkoordination und Kontakt:
PD Dr. sc. sc. ETH Markus Christen
Universität Zürich (UZH), Digital Society Initiative
Rämistrasse 66, 8001 Zürich

Slidedocs-Version:
Version 2.0 Oktober 2019

Projektdauer:
Sept. 2016 - Okt. 2019

Partner:
Das CANVAS-Konsortium besteht aus 11 Partnern (9 akademische Institutionen und 2 Partner außerhalb der akademischen Welt) in 7 europäischen Ländern.

Finanzierung:
1,57 Mio. €, wovon 1 Mio. € von der Europäischen Kommission finanziert wird und der restliche Teil aus dem Schweizer Staatssekretariat für Bildung, Forschung und Innovation stammt.

Förderhinweis für CANVAS

Kofinanziert durch das Programm
„Horizont 2020“ der Europäischen Union

Das Projekt CANVAS (Constructing an Alliance for Value-driven Cybersecurity) wurde im Rahmen der Fördervereinbarung Nr. 700540 aus dem Forschungs- und Innovationsprogramm Horizon 2020 der Europäischen Union finanziert. Diese Arbeit wurde (teilweise) vom Staatssekretariat für Bildung, Forschung und Innovation (SERI) unter der Vertragsnummer 16.0052-1 unterstützt. Die darin geäußerten Meinungen und Argumente spiegeln nicht unbedingt die offizielle Meinung der Schweizer Regierung wider.