POLICY BRIEF NO. 3

ALLE GRUNDRECHTE SIND FÜR DIE CYBERSICHERHEIT RELEVANT

Ein umfassender Ansatz für den Schutz der Grundrechte in der EU-Cybersicherheit

Wann immer die Europäische Kommission Vorschläge für die Politik und die Regulierung im Bereich der Cybersicherheit vorlegt, konzentriert sich ihre Bewertung oft lediglich auf ihre Vereinbarkeit mit dem Recht auf Schutz personenbezogener Daten und dem Recht auf Achtung des Privat- und Familienlebens. In der Tat gehören diese Rechte auf Datenschutz und Privatsphäre zu den wichtigsten Anliegen im digitalen Bereich. Doch während diese beiden Rechte, die in den Artikeln 7 und 8 von der Charta der Grundrechte der Europäischen Union (EU-Charta) verankert sind, nach wie vor zu berücksichtigen sind, sollten politische Entscheidungsträger ein breiteres Spektrum von Grundrechten in Betracht ziehen, welche von der EU-Cybersicherheitspolitik und den Regulierungsmaßnahmen der EU betroffen sind oder sein könnten.

Politische Entscheidungsträger sollten ein breiteres Spektrum von Grundrechten in Betracht ziehen, die durch EU-Cybersicherheitsrichtlinien und Regulierungsmaßnahmen betroffen sind oder sein können.

Europäisches Primärrecht verlangt den Schutz von europäischen Werten

Gemäß Artikel 2 des EU-Vertrags heißt es: „Die Werte, auf die sich die Union gründet, sind die Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte einschließlich der Rechte der Personen, die Minderheiten angehören.“ Diese EU-Werte werden durch die Grundsätze des Pluralismus, der Nichtdiskriminierung, der Toleranz, der Gerechtigkeit und der Gleichbehandlung von Männern und Frauen bestimmt und sind in der EU-Charta näher beschrieben. Darüber hinaus sieht die EU-Charta ein breites Spektrum von Grundrechten vor, die EU-Bürger und Einwohner genießen, einschließlich der Rechte auf ein faires Verfahren, Gedankenfreiheit, Meinungs- und Informationsfreiheit, Rechte auf Eigentum, Bildung und wirksame Rechtsbehelfe. Diese Werte und Rechte müssen sich in den Regulierungsmaßnahmen der Europäischen Union widerspiegeln.

Schritt 1: Anerkennung von Herausforderungen des Schutzes der Grundrechte auf EU-Ebene im digitalen Umfeld

In den Richtlinien und Verordnungen der EU im Bereich der Cybersicherheit wird anerkannt, dass alle Maßnahmen, die in Bezug auf den Schutz der EU-Bürger, der Gesellschaft sowie der Informationssysteme und der Infrastruktur ergriffen werden, im Einklang mit der Verpflichtung zur Achtung der grundlegenden Menschenrechte entwickelt werden sollten.

So stellt beispielsweise die NIS-Richtlinie in ihrer Begründung 75 fest, dass die Richtlinie „[...] mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang [...]“ steht. Daher soll die Richtlinie im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden.

Cybersicherheit kann nur dann solide und wirksam sein, wenn sie auf den Grundrechten, Freiheiten und Werten beruht, wie sie in der Charta der Grundrechte der Europäischen Union verankert sind.

Trotz der Anerkennung der zentralen Rolle, welche die Grundrechte spielen, erweist sich ihre praktische Umsetzung allerdings immer noch als schwierig. Die Komplexität des Themas wird durch europäische Governance-Vereinbarungen noch verstärkt – eine Vielzahl an Gremien und Institutionen, die sich mit Fragen der Cybersicherheit befassen, haben Zuständigkeiten in diesem Bereich. So konzentriert sich beispielsweise die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) auf ein hohes Maß an ebenjener Netz- und Informationssicherheit. Die Europäische Verteidigungsagentur (EDA) spielt eine Rolle in der europäischen militärischen Koordination, Sicherheits- und Verteidigungspolitik, während Europol die Mitgliedstaaten darin unterstützt, in Fällen von Cyberkriminalität zu ermitteln. Darüber hinaus kümmert sich das Computer Emergency Response Team für die EU-Institutionen, Agenturen und Einrichtungen (CERT-EU) um die Sicherung der europäischen IT-Infrastruktur. Obwohl alle diese Einrichtungen über Mittel zur Zusammenarbeit und zum Informationsaustausch verfügen, ist nicht klar, ob, inwieweit und bei welchen von ihnen hinreichende Grundrechtsschutzmechanismen vorgesehen sind.

Schritt 2: Gerichtliche Überprüfung von EU-Rechtsvorschriften

Der Europäische Gerichtshof (EuGH) legt das EU-Recht auch im Hinblick auf Maßnahmen zur Cybersicherheit aus. Durch seine Rechtsprechung betont der EuGH: „Die Anwendbarkeit des Unionsrechts umfasst die Anwendbarkeit der durch die Charta garantierten Grundrechte.“

Ein Musterfall für die Rechtsprechung des EuGH, welche die Nichteinhaltung der europäischen Grundrechte feststellt, ist die Entscheidung über die Geltung der Richtlinie 2006/24/EG über die Aufbewahrung von Daten, welche im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden (Richtlinie zur Vorratsdatenspeicherung).

Diese Richtlinie wurde von der Großen Kammer des Gerichtshofs mit der Begründung für nichtig erklärt, dass die flächendeckende Erhebung von Kommunikationsdaten, insbesondere Verkehrsdaten und Standort, durch Anbieter von Kommunikationsanbietern nicht verhältnismäßig (d.h. übermäßig) sei. Daher stelle diese Gesetzgebung eine Verletzung der Rechte auf Privatsphäre und auf den Schutz personenbezogener Daten von Individuen dar. Während die Gerichtsentscheidung nicht automatisch die Rechtsvorschriften der Mitgliedstaaten selbst zur Umsetzung der Vorratsdatenspeicherungsrichtlinie aufhob, ist die Richtlinie exemplarisch für eine regulatorische Maßnahme, welche als unvereinbar mit den in der EU-Charta verankerten Rechten erklärt worden ist.

Die Stellungnahme 1/15 des EuGH zum Entwurf eines Abkommens zwischen der Europäischen Union und Kanada über die Übermittlung von Fluggastdatensätzen (Passenger Name Records, PNR) ist ebenfalls ein anschauliches Beispiel dafür, wie wichtig die Einhaltung der von der EU anerkannten Grundrechte ist. In dieser Stellungnahme kam der EuGH zum Schluss, dass das geplante Abkommen in seiner jetzigen Form nicht abgeschlossen werden sollte, da die Vorschriften für die Übermittlung von PNR-Daten aus der EU nach Kanada einen Eingriff in die Grundrechte auf Achtung der Privatsphäre und Schutz personenbezogener Daten darstellen.

Diese Beispiele zeigen, dass die Werte, die sich aus der EU-Charta ergeben, zuweilen durch EU-Gesetzgebung herausgefordert werden. Dennoch werden solche gerichtlichen Überprüfungen von Gesetzesmaßnahmen nicht standardmäßig durchgeführt, sondern sind von proaktiven EU-Institutionen oder Richtern an nationalen Gerichten abhängig. Die gerichtliche Überprüfung der EU-Gesetzgebung ist ein wesentliches Mittel für den Schutz der EU Werte und sollte standardmässig erfolgen.

Schritt 3: Beibehaltung eines werteorientierten EU-Ansatzes zur Cybersicherheit

Nur eine starke Betonung des Schutzes der Grundrechte kann zu einer wertorientierten Cybersicherheit beitragen. Die Cybersicherheitsstrategie 2013 beansprucht dies: „Die Sicherheit im Cyberraum kann nur zufriedenstellend und wirksam gewährleistet werden, wenn sie auf den in der Charta der Grundrechte der Europäischen Union garantierten Grundrechten und Grundfreiheiten und auf den Grundwerten der EU basiert." Dennoch wird dieser Ansatz oft von den EU-Institutionen selbst in Frage gestellt, wie im vorherigen Abschnitt dargestellt wurde. Um diesen Ansatz beizubehalten und die EU-Charta einzuhalten, muss die EU ihre Werte in den geltenden Rechtsrahmen einbetten.

Dies jedoch in die Praxis umzusetzen ist keine einfache Aufgabe, wenn es um die effektive Entwicklung und Anwendung von EU Verordnungen und Richtlinien geht. Der Umsetzungsprozess erfordert ein umfassendes Verständnis davon, was „Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte einschließlich der Rechte der Personen, die Minderheiten angehören" genau bedeutet.

Darüber hinaus ist ein gründliches Verständnis des Bereichs, auf den die Gesetzgebung abzielt erforderlich, während die bestmögliche Nutzung des gesamten Fachwissens nur durch proaktive Einbeziehung, Handeln und Zusammenarbeit verschiedener Interessengruppen erreicht werden kann. Die Einbettung der in der EU-Charta verankerten Werte kann sowohl ex ante als auch ex post erfolgen (z. B. durch gerichtliche Überprüfung).

Ex-ante-Basis: Folgenabschätzungen und Konsultation von Interessengruppen

Jene EU-Organe, welche Gesetzgebungsbefugnisse ausüben, nämlich die Europäische Kommission, der Rat der EU und das Europäische Parlament, können in dieser Hinsicht zusammen mit EU-Agenturen, insbesondere der ENISA, ex ante eine wichtige Rolle spielen[1]. So hat beispielsweise die Europäische Kommission bewährte Verfahren zur Durchführung von Kompatibilitätsprüfungen und Folgenabschätzungen von Gesetzesvorschlägen entwickelt. Diese Praktiken sollten das Risiko mindern, dass vorgeschlagene legislative Maßnahmen gegen die Grundrechte verstoßen. Das bei diesem Prozess gewonnene Wissen kann dann den Entscheidungsprozess erleichtern und sicherzustellen, dass jene Vorgehensweise umgesetzt wird, welche die Erfüllung der Grundrechte am besten unterstützt. Dennoch wird oft die Bedeutung dieser Instrumente während des Gesetzgebungsprozesses in Frage gestellt. Dies geschieht insbesondere durch spätere Änderungsanträge, die erhebliche Abweichungen vom ursprünglichen Text mit sich bringen, der sich auf den Schutz der Grundrechte bezog.

1 De Schutter, O., The Implementation of the Charter of Fundamental Rights in the EU institutional framework, Study for the AFCO Committee, 2016.

Im Bereich der Cybersicherheit haben sich Konsultationen und Beiträge der spezialisierten EU-Organe wie EDPS, ENISA und des Europäischen Datenschutzausschusses als nützlich erwiesen und es ermöglicht, die Grenzen der ersten Kompatibilitätsprüfungen und Folgenabschätzungen zu überwinden. Gleichzeitig wäre es eine begrüßenswerte Entwicklung, eine Folgenabschätzung für den endgültigen Text einer Legislativmaßnahme durchzuführen. Darüber hinaus kann auch ein partizipatorischer Ansatz die Integration von EU-Werten in den Rechtsrahmen und in die Regelwerke erleichtern. So wird beispielsweise in der Entwurfsphase von Legislativvorschlägen von der Europäischen Kommission in der Regel ein öffentlicher Konsultationsprozess eingeleitet, um die zentralen Anliegen der betroffenen Interessengruppen zu klären. Die Europäische Kommission hat gar eine dementsprechende Verpflichtung: „Um die Kohärenz und die Transparenz des Handelns der Union zu gewährleisten, führt die Europäische Kommission umfangreiche Anhörungen der Betroffenen durch".[2] Auf der Grundlage der Beiträge, die während des öffentlichen Konsultationsprozesses eingegangen sind, muss die Europäische Kommission Maßnahmen vorschlagen, welche die unterschiedlichen Interessen der Beteiligten ausgleichen könnten. Diese Maßnahmen müssen ebenfalls mit den in der EU-Charta verankerten Werten vereinbar sein. Nach Abschluss der Konsultationen können die betroffenen Interessengruppen aktiv bleiben, indem sie ihre Kommentare zu den Gesetzesvorschlägen in verschiedenen Phasen des legislativen Prozesses abgeben.

Einige Organisationen, insbesondere diejenigen, die Gruppen der Zivilgesellschaft vertreten, liefern oft detaillierte Analysen darüber, wie eine künftige Gesetzesmaßnahme die Bestimmungen der EU-Charta besser umsetzen könnte. Damit diese Analysen jedoch vom Gesetzgeber berücksichtigt werden können, müssen die betroffenen Interessengruppen oft kostspielige Lobbykampagnen durchführen. Daher sind üblicherweise die Interessengruppen der Wirtschaft weiterhin besser vertreten.

Alternative Wege zur Aufrechterhaltung eines europäischen Ansatzes für die Regulierung der Cybersicherheit

Neben Kompatibilitätsprüfungen, Folgenabschätzungen von Regulierungsvorschlägen und der Beteiligung der Interessengruppen kann der Gesetzgeber wählen, ob er bestimmte Werte im Gesetzestext besonders hervorheben möchte, wie beispielsweise den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 Abs. 1 DSGVO). Dieser verlangt ausdrücklich, dass die für die Verarbeitung personenbezogener Daten Verantwortlichen geeignete technische und organisatorische Maßnahmen ergreifen. Diese sollen die Risiken mindern, welche sich aus der Verarbeitung ergeben. Dadurch werden die Rechte und Freiheiten von Personen geschützt, deren Daten verarbeitet werden. Diese Maßnahmen sollten sicherstellen, dass die Anforderungen und Grundsätze der DSGVO von Anfang bei der vorgesehenen Verarbeitungstätigkeit berücksichtigt und kontinuierlich überprüft werden. In der Praxis verstärkt dieser Grundsatz die schon in Artikel 5 DSGVO genannten Prinzipien, die für jede Verarbeitung personenbezogener Daten gelten. Ähnliche regulative Ansätze könnten in Betracht gezogen werden, um ein insgesamt wertorientiertes EU-Vorgehen für mehr Cybersicherheit zu pflegen, bei dem die Bedeutung aller Grundrechte im digitalen Bereich anerkannt wird.

2 Konsolidierte Fassung des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union (2010/C 83/01); Vertrag über die Europäische Union (EUV), Artikel 11 Absatz 3.

Mehr Informationen

Dieser Policy Brief basiert auf der Forschungsarbeit des CANVAS-Projekts (Constructing an Alliance for Value-driven Cybersecurity). Detaillierte Berichte über diese Arbeit wurden in vier wichtigen Whitepapers in englischer Sprache veröffentlicht:

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

Alle Whitepapers finden Sie auf unserer Website, zusammen mit allen unseren (herunterladbaren und druckbaren) Policy Briefs, kurze Online-Erklärungen zu den wichtigsten Fragen der Cybersicherheit und kommentierte Literaturlisten zur vertieften Lektüre:

canvas-project.eu

Darüber hinaus finden Sie auf unserer Website noch mehr CANVAS Projektmaterial:

CANVAS Reference Curriculum
(Integration der Werteperspektive in die Aus- und Weiterbildung im Bereich Cybersicherheit)

CANVAS MOOC
(Massive Open Online Kurs)

Open Access Buch
“The Ethics of Cybersecurity”

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.

Projektdauer:
September 2016 – Oktober 2019

Ziel von CANVAS:
Die Zusammenführung von Interessengruppen aus Schlüsselbereichen der Europäischen Digitalen Agenda, um der Herausforderung zu begegnen, wie die Cybersicherheit mit den europäischen Werten und Grundrechten in Einklang gebracht werden kann.

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

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

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

Version und Veröffentlichungsdatum:
Version 2.0, Oktober 2019