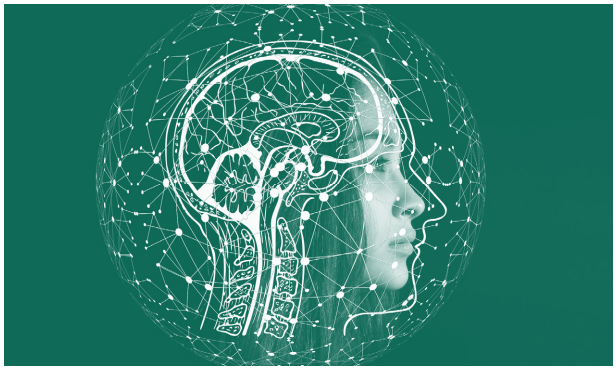
BRAUCHEN NEUE TECHNOLOGIEN NEUES RECHT?

IN KÜRZE

- Informations- und Kommunikations-technologien (IKT) entwickeln sich rasant weiter und stellen Politik und Regulierung vor große Herausforderungen.
- IKT stellen gleichzeitig eine Voraussetzung für und eine Bedrohung von Sicherheit dar. Die Herstellung von Sicherheit und der Schutz der Privatsphäre lassen sich am ehesten als nicht immer konfliktfreie Symbiose beschreiben.
- Die Einflüsse reichen von einer individuellen Ebene bis zum globalen Kontext. Entsprechend müssen auch Lösungsansätze auf allen Ebenen gesucht und gefunden werden.

WORUM GEHT ES?

Informationstechnologien, wie Künstliche Intelligenz-(KI)-Systeme oder Mobilfunknetze, werden immer leistungsfähiger und spielen in immer mehr beruflichen und privaten Bereichen eine Rolle. Auch Politik und Regulierung müssen sich mit immer neuen Fragestellungen in diesem Bereich auseinandersetzen. Wie können bei dieser rasanten Entwicklung aber wichtige ethische und rechtliche Erfordernisse bei der Entwicklung und beim Einsatz von IKT – etwa im Bereich Überwachungstechnologien – berücksichtigt werden? Wo sind bestehende Regelungen ausreichend, und wo müssen neue Richtlinien entwickelt und eingesetzt werden? Welche Empfehlungen müssen aktualisiert werden, um eine ethisch vertretbare Nutzung von Überwachungstechnologien zu ermöglichen? Können die immensen Datenmengen, die bei der Nutzung von IKT, z.B. von sozialen Netzwerken, anfallen, für Sicherheitszwecke genutzt werden ohne ethische Werte oder Grundrechte zu verletzen? Wie kann der tatsächliche oder vermeintliche Konflikt zwischen Privatsphäre und Sicherheit aufgelöst werden? Diese Fragen sind komplex. Umso mehr, wenn man bedenkt, dass Datenschutz eine Voraussetzung für (Cyber-)Sicherheit ist. Der Schutz der Privatsphäre ist darüber hinaus ein zentrales Element der Menschenrechte, die Schutz vor dem Missbrauch staatlicher und wirtschaftlicher Macht bieten sollen.



IKT als Überwachungs- und Sicherheitstechnologie: Ethische Probleme durch unzureichende Regulierung?

Das PANELFIT-Projekt untersuchte Probleme bei der Nutzung von IKT für Sicherheitszwecke. Zentrale Fragen waren dabei: Sind bestehenden Regelungen, wie etwa die Datenschutzgrundverordnung, stark genug? Werden bestehende gesetzliche Bestimmungen ausreichend durchgesetzt? Welche neuen Maßnahmen oder Anpassungen braucht es in so einem bewegten Feld wie der KI? Kann Regulierung sogar ethische Probleme entstehen lassen oder sie verstärken, etwa beim Versuch, Fake-News durch private Zensur einzudämmen? Ziel war, Maßnahmen vorzuschlagen, die eine ethisch vertretbare Nutzung von IKT zu Sicherheits- oder Überwachungszwecken möglich macht. Im Vordergrund stehen dabei der Einsatz und die Entwicklung von Technologien im Einklang mit Grundrechten und europäischen Werten. Wesentlich ist auch, F&E-Programme so zu gestalten, dass daraus ethisch vertretbare und im Einklang mit Grundrechten einsetzbare Technologien resultieren.

ECKDATEN

Projekttitel:	Participatory Approaches to a New Ethical and Legal Frame work for ICT (PANELFIT)
Projektteam:	Čas, J., Krieger-Lamina, J., Peissl, W., Schaber, F. (in int. Konsortium)
Laufzeit:	11/2018 – 04/2022
Auftraggeber:	EU-Horizon 2020
Webseite:	www.panelfit.eu

WESENTLICHE ERGEBNISSE

„Sicherheit" ist kein eindeutiger Begriff. Die vielen Facetten von Sicherheit führen zu rechtlicher Unsicherheit und verleiten zur missbräuchlichen Verwendung. Das Verhältnis von Privatheit und Freiheit einerseits und Sicherheit andererseits ist keine antagonistische Beziehung. Damit demokratische Gesellschaften Bestand haben können, muss beides gewährleistet sein. Dieses Gleichgewicht droht verloren zu gehen.

Zukünftige Kommunikationstechnologien, wie etwa 6G-Netze, bieten in Zusammenarbeit mit neuen KI-gestützten Analyseverfahren viel genauere und umfassendere Möglichkeiten der Überwachung, die auch physikalische Barrieren wie Mauern überwinden kann. Das Machtungleichgewicht zwischen Individuen und Regierungen bzw. privaten Unternehmen droht damit weiter zuzunehmen. Aber auch Staaten selbst sind betroffen.

Die Dominanz, insbesondere von US-Unternehmen, bei neuen IKT verringert die Souveränität europäischer Staaten.

Soziale Netzwerke werden missbraucht, Bürger*innen zu manipulieren, Wahlergebnisse zu beeinflussen und den sozialen Zusammenhalt zu zerstören. Sie gefährden die Existenz demokratischer Gesellschaften. Algorithmenbasierte Zensur in privater Hand als Gegenmaßnahme stellt eine weitere Bedrohung für Meinungsfreiheit und demokratische Debatten dar.

Einzelne Technologien bzw. Anwendungen werfen gravierende ethische Probleme auf. Beispiele dafür sind Verfahren zur Erkennung von Emotionen, die Nutzung von KI bei sicherheitsrelevanten Entscheidungen oder für prädiktive Polizeiarbeit. Wenn Menschen Verfahren ausgesetzt werden oder Entscheidungen unterworfen werden, die auf intransparenten oder nicht erklärbaren Technologien beruhen, wird die Menschenwürde verletzt. Prädiktive Verfahren wiederum stehen im Widerspruch zum Prinzip der Unschuldsvermutung.

WAS TUN?

Komplexe Herausforderungen können oft mit einfachen, aber konsequenten Antworten bewältigt werden. Deren Umsetzung erfordern aber ein radikales Umdenken und große Anstrengungen.

- Der Fortbestand von Demokratien ist eine zentrale Voraussetzung für Sicherheit. Wenn Demokratien Bestand haben sollen, müssen Sie sich selbst ernst nehmen. D. h. dafür zu sorgen, dass Gesetze, Grundsätze und Werte auch konsequent verteidigt und umgesetzt werden.
- Ein Festhalten an Grundsätzen bedeutet auch eine Abkehr von der üblichen Praxis, Konflikten zwischen neuen Technologien und bestehenden Regulierungen mit dem Ruf nach gesetzlichen Anpassungen zu begegnen. Wenn Grundrechte Bestand haben sollen, müssen Technologien an diese angepasst werden, und nicht umgekehrt.
- Sicherheit hat auch eine wirtschaftliche Dimension. Die Folgen der Covid-19-Pandemie und insbesondere des Krieges in der Ukraine zeigen deutlich, wie wichtig es ist, auch im Bereich IKT auf Produktionskapazitäten und Ressourcen der Europäischen Union zurückgreifen zu können, um nicht abhängig und erpressbar zu sein.
- Eine risikobasierte Regulierung, wie im Entwurf für ein KI-Gesetz der EU vorgesehen, ist nicht ausreichend. Nur klare Vorgaben können helfen, auch noch nicht bekannte Risiken zu minimieren.

ZUM WEITERLESEN

Čas, J. (2019). Issues and gap analysis on security and cybersecurity ELI in the context of ICT research and innovation (PanelFit Deliverable 4.1) (61 pp.). Wien
panelfit.eu/wp-content/uploads/2020/11/D41-Issues-and-gap-analysis-on-Security-and-Cybersecurity-ELI-in-the-context-of-ICT-research-and-innovation.pdf

KONTAKT

Johann Čas
E-Mail: *tamail@oeaw.ac.at*
Telefon:+43 1 51581-6582

IMPRESSUM: Medieninhaber: Österreichische Akademie der Wissenschaften; Juristische Person öffentlichen Rechts (BGBl. 569/1921 i.d.F. BGBl. I 31/2018); Dr. Ignaz Seipel-Platz 2, A-1010 Wien; Herausgeber: Institut für Technikfolgen-Abschätzung (ITA); Bäckerstr. 13, A-1010 Wien; *www.oeaw.ac.at/ita* | Erscheinungsweise: Die ITA-Dossiers erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des ITA. Die Dossiers werden in kleiner Auflage gedruckt und open access über das Portal „epub.oeaw" zur Verfügung gestellt: *epub.oeaw.ac.at/ita/ita-dossiers* | ISSN: 2306-1960

ITA-Dossier Nr. 67, Oktober 2022, *epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier067.pdf*