PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Bürgerinformationspaket und Leitfaden für schutzbedürftige Personen

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung-Keine kommerzielle Nutzung-Keine Bearbeitung 4.0 Internationalen Lizenz.

Dieses Projekt wurde mit Mitteln aus dem Programm für Forschung und Innovation Horizont 2020 der Europäischen Union unter der Finanzhilfevereinbarung Nr. 788039. gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung trägt allein der Verfasser; die Agentur haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Informationen zum Projekt

Titel des Projekts	Partizipative Ansätze für einen neuen ethischen und rechtlichen Rahmen für IKT
Projekt-Akronym	PANELFIT
Nummer der Finanzhilfevereinbarung	788039
Projektkoordinator	UPV/EHU

Informationen zum Dokument

Nummer des Meilensteins	D5.5
Titel des Dokuments	Bürgerinformationspaket
Version des Dokuments	3.0
Datum des Dokuments	22. April 2022
Arbeitspaket	WP5
Aufgabe	Aufgabe 5.7
Dokumentenleitung	OBCT / ECSA
Urheberrechtslizenz	Creative Commons Namensnennung-Keine kommerzielle Nutzung-Keine Bearbeitung 4.0 Internationale Lizenz
Verteilungsstufe	PU = Uneingeschränkter ÖFFENTLICHER Zugang – EU-Projekt
Vertragliches Fälligkeitsdatum	31.08.2021 (Monat 34)

An dem Dokument beteiligte Projektpartner

Nr.	Name der Organisation	Akronym
1	Universidad del País Vasco / Euskal Herriko Unibertsitatea	UPV/EHU
7	European Citizen Science Association	ECSA
8	European Network of Research Ethics Committees	EUREC
9	Institut de Ciències del Mar (Consejo Superior de Investigaciones Científic	ICM-CSIC
10	OBC Transeuropa	OBCT

Dokumentenhistorie

Status	Version	Datum	Autor(en)	Überprüft von
Entwurf	V1.0	21.7.2021	Tim Woods (ECSA)	
Bearbeitung	V1.1	22.7.2021		Iñigo de Miguel Beriain (UPV/EHU)
Bearbeitung	V1.2	18.8.2021		Federico Caruso (OBCT)
Finale Version	V2.0	19.8.2021		
Finale Version	V3.1	31.8.2021		Roberta Monachello (EU)
Finale Version	V4.0	08.04.2022		Carolina Doran (ECSA), Federico Caruso (OBCT), Johann Cas (ÖAW) und Alessandro Ortalda (VUB)

Haftungsausschluss: Der Inhalt dieser Veröffentlichung liegt in der alleinigen Verantwortung des PANELFIT-Konsortiums und gibt nicht unbedingt die Meinung der Europäischen Union wieder.

Inhaltsübersicht

IKT, Daten und schutzbedürftige Personen: ein Leitfaden für Bürger 4
Über diesen Leitfaden 5
Glossar der wichtigsten Begriffe 5
Was sind die ethischen und rechtlichen Fragen im Zusammenhang mit IKT? 8
Wer ist schutzbedürftig? 10
Wie wirken sich ethische und rechtliche Fragen im Zusammenhang mit der IKT auf schutzbedürftige Menschen aus? 14
Was können Sie tun? 27
Danksagung 35
Thematische Dossiers 37
1. Vermarktung von Daten: Telefonanbieter und personenbezogene Daten 37
2. Die EU Cybersicherheitsstrategie 48
3. Ungleichgewicht der Macht und Freiheit des Konsenses: Europas digitale Festung 64

IKT, Daten und schutzbedürftige Personen: ein Leitfaden für Bürger

Haftungsausschluss

Dieses Projekt wurde aus Mitteln des Programms für Forschung und Innovation Horizont 2020 der Europäischen Union unter der Finanzhilfevereinbarung Nr. 788039 finanziert. Die Verantwortung für den Inhalt dieses Dokuments trägt allein der Verfasser; die Agentur haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Quellenangabe

PANELFIT-Konsortium (2021) *IKT, Daten und schutzbedürftige Personen: ein Leitfaden für Bürger*. UPV-EHU, Bilbao.

Über diesen Leitfaden

IKT, personenbezogene Daten, digitale Rechte, DSGVO, Datenschutz, Online-Sicherheit – diese Begriffe und die dahinterstehenden Konzepte sind in unserem Leben immer häufiger zu finden. Einige von uns sind vielleicht mit ihnen vertraut, aber andere sind sich der wachsenden Rolle der IKT und der Daten in unserem Leben – sowie der damit verbundenen potenziellen Risiken – weniger bewusst.

In diesem Leitfaden wird der Begriff „Bürger“ für alle Personen verwendet, die unabhängig von ihrer Staatsangehörigkeit in Europa ansässig sind, oder deren Rechte, wenn auch nur vorübergehend, der europäischen Rechtsprechung unterliegen.

Diese Risiken sind für schutzbedürftige Gruppen in der Gesellschaft noch ausgeprägter. Menschen können auf unterschiedliche, sich oft überschneidende Weise schutzbedürftig sein, wodurch sie gegenüber der Mehrheit der Bürger benachteiligt sind (Tabelle 3 zeigt einige der vielen Formen und Ursachen von Schutzbedürftigkeit). Daher benötigen schutzbedürftige Menschen mehr Unterstützung, um sich in der digitalen Welt zurechtzufinden und ihre Rechte wahrnehmen zu können. In diesem Leitfaden wird erläutert, wo diese Unterstützung zu finden ist, und es werden die folgenden Fragen beantwortet:

- Was sind die wichtigsten ethischen und rechtlichen Fragen im Zusammenhang mit IKT für schutzbedürftige Bürger?
- Wer ist in Europa schutzbedürftig?
- Wie wirken sich Fragen im Zusammenhang mit IKT auf besonders schutzbedürftige Menschen aus?

Dieser Leitfaden ist ein Hilfsmittel für Angehörige schutzbedürftiger Gruppen, für Menschen, die mit schutzbedürftigen Gruppen arbeiten und für Bürger im weiteren Sinne. Er ist auch nützlich für „Verantwortliche“[5], die Daten über schutzbedürftige Bürger sammeln. Obwohl sich dieser Leitfaden auf Bürger in Europa konzentriert, kann er auch für Menschen in anderen Teilen der Welt von Interesse sein.

Er ist Teil des Informationspakets für Bürgerinnen und Bürger, das im Rahmen des PANELFIT-Projekts erstellt wurde, und in Deutsch, Englisch, Französisch, Italienisch und Spanisch erhältlich. Sie sind herzlich eingeladen, diesen Leitfaden in andere Sprachen zu übersetzen. Bitte senden Sie uns einen Link zu Online-Versionen in anderen Sprachen, damit wir sie auf die Projektwebsite stellen können.

Glossar der wichtigsten Begriffe

In Tabelle 1 werden einige der in diesem Leitfaden verwendeten Schlüsselbegriffe erläutert. Die Definitionen sind nicht das „letzte Wort“ zu diesen Begriffen, sondern bieten eine nützliche Information für diejenigen, die mit der Terminologie rund um IKT, Daten und schutzbedürftige Gruppen nicht vertraut sind.

Tabelle 1. Schlüsselbegriffe zum Verständnis von IKT, Daten und schutzbedürftigen Gruppen

Cybersicherheit	Dies bezieht sich darauf, wie gut private Online-Daten und Informationen geschützt sind, z. B. wie sicher sie davor sind, gehackt, gestohlen oder unerlaubt veröffentlicht zu werden.
Vermarktung von Daten	Dies bedeutet, dass Daten über Einzelpersonen oder Gruppen verarbeitet werden, um Geld zu verdienen, z. B. durch gezielte Online-Werbung oder durch den Verkauf der Daten an andere.
Verantwortlicher	Ein Verantwortlicher ist jeder, der Daten, einschließlich personenbezogener Daten, erhält, um sie für einen bestimmten Zweck zu verwenden. Dies kann unter anderem ein Unternehmen, eine Organisation, eine Regierung oder eine lokale Behörde, eine öffentliche Einrichtung (z. B. eine Schule oder ein Krankenhaus) oder ein Forschungsinstitut sein.
Datenverwaltung	Die Datenverwaltung umfasst den gesamten Lebenszyklus der Datenverarbeitung: Erhebung, Verwendung, Speicherung, Weitergabe und Löschung. Es bezieht sich auch auf die Tatsache, dass derjenige, der Ihre Daten sammelt (der Verantwortliche), kontrollieren muss, wozu die Daten verwendet werden und wer sie verwenden darf.
Datenschutz	Mit Ihren personenbezogenen Daten sollte nichts geschehen, es sei denn, Sie haben Ihre Einwilligung dazu gegeben. Die Verantwortlichen sind nach EU-Recht verpflichtet, Maßnahmen zu ergreifen, um eine sichere und vertrauliche Speicherung der Daten zu gewährleisten. Ihre Daten sollten nicht weitergegeben oder öffentlich zugänglich gemacht werden, es sei denn, Sie haben dem zugestimmt.
Betroffene Person	Die Person, deren personenbezogene Daten von dem Verantwortlichen erhoben und verwendet werden.
Verwendung und Weiterverwendung von Daten	Bei der Bitte um Daten sollten die Verantwortlichen erklären, für welche Zwecke die Daten verwendet werden sollen (z. B. für eine Volkszählung oder ein Forschungsprojekt). Wenn sie oder ein Dritter Sie betreffende Daten für einen weiteren Zweck verwenden wollen, die sogenannte Weiterverwendung von Daten, sollten sie Sie erneut um Ihre Einwilligung bitten. Sie können nicht davon ausgehen, dass Sie mit der Weiterverwendung Ihrer Daten einverstanden sind.

Digitale Kluft	Dies beschreibt die Kluft zwischen Menschen, die in der Lage sind, von der Technologie (z. B. IKT, Internet) zu profitieren, und jenen, die dies nicht können. Dieses Phänomen gewinnt zunehmend an Bedeutung, da immer mehr Aspekte unseres Lebens teilweise oder vollständig online ablaufen (z. B. Bildung, Gesundheitswesen, Bankgeschäfte, Einkaufen). Diejenigen, die nur begrenzten oder gar keinen Zugang zu digitalen Diensten haben, laufen Gefahr, „den Anschluss zu verlieren“.
Digitale Kompetenz	Manchmal auch als „IKT-Kompetenz“ bezeichnet. Dieser Begriff bezieht sich auf die Fähigkeit einer Person, Informationen auf digitalen Plattformen und Geräten zu finden, zu bewerten und zu kommunizieren.
Digitale Rechte	Dies bezieht sich auf die Gesetze und Verfahren (z. B. die DSGVO), die zum Schutz der Rechte von Personen in der digitalen Welt gelten. Zu diesen Rechten gehören u. a. das Recht auf Privatsphäre und das Recht, die Einwilligung zur Datennutzung zu widerrufen.
Diskriminierung	Diskriminierung bedeutet, ungerechtfertigte Unterscheidungen zwischen Menschen zu treffen, die auf Wahrnehmungen über die Gruppe oder Kategorie dieser Menschen beruhen, z. B. ihre ethnische Zugehörigkeit, ihr Geschlecht, ihr Alter, ihre Religion oder ihre sexuelle Ausrichtung.
DSGVO	Die Datenschutz-Grundverordnung regelt den Umgang mit den personenbezogenen Daten der europäischen Bürger. Sie legt also die Gesetze fest, durch die Sie betreffende personenbezogene Daten geschützt und geheim gehalten werden.
IKT	Zu den Informations- und Kommunikationstechnologien gehören alle Formen von Technologien, die für die Kommunikation genutzt werden, z. B. das Internet, Mobiltelefone und Smartphones, Computer, soziale Netzwerke, Videokonferenzsysteme und viele andere.
Einwilligung in Kenntnis der Sachlage	In Bezug auf Daten und IKT bedeutet dies, dass die betroffene Person informiert und um Erlaubnis gebeten werden muss, sie betreffende personenbezogene Daten in einer bestimmten Weise zu verwenden – und zwar vor der Erhebung oder Verwendung der Daten.
Personenbezogene Daten	Personenbezogene Daten sind alle Daten, die sich auf Sie als Einzelperson beziehen: Ihr Name, Ihr Alter oder Ihre Adresse zum Beispiel. In der digitalen Welt können dies auch Ihre Interessen, Gewohnheiten und Vorlieben sein, z. B. Seiten, die Sie in den sozialen Medien „liken“, Websites, die Sie besuchen, um Artikel zu kaufen, YouTube-Videos, die Sie sich angesehen haben, und viele andere.
Schutz der Privatsphäre	Im Zusammenhang mit IKT und Daten bezieht sich der Schutz der Privatsphäre darauf, wie vertraulich Ihre Informationen sind (Datenschutz) und wie weit sie weitergeben werden dürfen (z. B. öffentlich oder nur durch den Verantwortlichen).

Stigmatisierung	Stigmatisierung oder soziale Stigmatisierung bedeutet die Ablehnung oder Diskriminierung einer Person oder einer Gruppe von Menschen aufgrund von Wahrnehmungen über die Person oder die Gruppe(n), zu der sie gehören.
Schutzbedürftige Personen	Schutzbedürftige Personen sind diejenigen, die aus verschiedenen Gründen einem höheren Risiko ausgesetzt sind als die Mehrheit der Gesellschaft. Beispiele für schutzbedürftige Gruppen finden Sie weiter unten in diesem Leitfaden (Tabelle 3). Menschen, die bestimmten sozialen Gruppen angehören, werden manchmal als „benachteiligt“ oder „sozial ausgegrenzt“ bezeichnet.

Was sind die ethischen und rechtlichen Fragen im Zusammenhang mit IKT?

Die IKT hat unser Leben in vielerlei Hinsicht bereichert. Sie hat es möglich gemacht, schnell und kostengünstig mit Menschen auf der ganzen Welt zu kommunizieren; sie hat uns sofortigen Zugang zu mehr Informationen verschafft, als wir dachten, überhaupt benötigen zu würden; sie hat enorme Fortschritte im Gesundheitswesen gebracht; sie hat uns geholfen, die Armut zu bekämpfen und immer mehr Menschen weltweit Bildung zukommen zu lassen.

Doch diese Fortschritte sind nicht ohne Kosten geblieben. Viele IKT benötigen Daten, um zu funktionieren, und infolgedessen fragen Unternehmen, Organisationen, Forscher und Behörden zunehmend nach unseren Daten – oder nehmen sie sich einfach. Daten und Informationen sind mächtig, und diejenigen, die sie kontrollieren, sind zunehmend in der Lage, über jeden Aspekt unseres Lebens, sowohl beruflich als auch privat, etwas herauszufinden – und von diesen Informationen zu profitieren, sei es in finanzieller, politischer oder sonstiger Hinsicht.

Für viele Menschen sind die Debatten über diese ethischen und rechtlichen Fragen schwer zu verstehen oder werden als langweilig oder irrelevant für ihr tägliches Leben abgetan. Außerdem entwickeln sich die ethischen Debatten über IKT sehr schnell weiter, sodass es für die Menschen schwierig sein kann, mit ihnen Schritt zu halten. Infolgedessen sind wir oft schnell bereit, unsere Rechte aufzugeben, um die vielen Vorteile der IKT zu nutzen.

Da sich die IKT jedoch immer weiter in alle Bereiche unseres Lebens ausbreitet, werden diese Fragen durch die wachsende Nachfrage nach unseren personenbezogenen Daten immer wichtiger. Wer hat Zugriff auf unsere Daten? Mit wem werden sie noch geteilt? Was wird mit ihnen gemacht – und was kann ich tun, um das zu kontrollieren?

Die IKT ist ein sich rasch entwickelnder Bereich, und somit ändern sich auch die ethischen und rechtlichen Fragen im Zusammenhang mit ihr ständig. Tabelle 2 zeigt einige der wichtigsten aktuellen ethischen und rechtlichen Fragen der Bürger im Zusammenhang mit IKT.

Tabelle 2. Ethische und rechtliche Fragen im Zusammenhang mit IKT

Viele Bürger haben nur ein begrenztes Verständnis für und/oder Interesse an Fragen im Zusammenhang mit IKT	Fragen im Zusammenhang mit IKT sind für Nichtfachleute oft schwer zu verstehen. Dies gilt sowohl für rechtliche Fragen (z. B. die Details von Online-Geschäftsbedingungen) als auch für ethische Fragen wie die Überwachung und die künftige Rolle der künstlichen Intelligenz. Für viele ist dies mit einem mangelnden Interesse an komplexen Themen oder Dokumenten voller juristischer Terminologie wie der Datenschutz-Grundverordnung verbunden. In anderen Fällen möchten die Bürgerinnen und Bürger vielleicht mehr wissen, wissen aber nicht, wo sie Hilfe für das Verständnis dieser Themen finden können. Dies hat Folgewirkungen, beispielsweise, dass Menschen auf „Ich stimme zu“ klicken, ohne die Allgemeinen Geschäftsbedingungen oder die Datenschutzrichtlinie einer Website gelesen oder verstanden zu haben. Außerdem wissen die Menschen möglicherweise nicht, welche Gesetze zum Schutz ihrer Rechte in der digitalen Welt gelten – was es ihnen erschwert, diese Rechte wahrzunehmen.
Es gibt eine Reihe von Hindernissen, die das Verständnis der Bürger einschränken	Für viele Menschen gibt es große Hindernisse, die ihnen den Zugang zu weiteren Informationen über IKT und digitale Rechte verwehren. Eine davon ist die Sprache: Viele dieser Informationen sind auf Englisch oder auch in anderen wichtigen europäischen Sprachen verfügbar, aber nicht jeder in Europa spricht diese Sprachen fließend. Außerdem stehen viele dieser Informationen nur online zur Verfügung. Für Offline-Gemeinschaften – diejenigen mit begrenztem oder gar keinem Internetzugang – bleiben sie unerreichbar. Dieser fehlende Zugang zu Informationen über die IKT ist ein Beispiel für die „digitale Kluft“.
Es besteht ein empfundenes Machtungleichgewicht zwischen Bürgern und Technologieunternehmen	„Tech-Giganten“ – große globale Technologieunternehmen wie Facebook und Google – können sehr mächtig erscheinen. Für manche Menschen kann dies auch für kleinere Technologieunternehmen gelten. Daher kann es schwierig sein, auf „Nein“ oder „Ich stimme nicht zu“ zu klicken, wenn diese Unternehmen unsere Daten verlangen. Die Menschen glauben, dass sie ihre Dienste nicht mehr nutzen können, oder befürchten, dass diese Unternehmen ohnehin Zugang zu ihren Daten haben. Dieses Gefühl der Ohnmacht wird noch verstärkt, wenn Menschen die Informationen über ihre digitalen

	Rechte nicht lesen können oder wollen.
Die Diversität der Bürgerinnen und Bürger bedeutet, dass die Menschen unterschiedliche Anliegen in Bezug auf die IKT haben	Verschiedene Gruppen in der Gesellschaft nutzen IKT auf sehr unterschiedliche Weise – und haben daher unterschiedliche Anliegen, Probleme und Herausforderungen bei der Nutzung von IKT. Es ist schwierig, jeder Gruppe oder jedem Einzelnen die benötigten Informationen zur Verfügung zu stellen, und zwar in dem Format und in der Sprache, die sie wünschen. Infolgedessen sind viele Informationen über IKT und digitale Rechte allgemein gehalten, was es den Menschen erschwert, genau das zu finden, was sie brauchen.
Die IKT-Landschaft verändert sich ständig	IKT und digitale Rechte sind komplex. Zu dieser Komplexität kommt noch hinzu, dass sich die Technologie ständig weiterentwickelt und unsere Daten auf immer neue und immer kompliziertere Weise genutzt werden. Dies bringt eigene Herausforderungen mit sich, nicht zuletzt infolge der Tatsache, dass es immer neue Gesetze, Verfahren und Entwicklungen gibt, die wir versuchen müssen zu verstehen. Diese Komplexität wird durch die unterschiedlichen Auslegungen dieser Rechte und die Schutzmaßnahmen noch verstärkt, die in den verschiedenen Ländern zu deren Gewährleistung eingeführt wurden (z. B. die Datenschutz-Grundverordnung).

Quelle: Angepasst an den Bericht des COST Action/PANELFIT-Workshops vom März 2020; ergänzt durch die am Ende dieses Leitfadens aufgeführten weiteren Ressourcen.

Wer ist schutzbedürftig?

Die ethischen und rechtlichen Herausforderungen im Zusammenhang mit der IKT betreffen jeden – in Europa und darüber hinaus. Für schutzbedürftige Gruppen in der Gesellschaft sind diese Risiken jedoch oft noch akuter – und in vielen Fällen ist ihre Fähigkeit, sich an diese Risiken anzupassen, geringer. Darüber hinaus besteht die Möglichkeit, dass einige schutzbedürftige Menschen die Chancen und Vorteile der IKT nicht nutzen können, wenn sie sich ihrer nicht bewusst sind oder wenn ihre Angst vor diesen Risiken größer ist als ihr Wunsch nach den Vorteilen.

Aber wer gilt als schutzbedürftig? Diese Frage ist nicht einfach zu beantworten, da die Schutzbedürftigkeit aus zahlreichen Gründen komplex ist. Kasten 1 gibt einen Überblick über diese Komplexität. Die Faktoren, die zu dieser Komplexität beitragen, werden anschließend ausführlicher erläutert.

Kasten 1. Wie man Schutzbedürftigkeit „entschlüsselt“

Die hier dargelegten Punkte decken nicht alle Elemente der Schutzbedürftigkeit ab, sondern machen deutlich, dass es sich um ein kompliziertes und vielseitiges Konzept handelt. Die allgemeine Botschaft ist, dass Schutzbedürftigkeit ein fließendes, dynamisches Konzept ist und dass die meisten Menschen nicht in saubere, binäre Kategorien von Schutzbedürftigkeit passen.

Stattdessen schlagen wir vor, Schutzbedürftigkeit als ein Spektrum zu betrachten: Einzelpersonen oder Gruppen können ein hohes oder geringes Maß an Schutzbedürftigkeit aufweisen, die fest (statisch) oder sich verändernd (dynamisch) sein kann. Die Schutzbedürftigkeit ändert sich wahrscheinlich im Laufe des Lebens einer Person: mit dem Alter, durch sich verändernde persönliche Umstände und durch Faktoren, die sich ihrer Kontrolle entziehen.

Es sei auch darauf hingewiesen, dass *jeder Mensch* potenziell schutzbedürftig ist und dass der Grad seiner Widerstandsfähigkeit – seine Fähigkeit, mit der Schutzbedürftigkeit umzugehen – von seinem Zugang zu Ressourcen (z. B. den in einem Land verfügbaren öffentlichen Diensten) und kulturellen Faktoren (z. B. seinen Supportnetzwerken) abhängt.

Vor allem ist es wichtig, sich zu vergegenwärtigen, dass alle in diesem Leitfaden genannten Gruppen und Einzelpersonen in erster Linie *Menschen* sind und dass jede andere Definition – als betroffene Person, als schutzbedürftige Person, sogar als Bürger – dem untergeordnet ist.

Die Ursachen für die Schutzbedürftigkeit sind sehr unterschiedlich

Menschen können in vielerlei Hinsicht schutzbedürftig sein. So kann die Schutzbedürftigkeit beispielsweise durch finanzielle Probleme (darunter Arbeitslosigkeit, unüberwindbare Schulden) oder gesundheitliche und kapazitätsbezogene Hindernisse wie Krankheit, Alter oder Behinderung verursacht werden. Andere Ursachen für die Schutzbedürftigkeit können ortsbezogen sein, wie z. B. das Leben in abgelegenen ländlichen Gebieten mit wenigen Einrichtungen (z. B. Krankenhäuser, Schulen). Die Ursachen für die Schutzbedürftigkeit können gesellschaftlicher Natur sein, beispielsweise Vorurteile gegenüber Flüchtlingen, Ausländern oder Sinti. Sie können auch auf Diskriminierung aufgrund von ethnischer Zugehörigkeit, Nationalität, Klasse, Kaste, Religion, Weltanschauung, Geschlecht, Sprache, sexueller Ausrichtung, Geschlechtsidentität und Geschlechtsmerkmalen zurückzuführen sein, um nur einige zu nennen.

Menschen oder Gruppen können mehr als eine Form der Schutzbedürftigkeit erfahren

Die Form, in der die Schutzbedürftigkeit einer Person auftritt, kann kompliziert sein. Auf individueller Ebene kann eine Person von schlechter Gesundheit und geringer finanzieller Leistungsfähigkeit betroffen sein. Diese Arten der Schutzbedürftigkeit haben unterschiedliche Auswirkungen, sind aber oft miteinander verbunden; eine Ursache für die Schutzbedürftigkeit kann oft andere verschlimmern und einen „Teufelskreis“ schaffen. In Anlehnung an das genannte Beispiel kann Geldmangel zu gesundheitlichen Problemen führen (z. B. aufgrund einer eingeschränkten Ernährung oder unhygienischer Lebensbedingungen) und die daraus resultierende schlechte Gesundheit kann die Arbeitssuche erschweren – was wiederum die finanziellen Probleme der Person erhöht oder aufrechterhält.

Die Schutzbedürftigkeit kann innerhalb einer Gruppe in der Gesellschaft variieren

Einzelne Personen innerhalb einer schutzbedürftigen Gruppe können im Rahmen einer gemeinsame Situation unterschiedliche Auswirkungen und unterschiedlich hohe Folgen erfahren. Einige Flüchtlinge in Europa können beispielweise aufgrund einer Reihe von Faktoren schutzbedürftiger sein als andere: das Land, aus dem sie kommen (der Grund ihrer Flucht und ob dies ein Trauma oder psychologische Probleme verursacht hat); das Land, in dem sie derzeit leben (darunter seine Einrichtungen für Flüchtlinge, die Einstellung der Öffentlichkeit gegenüber Flüchtlingen); und ihre Bildung, Ausbildung und Kompetenzen (Sprachkenntnisse, berufliche Qualifikationen). All diese Faktoren beeinflussen ihre Fähigkeit, sich niederzulassen, Arbeit zu finden und die ihnen zur Verfügung stehenden Einrichtungen zu nutzen. Auch wenn die Aussage „Flüchtlinge sind schutzbedürftig“ zutrifft, so ist die Schwere der Schutzbedürftigkeit und die Erfahrung, die die Menschen damit machen, innerhalb dieser großen Gruppe sehr unterschiedlich. Wenn eine bestimmte Art von Schutzbedürftigkeit mit einem allgemeinen Begriff beschrieben wird, können die spezifischen Herausforderungen einzelner Personen übersehen werden, was es schwieriger macht, sie anzugehen.

Schutzbedürftigkeit kann dynamisch sein

Während sich einige Arten der Schutzbedürftigkeit im Laufe des Lebens nicht wesentlich ändern (darunter unheilbare Behinderungen), können sich andere im Laufe der Zeit verschlechtern oder verbessern. So ändern sich beispielsweise bei vielen Menschen die persönlichen Umstände, z. B. in Bezug auf ihre finanzielle Situation oder ihren Gesundheitszustand. Auch externe Faktoren, die sich auf die Schutzbedürftigkeit auswirken, können sich ändern; dies könnte das politische Klima in ihrem Land sein, das dazu führt, dass Randgruppen weniger unterstützt werden. In anderen Fällen kann die Ursache einer Schutzbedürftigkeit im Laufe der Zeit entfallen, z. B. wenn sich ein Gesundheitsproblem verbessert oder wenn Arbeitssuchende eine Arbeit finden, wodurch ihre finanzielle Schutzbedürftigkeit aufgehoben oder verringert wird.

Einige dieser Veränderungen sind vorhersehbar, darunter die zunehmende Schutzbedürftigkeit mit zunehmendem Alter. In einigen Fällen kann die Ursache der Schutzbedürftigkeit jedoch schnell und unerwartet eintreten: Menschen können von Phänomenen betroffen sein, die sich ihrer Kontrolle entziehen, wie etwa extreme Klimaereignisse. Diese „Katastrophen“ können eine Schutzbedürftigkeit hervorrufen, auf die die Menschen nicht vorbereitet sind.

Schutzbedürftigkeit kann angenommen werden

Bei der Betrachtung der Schutzbedürftigkeit innerhalb einer Gesellschaft ist man oft versucht, bestimmte Merkmale für bestimmte Gruppen anzunehmen – die aber nicht unbedingt auf alle Mitglieder dieser Gruppe zutreffen. Zum Beispiel können Flüchtlinge gut ausgebildet sein und die Sprache ihres Gastlandes beherrschen. Dennoch teilen sie wahrscheinlich andere schutzbedürftige Eigenschaften mit anderen Flüchtlingen, wie z. B. einen eingeschränkteren Zugang zu Ressourcen und Beschäftigungsmöglichkeiten (im Vergleich zu Nicht-Flüchtlingen) oder Missbrauch, Vernachlässigung, Ausbeutung, Vorurteile und Anfeindungen durch andere Mitglieder der Gesellschaft.

Bestimmte Gruppen, die oft als schutzbedürftig angesehen werden, müssen sorgfältig definiert und manchmal sogar in Unterkategorien eingeteilt werden. So werden beispielsweise Kinder und Jugendliche (im Alter von 16 bis 25 Jahren) häufig als schutzbedürftig eingestuft, aber die Art der Schutzbedürftigkeit kann abhängig von den folgenden Faktoren sehr unterschiedlich sein:

- Schüler, die rechtlich nicht in der Lage sind, alle Entscheidungen für sich selbst zu treffen
- Studenten an einer Hochschule, was zu Stress oder anderen psychischen Problemen führen kann
- Jugendliche in einem Beschäftigungsverhältnis, das in dieser Altersgruppe häufig schlecht bezahlt oder unsicher ist
- Ohne Bildung und Beschäftigung, was zu einer Reihe von Schwachstellen führen kann (z. B. finanzielle Probleme, Lebensbedingungen, psychische Probleme).

Schutzbedürftigkeit kann auch subjektiv und unsichtbar sein. Eine Person kann sich schutzbedürftig fühlen oder sich selbst als schutzbedürftig einstufen, während eine andere Person in einer ähnlichen (oder vielleicht sogar schlimmeren) Situation dies nicht tut. Gleichzeitig kann sich jeder Bürger aus Gründen, die für andere nicht unmittelbar ersichtlich sind, als schutzbedürftig betrachten.

Schutzbedürftigkeit kann die Person betreffen – aber auch ihre Kultur

In manchen Fällen sind nicht (nur) die Einzelnen innerhalb einer Gruppe schutzbedürftig. Bestimmte Gruppen können feststellen, dass ihr kulturelles Erbe bedroht ist oder dass ihr Zugang dazu schutzbedürftig ist. Dies kann auf externe Bedrohungen wie den Klimawandel zurückzuführen sein: In den Polarregionen ist die gesamte Lebensweise der indigenen Völker bedroht. Auch die kulturellen Ressourcen der Menschen können schutzbedürftig sein, z. B. ihre Sprache, ihre familiären und sozialen Strukturen und Netzwerke sowie ihr Naturerbe und ihre Umwelt.

Schutzbedürftige Gruppen in Europa

Ohne diese Komplexität zu vernachlässigen, ist es oft notwendig, schutzbedürftige Gruppen und Einzelpersonen zu identifizieren. Wer kann oder sollte also in Europa als „schutzbedürftig“ angesehen

werden? Es gibt zwar keine einheitliche Definition des Begriffs „schutzbedürftig“, aber eine hilfreiche Definition zur Absteckung des Rahmens ist die von der EU[6] für Migranten verwendete:

> *„Minderjährige, unbegleitete Minderjährige, Menschen mit Behinderungen, ältere Menschen, Schwangere, Alleinerziehende mit minderjährigen Kindern, Opfer des Menschenhandels, Personen mit schweren Krankheiten, Personen mit psychischen Störungen und Personen, die Folter, Vergewaltigung oder sonstige schwere Formen psychischer, physischer oder sexueller Gewalt erlitten haben, wie z. B. Opfer weiblicher Genitalverstümmelung.“*

Ausgehend von dieser Definition werden in Tabelle 3 mehrere schutzbedürftige Gruppen in Europa[7] sowie Personen aufgeführt, die von bestimmten Arten der Schutzbedürftigkeit betroffen sind.[8] Diese Tabelle sollte nicht als vollständige Liste schutzbedürftiger Gruppen in Europa angesehen werden; angesichts der sich verändernden Natur der Schutzbedürftigkeit wäre dies unmöglich. Sie bietet jedoch einen nützlichen Ausgangspunkt für die Überlegung, wer schutzbedürftig ist.

Tabelle 3 enthält auch ein Beispiel dafür, wie sich die Schutzbedürftigkeit in Bezug auf IKT auswirken kann (siehe den nächsten Abschnitt für weitere Erörterungen zu diesem Thema). Die angeführten Beispiele sollen mögliche Arten von IKT-bezogener Schutzbedürftigkeit für jede Gruppe veranschaulichen; wahrscheinlich gibt es noch viele weitere Arten je nach dem Grad der Schutzbedürftigkeit und den Umständen.

Wir haben diese Gruppen nicht unter breiteren Überschriften oder Themen zusammengefasst. Dies würde einer unserer Hauptempfehlungen widersprechen: Schutzbedürftigkeit sollte als dynamisch und komplex angesehen werden und nicht als „Etikett“, das auf bestimmte Gruppen oder Einzelpersonen anzuwenden ist. Große Gruppen in der Gesellschaft als schutzbedürftig abzustempeln, kann die Diskriminierung und Stigmatisierung, der sie ausgesetzt sind, sogar noch verstärken.

Wie wirken sich ethische und rechtliche Fragen im Zusammenhang mit der IKT auf schutzbedürftige Menschen aus?

Die ethischen und rechtlichen Fragen im Zusammenhang mit der IKT – z. B. im Zusammenhang mit dem Datenschutz, der Datenvermarktung und dem zunehmenden Einsatz neuer Technologien wie der Gesichtserkennung – betreffen jeden in der Gesellschaft. Doch wie bereits erwähnt, sind

schutzbedürftige Menschen und Gruppen in der Gesellschaft oft einem größeren Risiko ausgesetzt als andere – und zwar auf unterschiedliche Weise. Einige davon werden in Kasten 2 vorgestellt.

Kasten 2. Wie wirkt sich die IKT insbesondere auf schutzbedürftige Menschen aus?

Diese Menschen und Gruppen sind nicht nur aufgrund ihrer Umstände schutzbedürftig, sondern insofern stärker schutzbedürftig, als ihre Daten in einer Weise verwendet werden, die sie einem Risiko aussetzt (z. B. durch verstärkte Überwachung). Dies ist zwar ein Risiko für alle Bürger, doch sind schutzbedürftige Personen oft einem höheren Risiko ausgesetzt. So können sie beispielsweise nicht in der Lage sein, ihre Einwilligung zu erteilen, oder sie sprechen die Sprache(n) des Landes, in dem sie leben, nicht fließend.

Machtungleichgewichte zwischen betroffenen Personen und Verantwortlichen können sich bei schutzbedürftigen Personen noch verschärfen. In Fällen, in denen personenbezogene Daten von den Verantwortlichen missbraucht werden können, sind schutzbedürftige Personen möglicherweise weniger in der Lage, dies zu kontrollieren oder zu verhindern, weil sie weniger Macht, Wissen oder Bewusstsein für das Problem haben.

- Es besteht die Gefahr einer (stärkeren) Stigmatisierung, da die Menschen zum Zwecke der Forschung und Analyse in Gruppen eingeteilt werden.

Diese Risiken hängen nicht nur mit der Art der Schutzbedürftigkeit einer Person zusammen, sondern auch mit der Art der Daten, die über sie gesammelt und verwendet werden. Bestimmte Arten von Daten – wie Informationen über die Religion, die Krankengeschichte oder die sexuelle Ausrichtung einer Person – können je nach Ort und Kontext, in dem sie verwendet werden, ein größeres Risiko darstellen.

Darüber hinaus kann sich, wie bereits erwähnt, die Schutzbedürftigkeit im Laufe der Zeit ändern – und das wirft Fragen in Bezug auf die personenbezogenen Daten auf. Einzelpersonen oder Gruppen, die zum Zeitpunkt der Weitergabe ihrer Daten nicht schutzbedürftig sind, können dies später werden. Infolgedessen gelten die Bedingungen, unter denen sie ihre Einwilligung zur Verwendung ihrer Daten gegeben haben, möglicherweise nicht mehr. Forschungsteams, die über zu wenig Ressourcen verfügen, haben möglicherweise nicht die Zeit, das Geld und in manchen Fällen auch nicht die Informationen, die sie benötigen, um Maßnahmen zur Sicherstellung zu ergreifen, dass die Daten und die Rechte der betroffenen Personen geschützt werden.

Wie oben lautet die Botschaft: Schutzbedürftigkeit ist komplex! Tabelle 3 zeigt einige der Möglichkeiten auf, wie schutzbedürftige Gruppen in der Gesellschaft in Bezug auf die ethischen und

rechtlichen Fragen im Zusammenhang mit IKT und Daten besonders betroffen sein können. Wir sagen nicht, dass dies auf alle Mitglieder dieser Gruppen zutrifft; es sind lediglich Beispiele, die verdeutlichen sollen, auf welche Weise Schutzbedürftigkeit insbesondere im Zusammenhang mit IKT und Daten auftreten kann.

Tabelle 3. Beispiele für schutzbedürftige Gruppen in Europa und die Art ihrer Schutzbedürftigkeit

Schutzbedürftige Gruppe	**Mögliche Schutzbedürftigkeit**	**Mögliche Schutzbedürftigkeit in Bezug auf IKT und Daten**
Frauen	Schwangere oder stillende Frauen sind möglicherweise schutzbedürftiger als andere Frauen oder fühlen sich schutzbedürftig, z. B. aufgrund gesundheitlicher Veränderungen. Frauen im fruchtbaren Alter sind einem höheren Risiko der Diskriminierung bei Einstellungsverfahren ausgesetzt.	In Bezug auf Frauen, die sich einer geschlechtsangleichenden Operation unterzogen haben, können Daten gespeichert sein, die nicht mehr ihrem Status entsprechen.
Alleinerziehende Eltern oder Erziehungsberechtigte / Eltern oder Erziehungsberechtigte von schutzbedürftigen Kindern oder abhängigen Personen	Zusätzliche Betreuungsaufgaben können dazu führen, dass diese Personen weniger Zeit und Ressourcen haben, um sich selbst zu versorgen, was ihre Schutzbedürftigkeit erhöht.	Sie haben möglicherweise weniger Zeit, sich über IKT-bezogene Themen zu informieren und diese zu verstehen.
Obdachlose Menschen	Menschen, die sich in dieser Situation befinden, sind häufig größeren gesundheitlichen Risiken ausgesetzt und unterliegen einem erhöhten Risiko für Gewalt, Arbeitslosigkeit und Armut.	Sie haben wahrscheinlich weniger Zugang zu Informationen über diese Themen als andere in der Gesellschaft. Außerdem können Daten über sie ohne ihre Einwilligung in Kenntnis der Sachlage erhoben werden (z. B. wenn sie Obdachlosendienste von Wohlfahrtsverbänden in Anspruch nehmen).

Menschen mit einer oder mehreren Abhängigkeiten, wie Drogenabhängigkeit und/oder Alkoholismus	Menschen, die mit Suchtproblemen leben, sind in vielerlei Hinsicht schutzbedürftig, z. B. durch gesundheitliche Risiken, ein erhöhtes Gewaltrisiko, Arbeitslosigkeit und Armut.	Sie sind möglicherweise nicht in der Lage, Informationen über ihre IKT- und Datenrechte zu verstehen.
Menschen, die unter häuslicher Gewalt, psychischem und/oder sexuellem Missbrauch leiden oder davon bedroht sind	Menschen, die mit Gewalt und Missbrauch konfrontiert sind, sind wahrscheinlich in mehrfacher Hinsicht schutzbedürftig, z. B. durch körperliche und psychische Probleme.	In manchen Situationen kann der Zugang der Opfer zu Informationen als Teil des erlittenen Missbrauchs eingeschränkt sein, beispielsweise, wenn sie mit einem Partner zusammenleben, der ihre Möglichkeiten einschränkt, was sie tun oder wohin sie gehen können.
Menschen, die Folter, Vergewaltigung oder andere schwere Formen psychischer, physischer oder sexueller Gewalt erlitten haben, wie z. B. Opfer von Genital-verstümmelung bei Frauen	Neben vielen anderen Formen der Schutzbedürftigkeit sind Menschen, die diese Erfahrungen gemacht haben, wahrscheinlich zusätzlich zu den Auswirkungen auf ihre körperliche Gesundheit von einem langfristigen Trauma oder anderen psychologischen Folgen betroffen.	Die mangelnde Bereitschaft, personenbezogene Daten mitzuteilen – z. B. wenn sie Migranten sind oder keinen legalen Status in einem Land haben – kann dazu führen, dass die Opfer weniger bereit sind, medizinische Hilfe in Anspruch zu nehmen oder die Polizei über ihre Situation zu informieren.
Opfer von Menschenhandel	Ein fehlender rechtlicher Status in einem Land kann dazu führen, dass diese Menschen keinen Zugang zu den verfügbaren Supportangeboten haben, z. B. weil sie befürchten, abgeschoben zu werden.	Je nach ihren Bedingungen (z. B. rechtswidrige Gefangenschaft, moderne Sklaverei) haben diese Menschen möglicherweise keinen Zugang zu Online-Diensten oder Informationen. Gleichzeitig können sie, da sie nicht „im System“ sind, von Dienstleistern, die ihnen helfen könnten, übersehen werden.
Religiöse Minderheiten	Es kann schwierig sein, gesellschaftliche Vorurteile gegenüber diesen Gruppen zu beseitigen.	Manche Menschen mögen ihre Religion als Privatsache betrachten, aber bestimmte unvermeidliche Datenerhebungen erfordern dennoch die Angabe ihrer Religion (z. B. die Steuervorschriften in Deutschland).

LGBTQIA+ Menschen[9] und sexuelle Minderheiten	Personen aus dieser Gruppe werden in ganz Europa noch immer häufig diskriminiert.	Neue Technologien, die die Privatsphäre verletzen (z. B. die Erstellung von Gesichtsprofilen), könnten sich eher gegen solche Gruppen richten.
Transgender-Populationen	Personen aus dieser Gruppe werden in ganz Europa noch immer häufig diskriminiert. So hat beispielsweise Ungarn vor Kurzem ein Gesetz verabschiedet, das die rechtliche Anerkennung des Trans-Status abschafft.[10]	Das Ankreuzen von männlich/weiblich, das in vielen Datenerhebungsformularen zu finden ist, diskriminiert sie, genauso wie die „traditionelle“ Sprache in vielen Online-Situationen (z. B. er/sie/es, sein/ihr).
Häftlinge	Häftlinge sind von ihren Supportnetzwerken abgeschnitten und sehen sich oft zusätzlichen Bedrohungen ausgesetzt, wie z. B. einem erhöhten Risiko von Gewalt im Gefängnis.	Ein Gefängnisaufenthalt kann ihren Zugang zu Informationen über ihre Daten und digitalen Rechte einschränken.
Aus der Haft entlassene Personen	Aus der Haft entlassenen Personen fehlt es oft an Supportnetzwerken und sie haben es schwer, eine Beschäftigung zu finden oder eine Wohnung zu sichern.	Ihr schutzbedürftiger Zustand kann den Zugang zu Informationen über ihre Daten und digitalen Rechte einschränken. Je nachdem, wie lange sie im Gefängnis waren, sind sie möglicherweise nicht über die Entwicklungen im Bereich des Datenschutzes und der Privatsphäre informiert.
Menschen mit niedrigem oder schlechtem Bildungsniveau	Ihre Schutzbedürftigkeit wird noch dadurch verstärkt, dass sie die Unterstützungssysteme zur Verringerung ihrer Schutzbedürftigkeit nicht kennen oder nicht verstehen können. Sie verfügen in der Regel über ein geringeres Einkommen, was ihre finanzielle Schutzbedürftigkeit erhöht.	Informationen über IKT und Datenrechte sind in der Regel komplex und schwer zu verstehen; ein niedriger Bildungsstand wird diese Barriere noch vergrößern.
Personen, die sich außerhalb von Ausbildung und/oder Studium befinden	Diese Situation kann viele Arten von Schutzbedürftigkeit verschärfen, unter anderem in finanzieller, gesundheitlicher (insbesondere psychischer)	Informationen über IKT und digitale Rechte werden häufig an formellen Einrichtungen wie Schulen oder Hochschulen vermittelt. Wenn man sich außerhalb dieser Einrichtungen

	Hinsicht und in Bezug auf Supportnetzwerke.	aufhält, haben die Menschen weniger Zugang zu solchen Informationen.
Menschen, die falsch informiert sind, einschließlich solcher, die die bereitgestellten Informationen nicht verstehen können	Information ist Macht. Personen, die keinen Zugang zu hilfreichen Informationen haben oder diese nicht verstehen, sind infolgedessen schutzbedürftiger als diejenigen, die dazu in der Lage sind.	Dies gilt sowohl für digitale Informationen als auch für nicht-digitale Formen von Informationen.
Menschen mit Lernschwierigkeiten wie Legasthenie, Dysorthografie, Dysgrafie und Dyskalkulie	Lernschwierigkeiten können Menschen in mehrfacher Hinsicht schutzbedürftig machen. Zum Beispiel sind Menschen, die hilfreiche Informationen nicht verstehen können, infolgedessen schutzbedürftiger als diejenigen, die dazu in der Lage sind.	Diese und andere Lernschwierigkeiten erschweren es, Informationen über Datenrechte, Datenschutz, IKT usw. zu erfahren und/oder zu verstehen.
Indigene Gruppen	Das Erbe solcher Gruppen, die bedroht sind oder deren Zahl zurückgeht, muss eventuell geschützt werden, zum Beispiel in Museen.	Herkunftsdaten – über die Herkunft, den Besitz und die Aufbewahrung von Objekten – werden nicht immer von den IKT erfasst; in anderen Fällen wird das Wissen indigener Personen möglicherweise ohne ihr Wissen oder ihre Einwilligung gespeichert.
Die Samen[11]	Als Minderheitengruppe, die in einer der rauesten Regionen Europas lebt, sind die Samen in vielerlei Hinsicht schutzbedürftig. Ein Bericht des Sonderberichterstatters der Vereinten Nationen für die Rechte indigener Völker kam zu dem Schluss, dass Schweden, Norwegen und Finnland ihre erklärten Ziele, die Menschenrechte der Samen zu garantieren, nicht erfüllen.[12]	Die Samen waren schon immer Ziel verschiedener Forschungsarbeiten. Dazu gehören Register- und Biobank-basierte Forschung. Bei diesen Projekten wurden manchmal ethische Erwägungen umgangen, indem beispielsweise nicht vollständig kommuniziert wurde, dass ein Projekt auf die Samen abzielt.

Ethnische Minderheiten	Ethnische Minderheiten in einem Land sind häufig mit Diskriminierung konfrontiert und weisen möglicherweise eine höhere Prävalenz verschiedener Arten von Schutzbedürftigkeit auf (z. B. niedriges Einkommen, geringe Bildung, Gesundheitsprobleme, Sprachbarrieren).	Sie haben möglicherweise weniger Zugang zu Informationen über ihre Datenrechte (z. B. wenn diese nicht in ihrer Muttersprache verfügbar sind).
Flüchtlinge	Flüchtlinge werden häufig diskriminiert und sind häufiger von verschiedenen Problemen betroffen (z. B. niedriges Einkommen, geringe Bildung, Gesundheitsprobleme, Sprachbarrieren).	Aus Sorge vor Missbrauch zögern sie möglicherweise, personenbezogene Daten bereitzustellen. Dies kann sie von den potenziellen Vorteilen, die IKT bieten können, ausschließen.
Asylsuchende	Asylsuchende können psychische Probleme haben oder traumatisiert sein, z. B. wenn sie aus einem Kriegsgebiet oder vor einer Katastrophe geflohen sind.	Aus Sorge vor Missbrauch zögern sie möglicherweise, personenbezogene Daten bereitzustellen. Dies kann sie von den potenziellen Vorteilen, die IKT bieten können, ausschließen.
Migranten	Die Art der Schutzbedürftigkeit von Migranten ist sehr unterschiedlich. Ärmere Migranten können viele der Arten erfahren, mit denen Flüchtlinge und Asylbewerber konfrontiert sind, während Migranten mit hohem Einkommen ganz andere Arten von Schutzbedürftigkeit erfahren können (z. B. Stress, Ressentiments in der lokalen Bevölkerung).	Sprachbarrieren können das Risiko erhöhen, dass ihre personenbezogenen Daten missbraucht werden. Außerdem können sich die Daten- und IKT-Vorschriften in ihrem neuen Land von denen unterscheiden, an die sie gewöhnt sind.
Mitglieder der Sinti-Gemeinschaft	Sinti werden häufig diskriminiert und befinden sich oft außerhalb der formalen Supportsysteme (z. B. Schulen, Gesundheitswesen).	Aus Sorge vor Missbrauch zögern sie möglicherweise, personenbezogene Daten bereitzustellen. Dies kann sie von den potenziellen Vorteilen, die IKT bieten können, ausschließen.
Mitglieder der Roma-Gemeinschaft	Die Roma wurden in der Vergangenheit in ganz Europa verfolgt, was dazu führt, dass viele Roma in Bezug auf geringes	Aus Sorge vor Missbrauch zögern sie möglicherweise, personenbezogene Daten bereitzustellen. Dies kann sie von

	Einkommen, Beschäftigung, Bedrohung ihres Wohlergehens und viele andere Formen der Schutzbedürftigkeit stärker schutzbedürftig sind als andere Bevölkerungsgruppen.	den potenziellen Vorteilen, die IKT bieten können, ausschließen.
Kranke oder verletzte Personen, einschließlich Krankenhaus- und Langzeitpatienten	Gesundheitsprobleme machen die Menschen unmittelbar verwundbar und können andere Arten der Schutzbedürftigkeit (z. B. Einkommensverluste) noch verschärfen.	Eventuell sind sie nicht in der Lage, in die Verwendung ihrer Daten einzuwilligen, zum Beispiel wenn sie sediert, verwirrt oder bewusstlos sind. Oder sie willigen zu leicht ein, zum Beispiel wenn sie sich eine Verbesserung durch die medizinische Forschung versprechen (vorübergehende Schutzbedürftigkeit).
Menschen mit chronischen und/oder langfristigen Erkrankungen oder mehreren chronischen Erkrankungen	Die Schutzbedürftigkeit hängt von der Art und Schwere der Erkrankung ab. Viele dieser Erkrankungen schränken zum Beispiel die Fähigkeit der Menschen ein, zu arbeiten und ein Einkommen zu erzielen.	Diese Menschen werden oft von Online-Informationen ausgeschlossen, je nachdem, ob integrative IKT-Tools implementiert und verfügbar sind. Zum Beispiel können Menschen mit Epilepsie aufgrund von Blitzen/Licht von Bildschirmen (lichtempfindliche Epilepsie) von bestimmten nicht inklusiven Online-Ressourcen ausgeschlossen werden.[13]
Menschen, die in einem Pflegeheim leben	Menschen, die in einem Pflegeheim leben, werden viele alltägliche Entscheidungen abgenommen. Dieser Mangel an Kontrolle über ihr Leben kann ihre Schutzbedürftigkeit in vielerlei Hinsicht erhöhen (z. B. in Bezug auf ihre Ernährung, ihre Gesundheitsversorgung, ihre Finanzen).	Bei vielen Heimbewohnern kann es vorkommen, dass die Daten über sie von anderen kontrolliert werden, z. B. von Familienmitgliedern oder vom Personal des Heims. Dies schränkt ihre Möglichkeiten ein, die Verwendung ihrer personenbezogenen Daten zu kontrollieren oder gar zu beeinflussen.

Menschen mit körperlichen oder geistigen Behinderungen und Störungen (oder beidem), sowohl vorübergehend als auch dauerhaft	Die Schutzbedürftigkeit hängt von der Art und Schwere der Behinderungen und Störungen ab. Beispielsweise können Menschen mit eingeschränkter Mobilität von anderen abhängig sein, was ihre Schutzbedürftigkeit in Bezug auf Ausbeutung oder Vernachlässigung erhöht.	Manche Behinderungen können dazu führen, dass Menschen Hilfe benötigen, um auf Daten zuzugreifen oder sie weiterzugeben, oder um Datenschutzerklärungen zu verstehen bzw. ihre Einwilligung zu geben. Dies schränkt ihre Kontrolle über den eigenen Datenschutz ein.
Menschen mit eingeschränkten Kommunikationsfähigkeiten, z. B. Sprachbehinderungen	Eingeschränkte Kommunikationsfähigkeiten hindern Menschen daran, in einer Reihe von Szenarien Informationen anzufordern oder dazu beizutragen. Dies kann bedeuten, dass ihre Bedürfnisse, Ansichten oder Erwartungen nicht in vollem Umfang berücksichtigt werden (z. B. in öffentlichen Debatten).	Einige Einschränkungen in der Kommunikationsfähigkeit können dazu führen, dass Menschen Hilfe benötigen, um auf Daten zuzugreifen oder sie weiterzugeben, oder um Datenschutzerklärungen zu verstehen bzw. ihre Einwilligung zu geben. Dies schränkt ihre Kontrolle über den eigenen Datenschutz ein.
Sehbehinderte oder blinde Menschen	Zwar gibt es zahlreiche Angebote für sehbehinderte und blinde Menschen, doch sind diese nicht für alle verfügbar oder erschwinglich, was ihre Schutzbedürftigkeit erhöht.	Sie verwenden wahrscheinlich Software, die ihnen den Bildschirm/die Plattform vorliest, wodurch die Privatsphäre dieser Informationen eingeschränkt wird. Darüber hinaus könnte ihr Zugang zu Informationen eingeschränkt sein, wenn beispielsweise die benötigten Websites es der Software nicht erlauben, alles vorzulesen (z. B. Optionen in Ankreuzfeldern).
Menschen, die aufgrund ihrer Sprache ausgegrenzt sind oder mit Sprachbarrieren zu kämpfen haben	Menschen, die die Sprache ihres Wohnsitzlandes nicht sprechen (z. B. einige Migranten und Flüchtlinge oder Minderheiten wie die kreolischsprachige Bevölkerung in Portugal), haben weniger Zugang zu Informationen über Unterstützungsmaßnahmen, was ihre Schutzbedürftigkeit erhöht.	Nicht-Muttersprachlern innerhalb eines Landes oder Sprechern von Minderheitensprachen fehlen oft Informationen über ihre digitalen Rechte in ihrer eigenen Sprache.

Menschen, die nicht fließend Englisch sprechen	Da Englisch die vorherrschende Sprache in ganz Europa ist, sind bestimmte Informationen möglicherweise nur in dieser Sprache verfügbar oder werden in dieser Sprache besonders hervorgehoben. Diejenigen, die kein Englisch sprechen oder verstehen, können gegenüber denjenigen, die es können, im Nachteil sein.	Ein Großteil der Informationen über Datenrechte und den Schutz der Privatsphäre ist in englischer Sprache, wodurch diese Gruppen benachteiligt werden. Wenn Umfragen und Debatten in englischer Sprache abgehalten werden, haben sie wahrscheinlich auch weniger Möglichkeiten, ihre Ansichten über die Entwicklung und den Fortschritt der IKT mitzuteilen.
Kinder / Unterhaltsberechtigte / Minderjährige	Jüngere Menschen sind von Natur aus schutzbedürftig, da ihnen viele der Eigenschaften fehlen, die die Schutzbedürftigkeit verringern (z. B. Größe, Stärke, abgeschlossene Ausbildung, Unabhängigkeit, Einkommen).	Junge Menschen können rechtlich nicht in die Verwendung ihrer Daten einwilligen. Sie wissen vielleicht nicht, wie sie sich über den Missbrauch ihrer Daten beschweren können, oder sind sich nicht bewusst, dass sie es können.
Junge Erwachsene (18-25 Jahre)	In vielen Ländern hat diese Altersgruppe Schwierigkeiten, Zugang zu den Vorteilen zu erhalten, die die älteren Generationen hatten, z. B. sichere und gut bezahlte Arbeitsplätze oder erschwinglichen Wohnraum.	Ein Mangel an Arbeit und/oder Wohnraum kann den Zugang zu Informationen über digitale Rechte und IKT erschweren (z. B. aufgrund eines fehlenden Internetzugangs zu Hause).
20- bis 40-Jährige	In vielen europäischen Ländern (z. B. in Portugal und den Niederlanden) sind Menschen dieser Altersgruppe häufiger selbständig oder freiberuflich tätig. Als solche sind sie, insbesondere in Krisenzeiten (wie der Covid-19-Pandemie), anfällig für dramatische Einkommensschwankungen. Möglicherweise haben sie auch junge Familien und sind daher stärker schutzbedürftig (z. B. in finanzieller Hinsicht).	Umgekehrt verfügen sie möglicherweise über ein höheres Maß an technischen Fähigkeiten und Bildung als andere Altersgruppen. Das bedeutet, dass sie weniger anfällig für rechtliche und ethische Fragen in Bezug auf Datenschutz, IKT und ihre digitalen Rechte sind.

Ältere, gebrechliche oder gehbehinderte Menschen	Das Alter ist von Natur aus eine schutzbedürftige Lebensphase, da die Menschen schwächer und abhängiger von anderen werden können.	Auch wenn das Alter nicht immer mit digitalem Analphabetismus verbunden ist, so ist das Bewusstsein für rechtliche und ethische Fragen im Zusammenhang mit IKT, Daten und Privatsphäre bei älteren Menschen möglicherweise geringer als bei der „digitalen Generation“, die mit dieser Technologie aufgewachsen ist.
Menschen, die sowohl kurz- als auch langfristig arbeitslos oder unterbeschäftigt sind	Arbeitslosigkeit verschlimmert andere Formen der Schutzbedürftigkeit, insbesondere die finanzielle Schutzbedürftigkeit und die Wohnsituation. Sie kann auch zu gesundheitlichen und psychischen Problemen führen.	Arbeitslose verpassen möglicherweise die IKT-Schulungen und Informationen, die am Arbeitsplatz angeboten werden. Möglicherweise haben sie zu Hause keinen Online-Zugang (aus finanziellen Gründen), was bedeutet, dass sie keine Kenntnis von Informationen über IKT haben, die zunehmend online verbreitet werden.
Menschen mit niedrigem wirtschaftlichen Status	Ähnlich wie die Arbeitslosigkeit verschlimmert ein niedriger wirtschaftlicher Status andere Formen der Schutzbedürftigkeit, insbesondere die finanzielle Schutzbedürftigkeit und die Wohnsituation. Er kann auch zu gesundheitlichen und psychischen Problemen führen.	Die Menschen in dieser Gruppe haben möglicherweise zu Hause keinen Online-Zugang (aus finanziellen Gründen), was bedeutet, dass sie die Informationen über IKT, die zunehmend online verbreitet werden, nicht kennen.
Empfänger von Sozialfürsorgeleistungen	Menschen dieser Gruppe können viele andere Formen der Schutzbedürftigkeit erfahren (z. B. schlechter Gesundheitszustand, geringes Einkommen, unsichere Wohnverhältnisse).	Menschen in dieser Gruppe haben möglicherweise keinen Zugang zu IKT-Schulungen und -Informationen, die am Arbeitsplatz angeboten werden, und/oder sie haben zu Hause keinen Online-Zugang (aus finanziellen Gründen), was bedeutet, dass sie die Informationen über IKT, die zunehmend online verbreitet werden, nicht kennen.

Analphabeten	Viele der Informationen, die unser Leben bestimmen und uns unterstützen sollen, werden hauptsächlich in schriftlicher Form bereitgestellt. Analphabetismus ist ein großes Hindernis für den Zugang zu diesen Informationen und macht diese Menschen verwundbar. Analphabetismus kann auch ein Faktor sein, wenn Menschen einen niedrigeren wirtschaftlichen Status haben.	Viele Informationen über rechtliche und ethische Fragen im Zusammenhang mit IKT werden in schriftlicher Form weitergegeben, insbesondere online. Analphabetismus bedeutet, dass die Menschen diese Informationen weniger gut kennen und verstehen können.
Digitale Analphabeten oder Menschen mit begrenzten technischen Kenntnissen	Viele der Informationen, die unser Leben bestimmen und uns unterstützen sollen, werden zunehmend online zur Verfügung gestellt, z. B. Arzttermine, die nur online gebucht werden können, oder Informationen, die nur über soziale Medien verbreitet werden.	Diese Menschen laufen Gefahr, den Anschluss zu verlieren, da Informationen und Dienstleistungen zunehmend online angeboten werden.
Offline-Gemeinschaften	Dies ist nicht dieselbe Schwachstelle wie digitaler Analphabetismus: Es handelt sich eher um ein Problem des Zugangs/der Infrastruktur als um ein Problem der Fähigkeiten/Kapazitäten. Offline-Gemeinschaften sind jedoch mit vielen der gleichen Probleme konfrontiert wie digitale Analphabeten.	Diese Menschen laufen Gefahr, den Anschluss zu verlieren, da Informationen und Dienstleistungen zunehmend online angeboten werden.
Menschen mit eingeschränktem Zugang zu öffentlicher Infrastruktur	Beispielsweise haben Menschen in ländlichen Gebieten in einigen Ländern keinen guten Zugang zu Infrastrukturen wie Krankenhäusern, Bibliotheken, leistungsfähigen Breitbandnetzen, Kinderbetreuung und anderen Unterstützungssystemen. Dies macht sie relativ schutzbedürftig, insbesondere in Krisenzeiten wie der Covid-19-Pandemie.	Der Mangel an Infrastruktur kann sich auf einen begrenzten Internetzugang (z. B. schwache oder teure Breitbandverbindungen) und andere IKT-Dienste erstrecken. Dies kann den Zugang zu Informationen über die Rechte der Personen in Bezug auf IKT, Daten und Privatsphäre einschränken.

Gemeinschaften außerhalb der Forschungsprozesse	Wissenschaft und Forschung bilden die Grundlage für viele Bereiche der Gesellschaft, wie z. B. Gesundheitswesen, Regierungsführung und Bildung. Da diese Gemeinschaften außerhalb dieser Prozesse stehen, entweder als Forscher oder als Betroffene Personen, wird ihr Leben von Forschungsprozessen beeinflusst, an denen sie weder beteiligt sind noch eine Stimme haben. Infolgedessen kann es sein, dass die aus der Forschung abgeleiteten Richtlinien nicht auf ihre besonderen Bedürfnisse eingehen oder ihre spezifischen Schwachstellen nicht verringern.	Dies gilt auch für die IKT-gestützte Forschung: Gemeinschaften, die keinen Anteil oder kein Mitspracherecht am Prozess oder keinen Zugang zu den Ergebnissen haben, können feststellen, dass die Auswirkungen dieser Forschung (z. B. Richtlinien, Finanzierungsentscheidungen) nicht ihren Bedürfnissen entsprechen oder sie nicht unterstützen. Online-Umfragen oder -Fragebögen sind zum Beispiel eine zunehmend verbreitete Forschungsmethode – schließen aber Offline-Gemeinschaften fast vollständig aus.
Menschen, die von Phänomenen betroffen sind, auf die sie keinen Einfluss haben	Extreme Ereignisse oder Phänomene können zu einer unerwarteten Schutzbedürftigkeit führen. Dies kann in Form von Naturkatastrophen (z. B. Vulkane, globale Pandemien) und extremen Klimaereignissen (z. B. Dürren, Überschwemmungen) geschehen, aber auch in Form von Lebensereignissen (z. B. unerwartete Krankheit, Unfälle, Verlust des Arbeitsplatzes, Tod in der Familie). Das unerwartete Eintreten solcher Ereignisse macht es schwierig, sich darauf vorzubereiten, sodass die Menschen weniger widerstandsfähig sind.	Nach einer Krise können die Menschen müde, gestresst oder verwirrt sein und daher personenbezogene Daten eher (d. h. mit weniger Aufmerksamkeit) weitergeben oder dies tun, um Zugang zu bestimmten Diensten zu erhalten (z. B. Unterstützung nach einer Katastrophe, medizinische Notversorgung). Ein aktuelles Beispiel ist die Covid-19-Pandemie, bei der persönliche Freiheiten und Fragen der Privatsphäre oft zurückgestellt wurden, um die Ausbreitung des Virus zu bekämpfen.
Jeder Bürger, der sich aus irgendeinem Grund für schutzbedürftig hält	Die Art und Schwere dieser Schutzbedürftigkeit, ob IKT-bezogen oder nicht, hängt von der Wahrnehmung des Betroffenen ab. Es ist jedoch wichtig zu erkennen, dass Schutzbedürftigkeit kein einfaches, messbares Thema ist, sondern subjektiv, verborgen und persönlich sein kann.	

Quelle: Angepasst an den Bericht des COST Action/PANELFIT-Workshops vom März 2020; ergänzt durch die am Ende dieses Leitfadens aufgeführten weiteren Ressourcen.

Was können Sie tun?

Es liegt auf der Hand, dass schutzbedürftige Menschen in ethischen und rechtlichen Diskussionen über IKT mehr Beachtung finden sollten. Darüber hinaus sollten größere Anstrengungen unternommen werden, um sie in die Entwicklung und den Einsatz sie betreffender IKT und anderer neuen Technologien einzubeziehen (z. B. künstliche Intelligenz). Idealerweise sollte es spezielle Schutzmaßnahmen geben, um schutzbedürftige Menschen in Bezug auf ihre Privatsphäre und die Verwendung ihrer Daten zu schützen.

Wie bereits erwähnt, ist es jedoch schwierig – vielleicht sogar unmöglich –, eine endgültige Liste aller schutzbedürftigen Gruppen in der Gesellschaft zu erstellen. Dies ist aufgrund des dynamischen Charakters der Schutzbedürftigkeit und des Risikos, die komplexen Situationen der Menschen zu vereinfachen oder die Gefahr der Stigmatisierung zu erhöhen, nicht einmal wünschenswert. Daher kann es eine Weile dauern, bis spezifische Schutzmaßnahmen für die digitalen Rechte schutzbedürftiger Personen in Kraft treten – wenn dies überhaupt jemals der Fall sein wird.

In der Zwischenzeit können alle Bürger Maßnahmen ergreifen, um die Wahrung der digitalen Rechte schutzbedürftiger Personen sicherzustellen. Abbildung 1 skizziert eine Reihe von Maßnahmen.

Es gibt auch spezifische Maßnahmen, die Verantwortliche zum Schutz schutzbedürftiger Personen ergreifen können. Abbildung 2 veranschaulicht einige dieser Maßnahmen.

ABBILDUNG 1	**ABBILDUNG 2**
Betroffene Personen	**Verantwortlicher**
Wer? *Alle Bürger, einschließlich schutzbedürftiger Bürger und derjenigen, die Verantwortung für schutzbedürftige Bürger tragen*	**Wer?** *Forscher, Mitarbeiter, Unternehmen, Behörden, Projektträger usw.*
Wenn jemand Ihre Daten anfordert, prüfen Sie Folgendes: Wer fordert sie an? Wofür werden die Daten verwendet? Wie lange werden die Daten gespeichert? Mit wem werden sie geteilt?	Fragen Sie sich gleich zu Beginn des Prozesses: Wer sind die schutzbedürftigen Personen in meinem Projekt, Prozess oder meiner Aufgabe? Inwieweit sind sie schutzbedürftig?

Falls Sie allgemeine Informationen (z. B. Geschäftsbedingungen, Einwilligungsformulare) erhalten, dann fragen Sie sich: Haben Sie diese verstanden? Bitten Sie anderenfalls um eine leichter verständliche Version (z. B. in Ihrer Muttersprache).	Überlegen Sie, welchen Risiken die Mitglieder jeder schutzbedürftigen Gruppe ausgesetzt sind, wenn Sie deren Daten verwenden – und überlegen Sie, wie diese Risiken verringert oder überwunden werden können.
Wenn Sie immer noch unsicher oder unglücklich darüber sind, wie Ihre Daten verwendet werden, informieren Sie sich. Dies kann über eine Bürgerberatungsstelle oder Ihre nationale Datenschutzbehörde geschehen.	Wenn Sie schutzbedürftige Bürger um personenbezogene Daten bitten, prüfen Sie: Haben sie verstanden, wofür ihre Daten verwendet werden sollen? Wie kann ich ihnen das Verständnis erleichtern? Haben sie ihre Einwilligung in die Verwendung wirklich freiwillig erteilt?
In den meisten Fällen haben Sie das Recht, die Einwilligung in die Verwendung Ihrer Daten zu widerrufen. Prüfen Sie Folgendes, bevor Sie Ihre Daten weitergeben: Wie kann ich meine Einwilligung später widerrufen? An wen muss ich mich wenden?	Suchen Sie nicht nach konkreten Lösungen und betrachten Sie die Behebung von Schwachstellen nicht als ein „Kästchen, das im Rahmen Ihres Projekts abgehakt werden muss“. Betrachten Sie es stattdessen als einen fortlaufenden Prozess, der regelmäßig überprüft werden sollte.
Wenn Ihre Datenrechte verletzt wurden, wenden Sie sich unverzüglich an die zuständige Datenschutzbehörde. Wenn Sie sich dabei nicht sicher fühlen, finden Sie in Tabelle 4 eine Liste von Organisationen, die Ihnen helfen können.	Denken Sie in jeder Phase des Projekts an den Datenschutz für schutzbedürftige Gruppen: Stellt diese Aktivität ein Risiko für schutzbedürftige Gruppen dar? Wie kann ich dies berücksichtigen?

Nützliche Ressourcen

Es gibt mehrere Organisationen, Websites und Projekte, die sich dafür einsetzen, dass die Menschen ihre Rechte in unserer zunehmend digitalen Welt verstehen, und die schutzbedürftige Gruppen auf unterschiedliche Weise unterstützen. In Tabelle 4 finden Sie eine Liste von Nichtregierungsorganisationen, an die Sie sich wenden können, um Informationen/Hilfe im Falle von Datenschutzverstößen zu erhalten. Wenn Sie mehr über diese Themen erfahren möchten, empfehlen wir Ihnen Folgende:

Tabelle 4. Beispiele von Organisationen, die Unterstützung für schutzbedürftige Gruppen in Europa anbieten.

Schutzbedürftige Gruppe	NRO	NRO-Kontaktinformationen
Frauen	European Women's Lobby: https://womenlobby.org/?lang=en	ewl@womenlobby.org
Alleinerziehende Eltern oder Erziehungsberechtigte / Eltern oder Erziehungsberechtigte von schutzbedürftigen Kindern oder abhängigen Personen	COFACE Families Europe: https://coface-eu.org/about-us/	secretariat@coface-eu.org
Obdachlose Menschen	FEANTSA: https://www.feantsa.org/en/about-us/what-is-feantsa	information@feantsa.org
	Homeless in Europe International: https://www.homelessineurope.eu/	homelessineuropehope@gmail.com
Menschen mit einer oder mehreren Abhängigkeiten, wie Drogenabhängigkeit und/oder Alkoholismus	Dianova International: https://www.dianova.org/	switzerland@dianova.org
Menschen, die unter häuslicher Gewalt, psychischem und/oder sexuellem Missbrauch leiden oder davon bedroht sind	Women Against Violence Europe: https://wave-network.org/	office@wave-network.org
	Rape Crisis Network Europe --> Dort gibt es auch eine lange Liste von Organisationen (einige sind NROs): https://www.rcne.com/contact/countries/	Jede Organisation hat ihre eigene E-Mail
Menschen, die Folter, Vergewaltigung oder andere schwere Formen psychischer, physischer oder sexueller Gewalt erlitten haben, wie z. B. Opfer von Genitalverstümmelung bei Frauen	International Rehabilitation Council for Torture Victims:: https://www.irct.org/	irct@irct.org
	End FGM European Network: https://www.endfgm.eu/who-we-are/vision-and-mission/	https://www.endfgm.eu/resources/resource-items/contact/
Opfer von Menschenhandel	La Strada International: https://www.lastradainternational.org/	info@lastradainternational.org
Religiöse Minderheiten	Minority Rights Group International: https://minorityrights.org/about-us/	minority.rights@minorityrights.org
LGBTQIA+ Menschen[1] und sexuelle Minderheiten	Hier finden Sie eine lange Liste mit NROs aus verschiedenen Ländern: https://www.ilga-	

	europe.org/who-we-are/members	
Transgender-Populationen	Transgender Europe: https://tgeu.org/	tgeu@tgeu.org
Häftlinge	European Prison Education Association: https://www.epea.org/epea/	secretary@epea.org
	European Prison Observatory: http://www.prisonobservatory.org/	info@prisonobservatory.org
Haftentlassene	European Prison Observatory: http://www.prisonobservatory.org/	info@prisonobservatory.org
Menschen mit niedrigem oder schlechtem Bildungsniveau	Waag – https://waag.org/en	https://waag.org/en/contact
Personen, die sich außerhalb von Ausbildung und/oder Studium befinden	Waag – https://waag.org/en	https://waag.org/en/contact
Menschen, die falsch informiert sind, einschließlich solcher, die die bereitgestellten Informationen nicht verstehen können	European Association for Viewers Interests (EAVI): https://eavi.eu/about-us/	eavi@eavi.eu
Menschen mit Lernschwierigkeiten, wie Legasthenie, Dysorthografie, Dysgrafie und Dyskalkulie	European Dislexia Association: https://eda-info.eu/about-the-eda/	eda-info@eda-info.eu
Indigene Gruppen	Minority Rights Group International: https://minorityrights.org/about-us/	minority.rights@minorityrights.org
	Europäisches Netzwerk für indigene Völker: https://www.enip.eu/	enip@enip.eu
Die Samen[2]	Saami Coucil: https://www.saamicouncil.net/en/the-saami-council	saamicouncil@saamicouncil.net
Ethnische Minderheiten	Minority Rights Group International: https://minorityrights.org/about-us/	minority.rights@minorityrights.org
	European Network Against Racism:: enar-eu.org/About-us	info@enar-eu.org

Flüchtlinge	European Council on Refugees and Exiles: https://ecre.org/	vzahle@ecre.org
	RotKreuz Europa: https://redcross.eu/about	infoboard@redcross.eu
Asylsuchende	European Council on Refugees and Exiles: https://ecre.org/	vzahle@ecre.org
	RedCross Europe:: https://redcross.eu/about	infoboard@redcross.eu
Migranten	Europäische NRO-Plattform Asyl und Migration: http://www.NRO-platform-asylum-migration.eu/	comms@migpolgroup.com
	RedCross Europe:: https://redcross.eu/about	infoboard@redcross.eu
Mitglieder von Sinti-Gemeinschaften	Waag – https://waag.org/en	https://waag.org/en/contact
Mitglieder der Roma-Gemeinschaft	European Roma Rights Centre: http://www.errc.org/	office@errc.org
Kranke oder verletzte Personen, einschließlich Krankenhaus- und Langzeitpatienten	Hirnverletzte und ihre Familien: https://bif-ec.com/about-2/	https://bif-ec.com/contact/
Menschen mit chronischen und/oder langfristigen Erkrankungen oder mehreren chronischen Erkrankungen	EUROFEA: https://www.euforea.eu/NRO	contact@euforea.eu
Menschen, die in einem Pflegeheim leben	AGE: https://www.age-platform.eu/about-age	info@age-platform.eu
Menschen mit körperlichen oder geistigen Behinderungen und Störungen (oder beidem), sowohl vorübergehend als auch dauerhaft	Inclusion Europe:: https://www.inclusion-europe.eu/what-we-do/	secretariat@inclusion-europe.org
Menschen mit eingeschränkter Kommunikationsfähigkeit, z. B. Sprachbehinderungen	Inclusion Europe:: https://www.inclusion-europe.eu/what-we-do/	secretariat@inclusion-europe.org
Sehbehinderte oder blinde Menschen	European Blind Union: https://www.euroblind.org/	ebu@euroblind.org
Menschen, die aufgrund ihrer Sprache ausgegrenzt sind oder mit Sprachbarrieren zu kämpfen haben	European Council on Refugees and Exiles:: https://ecre.org/	vzahle@ecre.org

Menschen, die nicht fließend Englisch sprechen	European Council on Refugees and Exiles:: https://ecre.org/	vzahle@ecre.org
Kinder / Unterhaltsberechtigte / Minderjährige	Eurochild: https://www.eurochild.org/	info@eurochild.org
Junge Erwachsene (18-25 Jahre)	ERYICA – European Youth Information and Counselling Agency: https://www.eryica.org/eryica	secretariat@eryica.org
20- bis 40-Jährige	ERYICA – European Youth Information and Counselling Agency: https://www.eryica.org/eryica	secretariat@eryica.org
Ältere, gebrechliche oder gehbehinderte Menschen	AGE: https://www.age-platform.eu/about-age	info@age-platform.eu
Menschen, die sowohl kurz- als auch langfristig arbeitslos oder unterbeschäftigt sind	Das Europäische Anti-Armuts-Netzwerk (EAPN): https://www.eapn.eu/who-we-are/what-is-eapn/	https://www.eapn.eu/who-we-are/contact-us/
Menschen mit niedrigem wirtschaftlichen Status	Das Europäische Anti-Armuts-Netzwerk (EAPN): https://www.eapn.eu/who-we-are/what-is-eapn/	https://www.eapn.eu/who-we-are/contact-us/
Empfänger von Sozialfürsorgeleistungen	Social Services Europe: https://www.socialserviceseurope.eu/why-we-do-it	info@socialserviceseurope.eu
Analphabeten	World Literacy Foundation (Diese NRO ist weltweit tätig. Es handelt sich nicht um eine europäische NRO, sie verfügt jedoch über ein Büro im Vereinigten Königreich): https://worldliteracyfoundation.org/about-us/	Kontaktformular am Ende der Seite: https://worldliteracyfoundation.org/about-us/
Digitale Analphabeten oder Personen mit begrenzten technischen Kenntnissen	All digital: https://all-digital.org/about-us/	contact@all-digital.org
	European Digital Learning Network: http://dlearn.eu/	http://dlearn.eu/contact/
Offline-Gemeinschaften	EU-Büro des Roten Kreuz	+32 (0) 2 230 54 64
Menschen mit eingeschränktem Zugang zu öffentlicher Infrastruktur	PREPARE – Partnership for Rural Europe: http://www.preparenetwork.org/partnership/partners#ecovast	Kim.Smedslund@suomenkylat.fi
	European Council for the Village and Small Town: http://www.ecovast.org/english/	valeriecarter@ecovast.org

	about_e.html	
Gemeinschaften außerhalb von Forschungsprozessen	European Centre for Minority Issues: https://www.ecmi.de/	info@ecmi.de
Menschen, die von Phänomenen betroffen sind, auf die sie keinen Einfluss haben	Climate Action Network (CAN) Europa: https://caneurope.org/about-us/	info@caneurope.org
Jeder Bürger, der sich aus irgendeinem Grund für schutzbedürftig hält	Waag – https://waag.org/en	https://waag.org/en/contact

Schutzbedürftige Personen und Gruppen

Statewatch fördert die Veröffentlichung von investigativem Journalismus und kritischer Forschung in Europa in den Bereichen Staat, Justiz und Inneres, bürgerliche Freiheiten, Rechenschaftspflicht und Offenheit. Verfügbar in Englisch. www.statewatch.org/about/

Die Website S**ocial Protection and Human Rights** enthält einen Leitfaden zu benachteiligten und schutzbedürftigen Gruppen in der Gesellschaft. Verfügbar in Englisch.

https://socialprotection-humanrights.org/key-issues/disadvantaged-and-vulnerable-groups/

In diesen Videos der Web Accessibility Initiative werden die Auswirkungen einer besseren Zugänglichkeit zum Internet und die Vorteile für alle Beteiligten anhand von Beispielen aus verschiedenen Bereichen erläutert. Verfügbar in Englisch.

www.w3.org/WAI/perspective-videos/

Rechtliche und ethische Fragen im Zusammenhang mit IKT, Daten und Privatsphäre

Das Projekt **„Global Data Justice“** konzentriert sich auf die verschiedenen Debatten und Prozesse rund um die Datenverwaltung in verschiedenen Regionen und zeigt die übergreifenden Prinzipien und Bedürfnisse auf, die die Verwaltung der Datentechnologie in Richtung soziale Gerechtigkeit lenken können. Verfügbar in Englisch. https://globaldatajustice.org/

Das **Data Justice Lab** untersucht die Beziehung zwischen „Datafizierung“ und sozialer Gerechtigkeit, z. B. die Richtlinien und Auswirkungen von datengesteuerten Prozessen und Big Data.

Die Website des Labs enthält viele hilfreiche Veröffentlichungen und Informationen über bevorstehende Veranstaltungen. Verfügbar auf Englisch. https://datajusticelab.org/

Die Digital Security Helpline von Access Now arbeitet mit Einzelpersonen und Organisationen auf der ganzen Welt zusammen, um deren Sicherheit im Internet zu gewährleisten. Wenn Sie schutzbedürftig sind, können sie Ihnen helfen, Ihre digitalen Sicherheitsmaßnahmen zu verbessern. Wenn Sie bereits betroffen sind, bietet Access Now schnelle Hilfe in Notfällen. Verfügbar in Arabisch, Englisch, Französisch, Deutsch, Italienisch, Portugiesisch, Russisch, Spanisch und Tagalog. www.accessnow.org/help/

Das Data Detox Kit von Tactical Tech bietet alltägliche Schritte, mit denen Sie Ihre digitale Privatsphäre, Ihre Sicherheit und Ihr Wohlbefinden auf eine Weise kontrollieren können, die Sie als richtig empfinden. Erhältlich in 35 Sprachen. https://datadetoxkit.org/en/home

Das **Future of Privacy Forum** und die **FPF Education and Innovation Foundation** sind Katalysatoren für den Datenschutz und die Wissenschaft und fördern auf Grundsätze gestützte Datenpraktiken zur Unterstützung neuer Technologien. Verfügbar in Englisch. https://fpf.org/resources/

Das Netzwerk **European Digital Rights** (EDRi) verteidigt die Grundrechte im digitalen Zeitalter, setzt sich für angemessene Gesetze und politische Maßnahmen ein und sensibilisiert für die wichtigsten Fragen im Zusammenhang mit digitalen Rechten. Verfügbar auf Englisch. https://edri.org/

Der Datenschutzleitfaden von **Privacy International** enthält eine Fülle von nützlichen Informationen zu Fragen des Datenschutzes. Erhältlich in Englisch.

https://privacyinternational.org/report/2255/data-protection-guide-complete

Weitere Lektüre

Wenn Sie mehr über einige der in diesem Leitfaden angesprochenen Themen lesen möchten, empfehlen die Autoren dieses Leitfadens die folgenden Artikel als guten Ausgangspunkt.

Dieser Artikel von **Privacy International** untersucht, wie datengesteuerte Einwanderungspolitiken routinemäßig zu einer diskriminierenden Behandlung von Migranten führen, wobei der Schwerpunkt

auf dem Vereinigten Königreich liegt. https://privacyinternational.org/long-read/4000/10-threats-migrants-and-refugees

Dieser Artikel auf der Website der **Data-Pop Alliance** ist die Zusammenfassung eines Buchkapitels mit dem Titel „Group privacy in the age of Big Data“. Darin wird erörtert, wie Big Data die Grenzen zwischen individuellen Daten und Gruppendaten verwischten und was dagegen getan werden kann.

https://datapopalliance.org/item/group-privacy-in-the-age-of-big-data/

Dieser Artikel des **European Data Journalism Network** mit dem Titel „Das Unzählbare: Wie Covid-19 die Gesundheit von Migranten und Flüchtlingen beeinflusst hat" ist ein Beispiel dafür, wie sich Arten von Schutzbedürftigkeit oft gegenseitig verstärken. Verfügbar auf Englisch, Französisch, Deutsch und Italienisch.

www.europeandatajournalism.eu/eng/News/Data-news/The-uncountable-How-Covid-19-affected-migrants-and-refugees-health

Weitere Informationen

Die monatlichen PANELFIT-Chats behandelten eine breite Palette von Themen rund um Daten, IKT, Datenschutz und Rechte. Die gesamte Reihe kann über die PANELFIT-Website erneut angesehen – oder auch angehört – werden. Verfügbar in Englisch.

www.panelfit.eu/2020/03/23/monthly-chats/

Danksagung

Für diesen Leitfaden verwendete Informationsquellen

Im Rahmen des PANELFIT-Projekts wurden die Informationen in diesem Leitfaden aus den folgenden Quellen zusammengetragen (spezifische Quellen sind im Text angegeben).

Vorträge und Workshops

- Ein PANELFIT-Workshop zum Thema „Creating a citizens’ information pack on ethical and legal issues around ICTs: what should be included?“, 9. bis 10. März 2020 in Berlin, Deutschland.

- Ein Vortrag über schutzbedürftige Bevölkerungsgruppen von Dr. Jedrzej Niklas, Department of Media and Communications, LSE, UK (ehemals University of Leeds), bei einem PANELFIT-Workshop am 5. Juni 2019 in Bilbao, Spanien.
- Persönliche Mitteilung an Professor Anna Lydia Svalastog, Fachbereich Gesundheits- und Sozialstudien, Østfold University College, Norwegen.
- Persönliche Mitteilung an Professor Iñigo de Miguel Beriain, Fakultät für öffentliches Recht der Universität des Baskenlandes, Spanien.
- Überprüfung der endgültigen Fassung und konstruktives Feedback: Professor Gianclaudio Malgieri, EDHEC Business School; Aurelie Pols, Vorstandsmitglied des Center for Privacy & Cybersecurity; Dr. Anna Berti Suman, The European Comission JRC und Marko Šijan, AZOP.

Dokumente

- A. Berti Suman und R. Pierce (2018) „Challenges for citizen science and the EU Open Science Agenda under the GDPR“, *European Data Protection Law Review* 4(3): 284–95, https://doi.org/10.21552/edpl/2018/3/7 (öffentlich zugänglich)
- G. Malgieri und J. Niklas (2020) „Vulnerable data subjects“, *Computer Law & Security Review* 37: 105415, https://doi.org/10.1016/j.clsr.2020.105415 (öffentlich zugänglich)
- S. Milan und T. Treré (2017) „Big Data from the South: The beginning of a conversation we must have“, DataActive, 16. Oktober, https://data-activism.net/2017/10/bigdatasur/ (öffentlich zugänglich)
- L. Peroni und A. Timmer (2013) „Vulnerable groups: The promise of an emerging concept in European Human Rights Convention law“, *International Journal of Constitutional Law* 11(4): 1056–85, https://doi.org/10.1093/icon/mot042 (öffentlich zugänglich)
- PANELFIT-Konsortium (2020) „D5.2 Kritische Analyse des IKT-Datenschutz-Rechtsrahmens (konsolidierte Fassung)", Bilbao, Spanien

Videos und Podcasts

- PANELFIT-Podcast mit Gianclaudio Malgieri, „Vulnerable data subjects and EU Law“, 27. Februar 2020. Verfügbar unter: www.youtube.com/watch?v=fqLfvF-cS70&feature=emb_title

Fotos

Seite 1: © pixabay.com; geralt-9301 / stocksnap-894430 / geralt-9301 / geralt-9301/ josemdelaa-2004715/ vipragen-13256880/

Mitwirkende

Wir möchten uns bei den folgenden Personen für ihre Hilfe bei der Erstellung dieses Leitfadens bedanken:

Alexandra Castañeda, Andreas Matheus, Andrzej Klimczuk, Anna Berti Suman, Annelies Duerinckx, Carolina Doran, Christoforos Pavlakis, Corelia Baibarac-Duignan, Elisabetta Broglio, Federico Caruso, Gefion Thuermer, Helen Feord, Janice Asine, Jaume Peira, Karen Soacha, Katerina Zourou, Katherin Wagenknecht, Katrin Vohland, Linda Freyburg, Marcel Leppée, Marta Camara Oliveira, Mieke Sterken, Tim Woods

Haftungsausschluss

Dieses Projekt wurde aus Mitteln des Programms für Forschung und Innovation Horizont 2020 der Europäischen Union unter der Finanzhilfevereinbarung Nr. 788039 finanziert. Die Verantwortung für den Inhalt dieses Dokuments trägt allein der Verfasser; die Agentur haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Der Workshop, der im März 2020 in Berlin stattfand, wurde in Zusammenarbeit zwischen der European Citizen Science Association (ECSA), der COST Action 15212, dem Institut für Meereswissenschaften (ICM-CSIC) und den Projekten PANELFIT und EU-Citizen.Science organisiert. Finanzielle Unterstützung wurde von PANELFIT (EU-Finanzhilfevereinbarung 788039) und der COST Action 15212 (unterstützt von European Cooperation in Science and Technology) gewährt.

© PANELFIT-Konsortium (2021)
Dieses Werk ist lizenziert unter einer CC BY 4.0 Lizenz: https://creativecommons.org/licenses/by/4.0/

Thematische Dossiers

1. Vermarktung von Daten: Telefonanbieter und personenbezogene Daten

Was geschieht mit unseren gesammelten Handydaten?

Abstract: Einst zeichneten sich diverse Mobilfunkanbieter durch skrupellose Praktiken in Bezug auf die persönlichen Daten ihrer Nutzer aus. Heute wurde dem Missbrauch in Europa zwar ein Riegel vorgeschoben, aber dennoch sollten wir wachsam bleiben, wenn wir neue Telefonverträge unterschreiben.

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/How-phone-companies-use-our-personal-data

Author: Gianluca De Feo, Federico Caruso (OBCT(CCI)

Text:

Fast alle Menschen pflegen ein sehr enges und langlebiges Verhältnis zu ihren Smartphones. Aber diese Endgeräte geben auch viele und unterschiedliche Daten über ihre Benutzer preis, aus denen Datenverarbeiter in verschiedenen Formen Mehrwert schöpfen.

Die gesammelten Daten können dabei durchaus unterschiedlicher Natur sein: Positionsdaten, Daten zum Surfverhalten im Internet, biometrische Daten, Verhaltensmuster etc. Aus diesen Daten lassen sich auch sehr problematische, weil intime Informationen schließen (sexuelle Orientierung, politische Überzeugungen, Zugehörigkeit zu Minderheiten oder verwundbaren Gruppen, Gesundheitszustand), die verwendet werden können, um die Nutzer mit gezielten Botschaften zu erreichen. Das bekannteste Beispiel hierfür ist wohl Cambridge Analytica, ein englisches Datenanalyseunternehmen, das 2016 von Facebook persönliche Daten von über 50 Millionen Nutzern erhielt und mit diesen den US-amerikanischen Wahlkampf beeinflusste, an dessen Ausgang Donald Trump zum Präsident der Vereinigten Staaten erklärt wurde.

In den letzten Jahren lassen sich jedoch Fortschritte beim Schutz der Benutzerdaten verzeichnen, die einerseits neuen Gesetzen der Europäischen Union (allen voran dem Inkrafttreten der GDPR (deutsch: DSGVO 2018), andererseits der Initiative der großen Tech-Konzerne geschuldet sind. So hat Apple 2019 beschlossen, die Geolokalisierung von Nutzern über die Apps in seinem “App Store” zu erschweren - eine Maßnahme, die den Datenschutz seiner Nutzer stärkt, gleichzeitig aber auch als Strategie zu sehen ist, Unternehmen mit ähnlichen Dienstleistungen auszubremsen.

Weshalb sammeln Mobilfunkanbieter unsere Daten überhaupt?

Ob “Smart” oder nicht - um Mobiltelefone zu nutzen, müssen Nutzer einen Vertrag mit einem Mobilfunkanbieter abschließen. Es gibt verschiedene solcher Unternehmen in jedem Land, die zu Konzernen unterschiedlicher Größe gehören und jeweils ihre eigenen Richtlinien bezüglich der Verarbeitung personenbezogener Daten haben.

Letzteres ist ein besonders heikles Thema für Mobilfunkgesellschaften, die anhand der Nutzerdaten Profilerstellungen vornehmen, um uns “maßgeschneiderte” Services oder gezielte Werbung anzubieten, oder diese Daten auch an Drittunternehmen abtreten oder verkaufen, die damit weitere Wertschöpfung erzielen, zum Beispiel Callcenter, deren Kontaktaufnahme zu kommerziellen Zwecken wir oftmals als belästigend empfinden.

Zulässige, unzulässige, problematische Praktiken

Dass es sich um einen für die Mobilfunkanbieter (und die anderen beteiligten Unternehmen) relevanten Markt handelt, lässt sich schon an den Skandalen ablesen, die in den letzten Jahren durch skrupelloses Vorgehen einiger Vertreter dieser Zunft bewirkt wurden. Zum Beispiel der spanische Betreiber Telefónica, der eine App für den deutschen Markt entwickelt hatte, die die Nutzer dafür belohnte, ihre persönlichen Daten zu teilen.

Durch das Inkrafttreten der Datenschutz-Grundverordnung (englisch General Data Protection Regulation, GDPR) in Europa ist der Spielraum für solche Praktiken kleiner geworden, da die Betreiber durch die zuständigen Aufsichtsbehörden nun mit Strafen belegt werden können. Dennoch kommt es immer wieder zu problematischen Vorfällen. Für den Mobilfunksektor enthüllte eine Untersuchung von Netzpolitik aus dem Jahr 2021, dass der deutsche Mobilfunkanbieter O2 seinen Kunden häufig eine Reihe "vorausgefüllter" Felder vorlegte, damit sie allen möglichen Nutzungsformen ihrer personenbezogenen Daten durch das Unternehmen im Voraus zustimmten.

Die Bedeutung persönlicher Daten hat sich darüber hinaus in der Pandemie gezeigt, als Telefongesellschaften den Behörden aggregierte Daten zur Mobilität der Personen zur Verfügung stellten, ohne sich viele Gedanken darüber zu machen, für welche Zwecke und über welchen Zeitraum diese verwendet werden würden. Natürlich handelte es sich um anonymisierte Daten, aber verschiedene Studien auch neueren Datums scheinen die Sorgen von Experten zu bestätigen, dass es möglich ist, auch innerhalb dieser großen Datensätze Personen zuzuordnen. Das bedeutet nicht, dass dies auch eintreten muss, aber schon die bloße Möglichkeit ist eine Bedrohung, vor allem in Zeiten wie diesen, in denen Hackerangriffe immer häufiger werden.

Was die Datenschutzrichtlinien italienischer Mobilfunkgesellschaften verraten

Wer von uns liest und versteht tatsächlich alle Autorisierungen und Klauseln, denen wir zustimmen, wenn wir eine Sim-Karte erwerben oder zu einem neuen Betreiber wechseln? Wir haben uns daher vorgenommen, die Datenschutzrichtlinien der Mobilfunkanbieter im Hinblick auf Telefondienstleistungen und Apps einmal genauer unter die Lupe zu nehmen, zu deren Installation fast alle Betreiber auffordern, um unser Profil zu verwalten, die Menge und die Art der erhobenen Daten sowie die Vollständigkeit der Informationen zu prüfen.

Die Betreiber fragen für das Erheben von Daten das Einverständnis der Nutzer ab. Das gilt für Daten zu Standorten, Internetnutzung und das Erstellen von Nutzerprofilen. Wofür oft kein besonderes Einverständnis eingefordert wird, ist die Weitergabe an Dritte - also an andere Firmen in einer Gruppe, Dienstleister oder noch andere Unternehmen. Bei manchen Fragen sind die Datenschutzrichtlinien aber unklar, was uns daran gehindert hat, die Fragen aus der folgenden

Infografik zu beantworten. Und dann ist da noch die Tatsache, dass viele Nutzer ihre Zustimmung geben werden, ohne sich bewusst zu sein oder darauf zu achten, was das bedeutet.

Denn alle späteren Probleme in Bezug auf den Schutz unserer Daten entstehen zum Zeitpunkt der Abschließung eines neuen Abonnements oder Prepaid-Vertrages, wenn wir ein Feld ankreuzen, das beispielsweise den Betreiber zur Verarbeitung unserer Daten zu kommerziellen Zwecken berechtigt. In diesem Fall dürfen die Telefongesellschaften personenbezogene Daten, aber auch Navigations- und Positionsdaten verwenden, um Gewohnheiten oder Kaufpräferenzen zu ermitteln, gezielte Werbeinhalte zu schalten sowie Daten an Drittanbieter weiterzugeben (die häufig schwer zu identifizieren oder sehr allgemein beschrieben sind), welche ihrerseits Daten zu kommerziellen Zwecken einsetzen. In einigen Fällen werden sie auch Jahre nach Kündigung des Vertrags zu diesen Zwecken weiterverwendet.

Datenschutz und die Apps der italienischen Mobilfunkanbieter

Mobilfunkbetreiber verfügen oft über ihre eigenen Smartphone-Apps, mit denen das Restguthaben, aktive Angebote und vieles mehr angezeigt werden kann. Auch diese Apps, deren Download vonseiten der Betreiber nahegelegt wird, haben ihre eigenen Datenschutzrichtlinien, die sich hinsichtlich der angebotenen Dienstleistungen voneinander unterscheiden können. Wir haben daher auch diese Apps untersucht und die Ergebnisse in der untenstehenden Infografik abgebildet, wobei eine Kategorie für die Apps speziell für Smartphones hinzugefügt wurde: die Trackers. Dabei handelt es sich um Software, die Informationen zum Nutzer der Anwendung sammelt (hier eine detailliertere Erläuterung zu ihrer Funktionsweise) und die in verschiedenen Formen auftreten kann. Die umstrittensten Tracker im Hinblick auf den Schutz persönlicher Daten – auf die wir unsere Untersuchung ausgerichtet haben – erheben Daten, um Nutzer zu identifizieren, erstellen ein Profil, um ihnen gezielte Werbeinhalte anzuzeigen und lokalisieren das mobile Endgerät.

Mit einem von εxodus entwickelten Tool können wir Anwendungen daraufhin untersuchen, welche und wie viele Tracker sie beinhalten.

Die Apps von Telekom und Vodafone haben jeweils drei Tracker: Die der Telekom zwei für Werbung und eine für den Standort, die von Vodafone jeweils einen für Werbung und Standort und noch einen für die Erstellung von Profilen. Congstar benutzt einen Tracker für Werbung und einen für den Standort, 1&1 einen zur Profilerstellung. Bei mobilcom-debitel, O2 und Aldi Talk konnte εxodus keine Tracker feststellen. Der meistgenutzte Tracker ist dabei Huawei Mobile Services Core, Telekom nutzt auch noch Google AdMob.

Wie die Apps deutscher Telefongesellschaften personenbezogene Daten sammeln und verwenden, gemäß ihren Datenschutzrichtlinien

Tippen Sie auf die Kästchen, um weitere Informationen zu erhalten und Auszüge aus den Datenschutzrichtlinien zu lesen

Legend:
🔴 gesammelte, übermittelte oder nicht erteilte Daten
🟡 mit Zustimmung des Nutzers oder nur zu bestimmten Zwecken erhobene oder übermittelte Daten, verschlüsselte Daten oder teilweise erteilte Auskünfte
🟢 nicht erhobene Daten oder vollständig erteilte Auskünfte
⚫ nicht angegeben oder nicht klar

Telekom

🟡 Standortdaten
⚫ Biometrische Daten
🟡 Daten zur Profilerstellung
🟡 Internetnavigationsdaten
🟡 Verhaltensdaten
🔴 Verkauf oder Weitergabe von personenbezogenen Daten an Dritte
⚫ Austausch von Daten mit anderen Unternehmen der Gruppe
🟢 Informationen über den Widerruf der Zustimmung
🟢 Informationen über den Zugang zu personenbezogenen
🟢 Informationen über die Möglichkeit einer Beschwerde

3

congstar GmbH

⚫ Standortdaten
⚫ Biometrische Daten
🔴 Daten zur Profilerstellung
⚫ Internetnavigationsdaten
🔴 Verhaltensdaten
🔴 Verkauf oder Weitergabe von personenbezogenen Daten an Dritte
⚫ Austausch von Daten mit anderen Unternehmen der Gruppe
🟢 Informationen über den Widerruf der Zustimmung
🟢 Informationen über den Zugang zu personenbezogenen
🟢 Informationen über die Möglichkeit einer Beschwerde

3

O2

🟡 Standortdaten
🟢 Biometrische Daten
⚫ Daten zur Profilerstellung
⚫ Daten zur Profilerstellung
🔴 Verhaltensdaten
🔴 Verkauf oder Weitergabe von personenbezogenen Daten an Dritte
⚫ Austausch von Daten mit anderen Unternehmen der Gruppe
🟢 Informationen über den Widerruf der Zustimmung
🟢 Informationen über den Zugang zu personenbezogenen
🟢 Informationen über die Möglichkeit einer Beschwerde

5

Aldi Talk

🟡 Standortdaten
⚫ Biometrische Daten
🔴 Daten zur Profilerstellung
⚫ Daten zur Profilerstellung
⚫ Daten zur Profilerstellung
🔴 Verkauf oder Weitergabe von personenbezogenen Daten an Dritte
🔴 Austausch von Daten mit anderen Unternehmen der Gruppe
🟢 Informationen über den Widerruf der Zustimmung
🟢 Informationen über den Zugang zu personenbezogenen
🟢 Informationen über die Möglichkeit einer Beschwerde

2

1&1 Telecom GmbH

🔴 Standortdaten
⚫ Biometrische Daten
🟡 Daten zur Profilerstellung
🟡 Internetnavigationsdaten
⚫ Daten zur Profilerstellung
🔴 Verkauf oder Weitergabe von personenbezogenen Daten an Dritte
⚫ Austausch von Daten mit anderen Unternehmen der Gruppe
🟢 Informationen über den Widerruf der Zustimmung
🟢 Informationen über den Zugang zu personenbezogenen
🟢 Informationen über die Möglichkeit einer Beschwerde

3

mobilcom-debitel GmbH

🔴 Standortdaten
⚫ Biometrische Daten
🔴 Daten zur Profilerstellung
🔴 Internetnavigationsdaten
🔴 Verhaltensdaten
🔴 Verkauf oder Weitergabe von personenbezogenen Daten an Dritte
⚫ Austausch von Daten mit anderen Unternehmen der Gruppe
🟢 Informationen über den Widerruf der Zustimmung
🟢 Informationen über den Zugang zu personenbezogenen
🟡 Informationen über die Möglichkeit einer Beschwerde

4

Vodafone

🔴 Standortdaten
⚫ Biometrische Daten
🟡 Daten zur Profilerstellung
🟢 Internetnavigationsdaten
🔴 Verhaltensdaten
🟢 Verkauf oder Weitergabe von personenbezogenen Daten an Dritte
⚫ Austausch von Daten mit anderen Unternehmen der Gruppe
🟢 Informationen über den Widerruf der Zustimmung
🟢 Informationen über den Zugang zu personenbezogenen
🟢 Informationen über die Möglichkeit einer Beschwerde

10

Source: EDJNet elaboration • Iliad doesn't have a mobile phone app

EUROPEAN DATA JOURNALISM NETWORK
EUROPE EXPLAINED THROUGH DATA

Strafen gegen unzulässige Praktiken

Aufgrund von Verstößen gegen die DSGVO haben die Behörden in ganz Europa bereits mehrere Geldstrafen gegen Telefongesellschaften verhängt. 2020 hat die italienische Aufsichtsbehörde zum Schutz personenbezogener Daten den Betreiber Tim aufgrund massiver Beschwerden der Kunden wegen unerwünschter Werbeanrufe zu einer Geldstrafe von immerhin 28 Millionen Euro verurteilt, da sie einen Missbrauch bei der Verwaltung der Nutzerdaten als erwiesen ansah. 2021 wurde der Anbieter Fastweb aus ähnlichen Gründen zu einer Geldstrafe von 4 Millionen Euro verurteilt. 2020 hat die polnische Aufsichtsbehörde das Unternehmen Virgin Mobile mit einer Strafe von 443.000 Euro belegt, weil es die Sicherheit der personenbezogenen Daten seiner Kunden nicht gewährleistet hat. Eine weitere Strafe verhängte Frankreich Ende 2021, als die nationale Aufsichtsbehörde den Betreiber Free Mobile zu einer Strafe von 300.000 Euro verurteilte, weil er das Auskunfts- und Widerspruchsrecht der Kunden zur Datenverarbeitung nicht garantiert hatte. Das jüngste Beispiel stammt von den verbundenen griechischen Unternehmen Cosmote und Ote, die beide aufgrund von Unregelmäßigkeiten im Gefolge eines Hacker-Angriffs, der zu einem Verlust von 30 GB personenbezogener Daten führte, zu 6 bzw. 3,25 Millionen Euro verurteilt wurden.

Methodik

Zunächst haben wir acht Telefongesellschaften für die Untersuchung ausgewählt: die vier wichtigsten italienischen Telefongesellschaften, die Eigentümer des Netzes sind (Telekom, O2, Vodafone), sowie vier weitere der bekanntesten und wichtigsten virtuellen Betreiber auf nationaler Ebene (Congstar, Aldi Talk, 1&1, Debitel). Wir haben dann die Datenschutzrichtlinie zu Mobiltelefonleistungen auf der Website eines jeden Betreibers untersucht sowie jene zur Nutzung der Betreiber-eigenen Smartphone-Apps untersucht, mit denen die Nutzer ihr Profil verwalten können. Zugrundegelegt wurden zehn vorformulierte Fragen (die in den Infografiken dieses Artikels enthalten sind) zur Art der gesammelten Daten, der Art und Weise, wie diese verwendet werden sowie der Vollständigkeit einiger Informationen. Die erhaltenen Daten wurden in zwei Datensätzen erfasst (einer hinsichtlich der Datenschutzrichtlinien der Dienstleistungen, der andere für die Apps) und dann in die Infografiken überführt. Dabei werden auch die Textteile angezeigt, in denen sich die Antworten auf die von uns gestellten Fragen befinden, die ebenfalls in die Infografiken eingeflossen sind.

So gehen europäische Telefonanbieter mit personenbezogenen Daten um

Abstract: In diesem Artikel erläutern wir unsere Recherchen zum Umgang von Telefonanbietern mit personenbezogenen Daten und weisen dabei auf Probleme mit dem europäischen Recht hin.

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Mobile-operators-and-personal-data-in-Europe

Author: Federico Caruso, Gianluca De Feo (OBCT/CCI)

Text:

Lesbarkeit

Die DSGVO schreibt an mehreren Stellen (Einleitung Nr. 39, 42 und 58, Artikel 7 und 12) vor, dass Informationen zu jeder potenziellen Verarbeitung von personenbezogenen Daten leicht zugänglich

und in klarer einfacher Sprache verfasst sein müssen. Allerdings geben sich die von uns geprüften Firmen trotz dieser Vorschriften keine erkennbare Mühe, sondern liefern weiterhin nur Unmengen an Text, ohne die Lesbarkeit durch Layout, Formulierungen oder grafische Hilfsmittel zu verbessern. Natürlich besteht dieses Problem nicht nur bei Telekommunikationsfirmen – das zeigen umfangreiche Recherchen und die alltäglichen Erfahrungen der Nutzer. Wissenschaftliche Forschungen haben schon vor langer Zeit die Hypothese aufgestellt, dass Informationen am besten grafisch und mit Sinnbildern (Icons) präsentiert werden. Keines der analysierten Unternehmen setzt solche Methoden ein. Dennoch gibt es unterschiedliche Konzepte: Einige Firmen veröffentlichen lediglich ein Rechtsdokument als PDF, ohne besonders auf das Layout oder die Lesbarkeit zu achten. Manche gehen bei der Kommunikation ihrer Richtlinien einen Schritt weiter und fügen zum Beispiel Frage- und Antwortseiten hinzu, oder Seiten, die fast wie kleine Websites aussehen. Insgesamt ist in diesem Punkt noch Luft nach oben. Mit einem einheitlicheren Konzept bei der Strukturierung der Richtlinien der verschiedenen Firmen würden diese eventuell transparenter und Nutzer könnten sie besser vergleichen.

Vollständigkeit

Informationen darüber, wie man auf personenbezogene Daten zugreifen, sie korrigieren, löschen, der Nutzung widersprechen, eine Nutzungserlaubnis kündigen oder sein Beschwerderecht wahrnehmen kann, sollten im Datenschutzhinweis deutlich sichtbar sein. In ihrem Bericht zu Videokonferenzsoftware zitiert die Organisation Noyb Artikel 29 der Richtlinie der Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten und weist darauf hin, dass eine bloße Information der Nutzer über die Existenz dieser Rechte nicht ausreicht: Der Betreiber sollte auch „eine Zusammenfassung der einzelnen Rechte und der Art und Weise, wie die betroffene Person diese Rechte ausüben kann, sowie etwaige Einschränkungen dieser Rechte“ darlegen. Die Unternehmen gehen dabei ganz unterschiedlich vor: Oft werden die Informationen nur teilweise angegeben, mit einer kurzen Beschreibung der Benutzerrechte und manchmal ohne Kontaktdaten für Anfragen. Ein bemerkenswertes Beispiel ist die App von Vodafone Deutschland, die in ihren Datenschutzbestimmungen gar keine diesbezüglichen Informationen liefert. Einige italienische Firmen verwenden hingegen eher vage Formulierungen wie „Sie sind berechtigt, beim Datenschutzbeauftragten eine Beschwerde einzureichen“ (TIM und das Tochterunternehmen Kena Mobile), ohne jegliche Information, wie diese Beschwerde vonstatten gehen soll und auf welcher Rechtsgrundlage.

Kategorien erfasster Daten und Datenverarbeitung

Welche Datenkategorien erfasst werden, ist von Land zu Land ziemlich ähnlich: Meistens werden der Standort, Navigations- und Verhaltensdaten erhoben. Rechtsgrundlage ist generell die Zustimmung des Benutzers. Einige Unternehmen erfassen Daten unabhängig von der Zustimmung und berufen sich auf ihr berechtigtes Interesse. Bei biometrischen Daten ist die Lage nicht mehr ganz so einheitlich. In vielen Fällen wird nicht angegeben, ob biometrische Daten erfasst werden oder nicht, das könnte aber

auch daran liegen, dass sie in die anderen erwähnten Kategorien eingegliedert werden. Typische Merkmale des Scrollens oder Tippens können tatsächlich als biometrische oder als Verhaltensdaten definiert werden. Aber auch Fingerabdrücke oder Gesichtserkennung sind biometrische Daten, die mit jedem in den letzten Jahren hergestellten Smartphone aufgezeichnet werden können. Aus diesem Grund wäre es besser, diese Daten getrennt aufzuführen.

Bei der Profilerstellung, also der Analyse von Nutzerdaten zur Verbesserung des Service, aber auch zur Erstellung „maßgeschneiderter" gewerblicher Angebote, scheint man generell auf das Einholen einer ausdrücklichen Einwilligung zu setzen. Manchmal (z. B. bei Orange und Vodafone in Spanien) wird jedoch angegeben, dass Profile sowieso erstellt werden. Für Kunden von Vodafone und der Congstar GmbH in Deutschland (und bis zu einem gewissen Grad auch von Digi und der Yoigo-App in Spanien) ist die Lage unklar, denn soweit wir dies überprüfen konnten, erwähnt keines dieser Unternehmen ausdrücklich, welche Kategorien von Daten es erfasst, und auch nicht ob diese Daten für die Profilerstellung genutzt werden oder nicht.

Übertragung und Löschung von Daten

Alle Firmen geben an, dass sie unter bestimmten Voraussetzungen personenbezogene Daten an Dritte übertragen. In den meisten Fällen geschieht dies im Zusammenhang mit der Vertragserfüllung oder der Prüfung der Zahlungsfähigkeit des Kunden. In einigen Fällen wird ausdrücklich auf gewerbliche Partner hingewiesen (manchmal solche, die mit dem Betreiber verbunden sind), an die Daten mit Zustimmung des Benutzers für eine Vielzahl von Verwendungszwecken übertragen werden können – so auch für gewerbliche Angebote für Waren oder Dienstleistungen, die mit Telefonen in keinerlei Zusammenhang stehen. Die verwendeten Formulierungen sind oft sehr allgemein gehalten, besonders bei französischen (Orange, Bouygues Telecom) oder deutschen (Vodafone, O2, Congstar GmbH) Unternehmen. Das Gleiche gilt für die Apps dieser Firmen, ebenso für diejenigen der spanischen Yoigo und der deutschen Telekom, Aldi Talk und 1&1 Telecom GmbH.

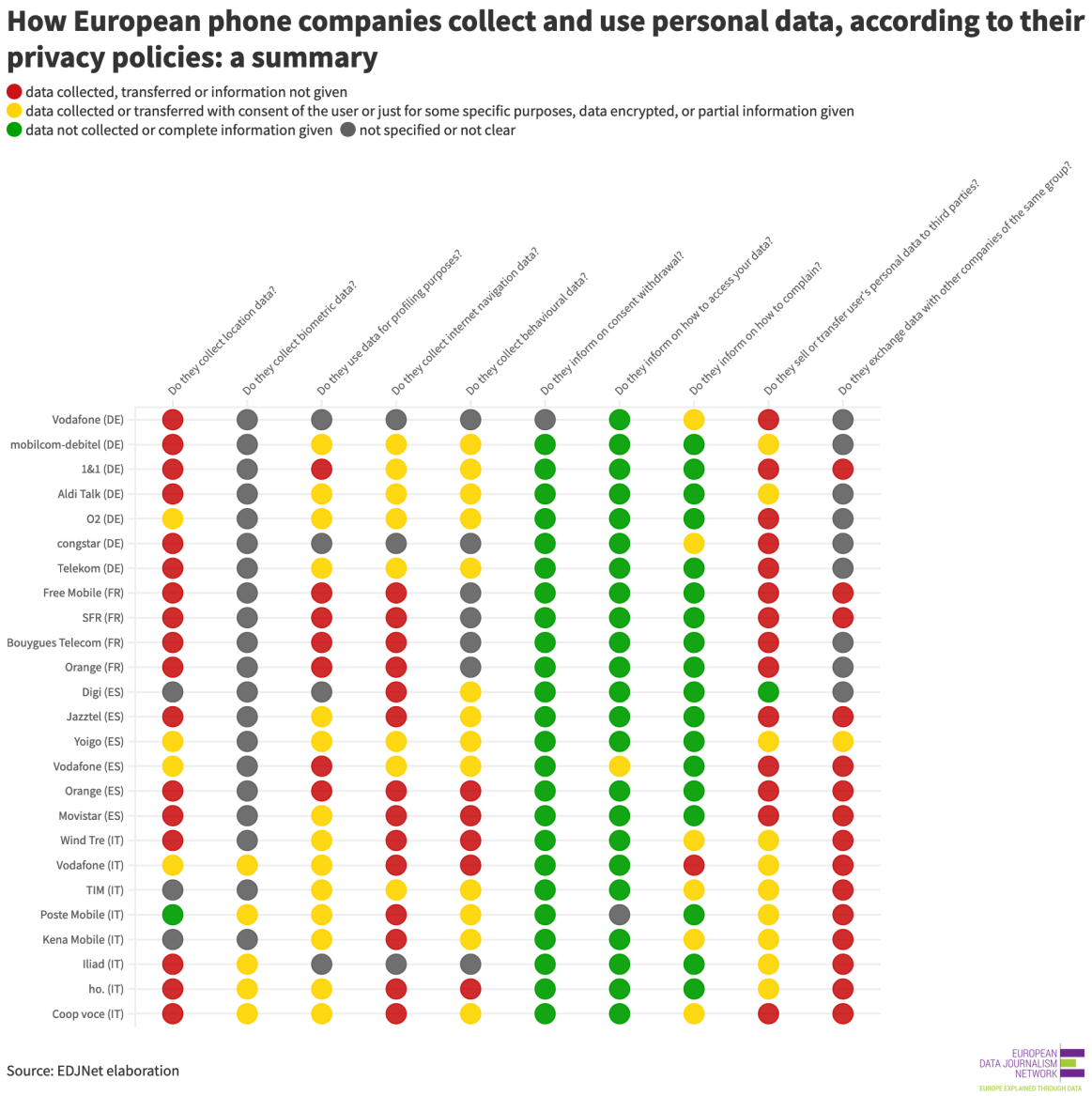
Für die Datenspeicherung verwenden einige Unternehmen kurze Formulierungen und erklären in ein paar Zeilen, dass Daten „für einen Zeitraum aufbewahrt werden, der die Erreichung der Zwecke, für die sie erhoben oder später verarbeitet wurden, nicht überschreitet" (TIM Italia), und nennen auch eine Frist, nach der die Daten gelöscht werden. Andere gehen transparenter vor und veröffentlichen eine Tabelle mit genauen Speicherfristen für verschiedene Datenkategorien (Coop Voce, Ho., Vodafone und Wind Tre in Italien, Bouygues Telecom in Frankreich). In Deutschland werden Daten generell nach 12-14 Monaten gelöscht.

DSGVO

Die zwei wichtigsten DSGVO-Artikel in diesem Zusammenhang sind die Artikel 13 und 15. Stefano Rossetti, ein Rechtsanwalt im Team von noyb.eu, erklärte uns, dass diese Artikel die zwei Zeitpunkte

regulieren, an denen die Verarbeitung personenbezogener Daten im Verhältnis zwischen Benutzer und Unternehmen relevant wird.

Artikel 13 führt die Informationen auf, die das Unternehmen im ersten dieser beiden Zeitpunkte zur Verfügung stellen muss, d. h. in dem Moment, in dem der Benutzer einen Dienst abonniert. Diese Information wird, wie im oben erwähnten noyb-Bericht erläutert, normalerweise in einem Dokument aufgelistet, das „Datenschutzrichtlinie“ heißt und um es in unserer Analyse hauptsächlich geht. In der Beschreibung der Datenschutzrichtlinien müssen drei Punkte immer enthalten sein: Die Datenkategorien, die erhoben werden, der Zweck, zu dem die Daten angefordert werden, und die Rechtsgrundlage auf der die Daten verarbeitet werden. Das Unternehmen muss zudem Folgendes angeben: den Datenverantwortlichen, mögliche Empfänger der erhobenen personenbezogenen Daten (Behörden, andere Unternehmen usw.), die Speicherdauer, und Informationen über mögliche Anträge auf Datenzugriff oder Datenlöschung und über die Möglichkeit, im Fall von Verstößen eine Beschwerde einzureichen.



Bei der Vollständigkeit der bereitgestellten Informationen scheint die neue Richtlinie zum Recht auf Datenzugriff, die derzeit vom Europäischen Datenschutzausschuss (EDSA) erarbeitet wird, dem Datenverarbeiter einen gewissen „allgemeinen Spielraum“ zu lassen: „Informationen [zur Verarbeitung und den Rechten der betroffenen Personen] können auf der Grundlage dessen erfolgen, was bereits im Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen (Art. 30) und der Datenschutzerklärung (Art. 13 und 14) erfasst ist. Diese allgemeinen Informationen müssen aber eventuell zum Zeitpunkt des Antrags aktualisiert oder angepasst werden, um die Verarbeitungstätigkeiten widerzuspiegeln, die in Bezug auf die jeweilige antragstellende Person durchgeführt werden.“

Damit kommen wir zum zweiten wichtigen Zeitpunkt in Artikel 15, der Folgendes festlegt: „Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten“. Während also Artikel 13 regelt, dass das

Unternehmen die nutzenden Personen informieren muss (und wie), legt Artikel 15 die Pflicht des Unternehmens fest, auf alle Zugriffsanträge zu antworten, sodass geprüft werden kann, ob die erhobenen Daten und deren Verarbeitung den Angaben in der Datenschutzrichtlinie und dem Gesetz entsprechen. Für diese Studie haben wir nur den ersten der relevanten Zeitpunkte, also den Moment, in dem Nutzer einen Dienst abonnieren,analysiert.

2. Die EU Cybersicherheitsstrategie

Brüssels Plan für den Schutz der EU vor Cyberattacken

Abstract: Durch die Covid-19-Krise sind wir zu einer digitalen Gesellschaft geworden. Ein Großteil unseres Alltags spielt sich heute in der digitalen Sphäre ab, und dies hat die Mitgliedstaaten verwundbarer gegenüber Cyberattacken gemacht. Um diese zu neutralisieren, hat die Europäische Kommission im Dezember 2020 ihre neue Cybersecurity-Strategie vorgestellt.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Brussel-s-plan-to-protect-the-EU-from-cyberattacks

Text:

"Wer sind Sie? Wie sind Sie in unsere Besprechung gekommen? General, was sollen wir tun? General, Sie haben Recht: Wir müssen in Datenschutz investieren." So reagierte Josep Borrell, Hoher Vertreter der Europäischen Union für Außen- und Sicherheitspolitik, als im vergangenen Jahr eine geheime Videokonferenz der EU-Verteidigungsminister gehackt wurde. Der niederländische Verteidigungsminister hatte zuvor versehentlich ein Bild auf Twitter geteilt, in dem man den Zugangscode für das Meeting erkennen konnte. Ein Landsmann von ihm, Journalist von Beruf, bemerkte das Versehen und schaltete sich bei der geheimen Besprechung zu - die EU-Institution war brüskiert.

Abgesehen von den chaotischen Umständen dieser Datenpanne zeigte der Vorfall die andauernden Schwierigkeiten der EU beim Thema Cybersicherheit auf: In einem Club von 27 Ländern, deren vertrauliche Meetings und Gespräche eigentlich persönlich stattfinden müssten, aufgrund der logistischen Probleme nun aber online abgehalten werden, lässt sich kaum verhindern, dass die eine oder andere Tür für Unbefugte geöffnet bleibt. In einer vernetzten Welt wie der unseren ist es dieses enorme Risiko, das die EU dazu gezwungen hat, sich gegen digitale Angriffe aller Art zu rüsten, wann und wo auch immer sie auftreten.

Die Bedrohung mag unhörbar sein, unsichtbar ist sie nicht. Die Europäische Agentur für Cybersicherheit (ENISA) hat 2020 erfolgreich 304 böswillige Angriffe gegen „kritische Bereiche" identifiziert, mehr als doppelt so viele wie im Jahr 2019. Viele von ihnen waren gegen Krankenhäuser und Gesundheitsdienste gerichtet, Einrichtungen, die während der Pandemie sehr wertvolle Informationen zur Entwicklung von Covid und zu Impfprojekten in ihrem Besitz hatten.

Die Ziele dieser Hackerangriffe können vielfältig sein, vom Datendiebstahl bis hin zur Lahmlegung zentraler Infrastruktur, mit oftmals verheerenden Folgen für das Land, auf das der Angriff abzielt. Eines der spektakulärsten Beispiele der jüngeren Geschichte ist die Attacke auf die Colonial-Pipeline, das größte Ölpipelinesystem der USA, im Mai 2021. Der von einer apolitischen Gruppe professioneller Hacker namens Darkside durchgeführte Angriff zwang die Betreiber zur Unterbrechung des Pipeline-Betriebs, was zu Kraftstoffknappheit an der ganzen Ostküste der USA führte und das Ölunternehmen die Summe von 75 Bitcoins (umgerechnet 3,8 Mio. Euro) kostete, die sie an die Hackergruppe als Lösegeld zahlen musste.

Zum Glück für die EU-Bürger verfügt die EU über einen Plan, so dass die gehackte Sitzung der Verteidigungsminister zwar eine amüsante Anekdote, aber keine Cyberattacke darstellte, in der die gesamte Sicherheit der Europäischen Gemeinschaft auf dem Spiel stand. Im Dezember 2020 legte die Europäische Kommission eine neue Cybersicherheits-Strategie und einen Vorschlag vor, die Richtlinie für Maßnahmen zur Erhöhung der Cybersicherheit in Gemeinschaften in der EU zu verstärken (Richtlinie NIS2).

Ein neues Wettrüsten

Seit 2013 rüstet sich die Europäische Union gegen digitale Angriffe. In den letzten Jahren hat sie verschiedene Initiativen gestartet, eine gemeinschaftliche Abwehr- und Sicherheitsstrategie voranzubringen.

Prominente Maßnahmen sind in diesem Zusammenhang die gemeinsame „Cyber Diplomacy Toolbox“ sowie ein gemeinsamer EU-Politikrahmen für die Cyberabwehr, die beide 2018 verabschiedet wurden und die Koordination zwischen Mitgliedsstaaten verbessern sollen, das Gesetz zur Cybersicherheit (2019), welches das Mandat der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) verlängerte und ihren Namen in Agentur der Europäischen Union für Cybersicherheit änderte und das EU-Instrumentarium für 5G-Sicherheit, ebenfalls 2019 verabschiedet.

In unser hypervernetzten Welt, in der hybride Bedrohungen immer ausgefeilter werden und Staaten wetteifern, Technologien zum Schutz ihrer Systeme auszuarbeiten, wird die Gefahr, im Cyberrennen abgehängt zu werden, allerdings ständig größer. In diesem Aspekt ähnelt das Cybersicherheitsrennen dem Wettrüsten im Kalten Krieg, als die Vereinigten Staaten, die Sowjetunion und ihre Verbündeten sich durch die Entwicklung von Atomwaffen einen stillen

Krieg lieferten. Genau wie heute wurde jeder Vorsprung eifersüchtig gehütet und die technische Entwicklung zwang jede Seite dazu, immer rascher zu agieren.

Deshalb überarbeitet die Europäische Union ihre Cybersicherheits-Strategie kontinuierlich und bemüht sich, Cyberkriminellen stets einen Schritt voraus zu sein. So wurde die 2013 verabschiedete Richtlinie 2017 und abermals im Dezember 2020 überarbeitet.

Dennoch stellt die jüngste Version einen Paradigmenwechsel dar: Den europäischen Institutionen und Mitgliedstaaten stehen inzwischen vereinheitlichte und koordinierte Sicherheitsmaßnahmen zur Verfügung und die EU beabsichtigt jetzt, Instrumente zu entwickeln, mit denen sie unverzüglich und effektiv auf Cyberattacken reagieren oder besser, diese verhüten kann.

Ein ehrgeiziger Plan

In dieser Hinsicht führt die neue Cybersicherheits-Strategie drei Schlüsselbereiche ein: Erstens soll die Erstellung eines Netzwerks mit Künstlicher Intelligenz betriebener Sicherheitseinsatzzentren im Territorium der EU die gemeinschaftliche Resilienz gegen Cyberattacken stärken; diesem wird eine Reform der Sicherheitsgesetze im Hinblick auf Datennetzwerke und -systeme an die Seite gestellt, die in die Richtlinie NIS2 eingeflossen ist.

Die 2016 verabschiedete NIS-Richtlinie führte dazu, dass sich der Fokus der Institutionen in den Mitgliedstaaten auf Cybersicherheit änderte. Sie zwang sie dazu, unter anderem eine nationale Cybersicherheitsstrategie auszuarbeiten und Cyber-Einsatzteams für den Notfall aufzustellen. Letztlich hat sich jedoch diese Richtlinie im heutigen Bedrohungskosmos als zu beschränkt erwiesen.

„Die digitale Transformation der Gesellschaft, die durch die Covid-Krise noch intensiviert wurde, hat die Bedrohungsstufe erhöht und neue Herausforderungen erzeugt, die neuartige und angepasste Reaktionen erfordern. Jede Unterbrechung kann heute weitreichende Auswirkungen auf den gesamten Binnenmarkt haben“ - mit diesen Worten begründete die Europäische Kommission die Vorlage ihrer neuen Strategie.

Diese neuen Maßnahmen sind in der Richtlinie NIS2 gebündelt, die im Oktober grünes Licht vom Europäischen Parlament erhielt, und u.a. die Definition kritischer Branchen erweiterte und die Vorschriften für die 160.000 Unternehmen, die Teil dieser Definition sind, verschärft.

Ziel ist es, die Lücke zwischen europäischen und US-amerikanischen Unternehmen zu schließen, die durchschnittlich 41 % mehr in Cybersicherheit investieren als ihre europäischen Pendants.

Zweitens möchte die Kommission mit ihrer neuen Cybersicherheitsstrategie auch ihre operative Leistungsfähigkeit erweitern, Cyberattacken zu verhüten, abzuschrecken und auf sie zu reagieren, was sich in der Gründung einer geplanten Gemeinsamen Cyber-Einheit ausdrückt. Dieses Team soll koordinierte EU-Reaktionen auf weitreichende Cybervorfälle und Cyberkrisen ausarbeiten und Unterstützung bei der Wiederherstellung nach solchen Attacken bieten. „Diese Bedrohungen sind ein gemeinsamer Feind, deshalb ist es so wichtig, koordiniert vorzugehen, Daten auszutauschen und früh Alarm auszulösen", so die Kommission weiter.

Drittens setzt sich Brüssel für einen globalen und offenen Cyberspace ein, in dem Länder außerhalb der EU mit Mitgliedstaaten an einen Tisch gebracht werden, um ihre Gesetze weltweit zu harmonisieren und so zur weltweiten Sicherheit beizutragen. Mit anderen Worten zielt diese Strategie darauf, eine dem Kalten Krieg ähnliche Cybersicherheits-Landschaft zu verhindern und stattdessen Nationen im kooperativen Geist zusammenzubringen, um die Welt gegen diese Arten von Bedrohungen zu schützen.

Die ENISA und die europäische Cybersicherheitsstrategie

Abstract: Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat die Aufgabe, eine gemeinschaftliche Verteidigung gegen Cyberkriminalität aufzubauen, um Internetattacken wirksam zu begegnen. Nach einem schwierigen Beginn ist die Agentur heute einer der wichtigsten Akteure im Kampf gegen Cyberkriminalität.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/ENISA-The-cornerstone-of-the-EU-s-cybersecurity-strategy

Text:
Bei der Gründung der Agentur im Jahr 2004 steckte Facebook noch in den Kinderschuhen, und Cybersicherheit war weder für die Regierungen noch für die Bürger ein vorrangiges Anliegen. Dieser Umstand kam auch in der Wahl des Sitzes der ENISA an der Peripherie der europäischen Entscheidungszentren – in den griechischen Städten Heraklion und Athen – sowie in ihrem zunächst auf fünf Jahre befristeten Mandat zum Ausdruck.

Im Laufe der Jahre wurde die Agentur jedoch federführend bei der Ausarbeitung einer gemeinschaftlichen Cybersicherheitsstrategie. 2019 wurde zusammen mit ihrer Bezeichnung auch ihr Zuständigkeitsbereich erweitert, obwohl das Akronym weiterhin auf den ursprünglichen Namen verweist (der alte Name der Agentur lautete *Europäische Agentur für Netz- und Informationssicherheit*, auf Englisch: *European network and information security agency).*

> *Die ENISA nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union zu erreichen, unter anderem indem sie die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Verbesserung der Cybersicherheit unterstützt.*
>
> Verordnung (EU) 2019/881, Artikel 3

Die Agentur ist also ein Bezugspunkt für die Entwicklung des europäischen Plans für die Sicherheit von Computernetzwerken. Ohne eine gemeinschaftliche Verteidigungsstrategie, ohne eine zentralisierte Cyberschutzbehörde auf europäischer Ebene wäre die Union ein leichtes Ziel für Cyberkriminelle. Die europäische Kommission hatte die Gründung der ENISA ursprünglich angeregt, um die einheitliche Absicherung des europäischen Kontinents gegen Cyberattacken zu garantieren. In diesem Zusammenhang war es wichtig, alle entsprechenden Richtlinien anzuwenden, damit einige Länder nicht verwundbarer als andere sind, und Hindernisse zu deren Vereinheitlichung aus dem Weg zu räumen. Zudem arbeitet die Agentur im engen Kontakt mit Europol und dem Europäischen Zentrum zur Bekämpfung von Cyberkriminalität.

Die Gründung der ENISA im Jahr 2004 war der Zeit ein wenig voraus, wenn man bedenkt, dass das Internet damals erst noch Teil der alltäglichen Lebenswirklichkeit der EU-Bürger werden sollte. Aber mit der Zunahme der Informations- und Kommunikationstechnologien (ITC) stiegen auch die mit diesen verbundenen Gefahren exponentiell, so dass der Schutz gegen Cyberkriminalität bald nicht mehr nur als Vorsichtsmaßnahme, sondern als Notwendigkeit wahrgenommen wurde, an der die Arbeit der Einrichtung entscheidenden Anteil haben sollte.

Ohne die ENISA wären Cyberattacken, wie die auf das Krankenhaus von Brno (Tschechische Republik) im März 2020, welche mitten in der Pandemie die Verschiebung dringender Operationen sowie die Verlegung schwerkranker Patienten nötig machte,wesentlich häufiger. Die Pandemie hat die Situation komplizierter gemacht: Durch die beschleunigte digitale Transformation der Gesellschaft und der Wirtschaft haben sich die Bedrohungen vervielfacht, während sich die Anwendungsbereiche der Informationstechnologie gleichzeitig diversifiziert haben, von der Wasserversorgung bis hin zur Domotik immer stärker vernetzter Eigenheime.

Kontinuierliches Wachstum

Die ENISA wurde als kleine Agentur mit einer begrenzten Aufgabenstellung gegründet: Für die sichere Vernetzung der Institutionen und Organisationen innerhalb der EU und der Mitgliedstaaten untereinander zu sorgen. 2008, ein Jahr vor Ablauf ihres ersten Mandats, beschlossen das europäische Parlament und der Rat auf Vorschlag der Kommission, ihr Mandat bis 2012 zu verlängern und gaben damit zum Ausdruck, dass die Wertschätzung und die Verbesserung des Schutzes europäischer Netzwerke im öffentlichen Bewusstsein angekommen waren.

2011 wurde das Mandat der Agentur erneut bis 2013 verlängert, dann abermals bis 2020. Im Unterschied zu den vorausgegangenen Maßnahmen wurde bei der zweiten Verlängerung der Mandatsfrist jedoch auch die Rolle der Agentur selbst ausgeweitet. Zeitgleich mit der Veröffentlichung der ersten Strategie für Cybersicherheit der EU wurde die Agentur modernisiert, um sie besser auf einige Aspekte ihrer neuen Amtszeit auszurichten, von denen der wichtigste die Aufstellung eines Netzwerks von *Teams* in allen europäischen Hauptstädten (Cert-Eu) war, um adäquat auf IT-Sicherheitsvorfälle zu reagieren.

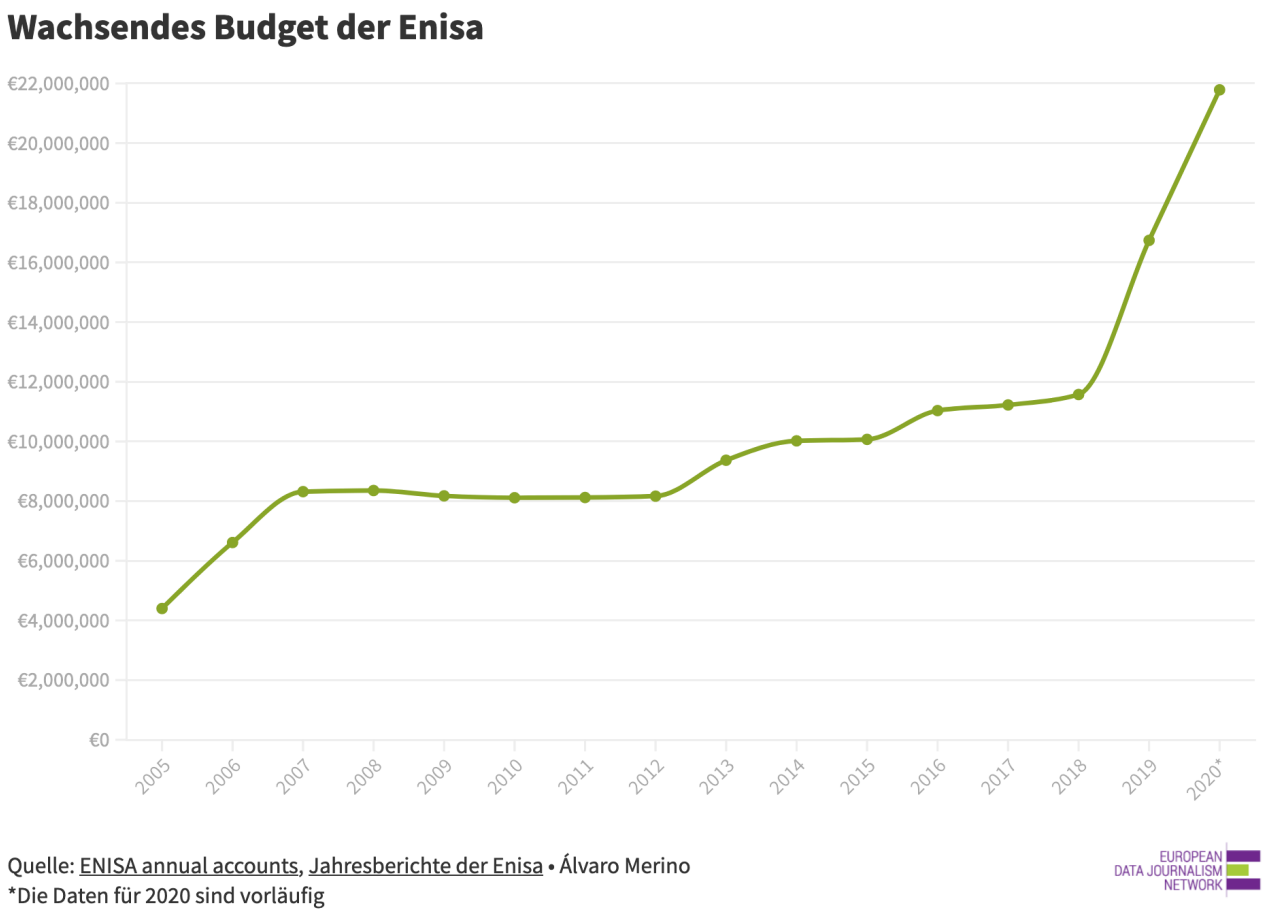
Erst seit Verabschiedung des Cybersecurity Act 2019 ist die Amtszeit der ENISA nicht mehr zeitlich begrenzt. Neben der Aufstockung der ihr zur Verfügung stehenden Mittel wurde die seit 2004 bestehende Befristung der Amtszeit auf fünf Jahre nun aufgehoben und die Agentur für einen unbegrenzte Zeitraum eingerichtet. Mit Änderung ihrer Bezeichnung in ‚Agentur der Europäischen Union für Cybersicherheit' wurde auch ihre beratende Rolle erweitert, und sie erhielt zum ersten Mal klare operative Vorgaben.

Die Agentur unterstützt nun auch die Mitgliedstaaten bei der Festlegung ihrer Prioritäten zur Finanzierung der Forschungs- und Entwicklungstätigkeit im IT-Bereich, und sie hat ein Zertifizierungssystem für ICT-Produkte und -Dienstleistungen in der EU auf den Weg gebracht.

Damit Unternehmen und Verbraucher Vertrauen in die Sicherheit ihrer Daten online haben können, werden sichere Endgeräte benötigt, aber das Fehlen eines einheitlichen europäischen Zertifizierungssystems untergräbt dieses Vertrauen und schränkt den grenzüberschreitenden Handel ein. Deshalb kommt der ENISA die Aufgabe zu, gemeinschaftliche Kriterien festzulegen und die nationalen Mechanismen zur Ausstellung von Zertifizierungen in der Cybersicherheit zu vereinheitlichen. Dies ist eine grundlegende Voraussetzung für eine ganze Reihe von Produkten und Dienstleistungen, von Smart Cards (Kreditkarten, ÖVP-Abos, SIM-Karten) bis hin zu Cloud-Services.

Das Budget der ENISA wurde von Jahr zu Jahr aufgestockt und erreichte 2020 fast 22 Millionen Euro, fünfmal so viel wie bei ihrer Gründung, was die Finanzierung vieler Initiativen im IT-Bereich sicherstellt.

Die meisten Mittel werden von der europäischen Kommission gestellt, während die EWR-Staaten (Island, Liechtenstein, Norwegen und Schweiz) sowie Griechenland – wo die Agentur ihren Sitz hat - kleinere Beiträge beisteuern. 2019 hatte die ENISA 75 Angestellte.



Angesichts der wachsenden Bedeutung der Agentur im Rahmen der europäischen Cybersicherheits-Strategie hat die Europäische Kommission beschlossen, den Sitz der Organisation näher an das europäische Machtzentrum zu rücken. Anstatt aber dafür einen neuen Sitz in einem anderen Land zu beziehen, wurde im vergangenen Juni die Eröffnung einer dritten Geschäftsstelle in Brüssel genehmigt, um eine „regelmäßige und systematische Zusammenarbeit" zwischen der Agentur und den europäischen Institutionen zu gewährleisten.

Seit ihrer Gründung 2004 ist die ENISA nach und nach ist zu einer tragenden Säule der Cybersicherheit in Europa geworden. Der bisherige Höhepunkt dieser Entwicklung sind die Eröffnung ihres neuen Büros in Brüssel und die Konsolidierung ihrer operativen Aufgaben. Dieser Wandel zeigt das Streben der Europäischen Union, die Abwehr von Cyberattacken zunehmend selbst in die Hand zu nehmen.

Cybersicherheit: Zwischen europäischer Koordination und nationalen Agenturen

Abstract: Europäische Agenturen sind für die Unterstützung und Koordination der europäischen Cybersicherheit wichtig. Bestimmte EU-Verordnungen erlauben es den Mitgliedstaaten aber, eigene Stellen für Privatpersonen oder bedeutende nationale Interessen zu bestimmen.

Author: Openpolis

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Cybersecurity-between-European-coordination-and-national-agencies

Text:

In den letzten Jahren ist die Agentur der Europäischen Union für Cybersicherheit (ENISA) angesichts der zunehmenden Herausforderungen in diesem Sektor zu einem immer wichtigeren *Instrument geworden. Der Aufgabenbereich Cybersicherheit in der Europäischen Union basiert auf Artikel 5 des Vertrags über die Europäische Union (EUV), der in Bereichen, in denen es keine ausschließliche Zuständigkeit gibt, geteilte Zuständigkeit vorsieht.*

> Nach dem Subsidiaritätsprinzip wird die Union in den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten weder auf zentraler noch auf regionaler oder lokaler Ebene ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind. (TEU Art 5.3)

Die EU (und im weiteren Sinne die ENISA) sollten daher ausschließlich für Probleme zuständig sein, die von einzelnen Mitgliedstaaten nicht gelöst werden können. Aus diesem Grund hat jeder Mitgliedstaat neben dieser europäischen Agentur seinen eigenen institutionellen Rahmen und eigene Stellen für Cybersicherheit eingerichtet. Es ist Aufgabe der ENISA, die Mitgliedstaaten und die Kommission zu unterstützen und die Zusammenarbeit und den Informationsaustausch zu erleichtern.

Koordination auf europäischer Ebene

Unter den Vorschriften ist derzeit die NIS-Richtlinie die Referenz für Cybersicherheit in Europa, aber es wird bereits über einen aktualisierten Text diskutiert, der zur Verabschiedung von NIS 2 führen dürfte.

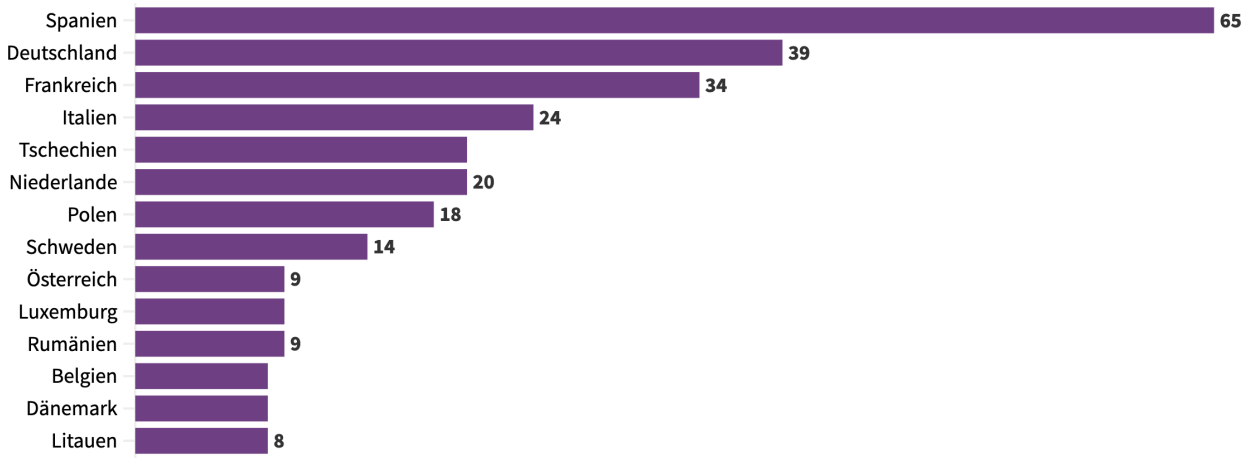
Aufgrund der Art der EU-Richtlinien (Artikel 288 des Vertrags über die Arbeitsweise der Europäischen Union, AEUV) beschränkt sich der Text darauf, die Mitgliedstaaten über die gewünschten Ergebnisse zu informieren und lässt ihnen viel Freiraum zur Strukturierung ihrer eigenen Agenturen für Cybersicherheit.

Zu den Verpflichtungen der Mitgliedstaaten zählt die Identifizierung spezifischer Agenturen, die die verabschiedeten Politiken koordinieren können, um ein hohes Niveau an Cybersicherheit zu gewährleisten. Hierbei handelt es sich um die zuständigen nationalen Agenturen, die zentralen Anlaufstellen und die CSIRTs (Computer-Notfallteams).

Letztere wurden bereits im Jahr 1990 eingerichtet. Es handelt sich um Strukturen, die dafür zuständig sind, Berichte über Zwischenfälle und potenzielle Schwachstellen von Software zu sammeln und zu verwalten. Die Zahl der CSIRTs unterscheidet sich von einem Land zum anderen, und sie können von unterschiedlichen internationalen Stellen wie Trusted Introducer, First (Forum of Incident Response and Security Teams) und dem europäischen CSIRT Network anerkannt sein.

Die 15 EU-Länder mit den meisten CSIRTs

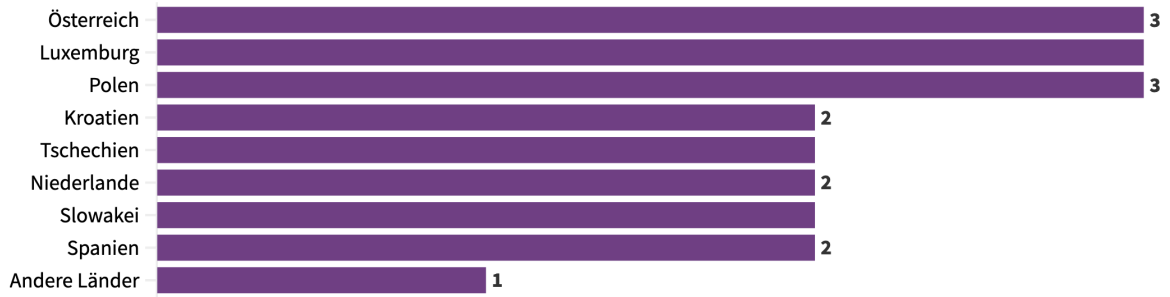
Die europäischen Länder, die über die meisten von den drei wichtigsten internationalen Stellen anerkannten Computer-Notfallteams (CSIRTs) verfügen



The NIS Directive obliges each member state to designate one or more CSIRT to join the European CSIRT Network. In most cases member states have designated a single CSIRT, but not all; in fact, some countries have designated two or three.

Von den Mitgliedstaaten benannte nationale CSIRTs

Zahl der von den einzelnen Mitgliedstaaten der Europäischen Union im Rahmen des CSIRTs-Netzwerks benannten nationalen CSIRTs



Während die CSIRTs für IT-Notfälle und potenzielle Schwachstellen zuständig sind, nehmen die im Rahmen von NIS zuständigen Behörden Aufgaben im Zusammenhang mit Regulation und Verwaltung wahr. Bei diesen Behörden handelt es sich um die Stellen, die für die Sicherheit von Netzwerken und Informationssystemen in den in der Richtlinie aufgeführten Sektoren zuständig sind. Auch hier kann jeder Mitgliedstaat eine oder mehrere Behörden benennen.

13 Länder haben eine einzige Behörde benannt, die für NIS zuständig ist.

Wenn nur eine Behörde benannt wurde, wird diese automatisch zum einzigen Kontakt. Andernfalls muss der Mitgliedstaat mitteilen, welche Behörde diese Rolle übernimmt, um die Zusammenarbeit mit den Behörden anderer Mitgliedstaaten sowie mit der ENISA und dem CSIRT-Netzwerk zu gewährleisten.

Im Rahmen von NIS zuständige Behörden – die Situation in Deutschland, Frankreich und Italien

Wie bereits erwähnt verfügt jedes Land über das Recht, in seinem Ermessen seine eigenen zuständigen Stellen zu strukturieren, solange es dabei die Vorgaben der EU-Richtlinie einhält. Betrachtet man die drei bevölkerungsreichsten EU-Länder als Beispiele, ist als erstes festzustellen, dass alle drei bisher eine einzige Behörde benannt haben, um die Aufgaben im Zusammenhang mit NIS wahrzunehmen.

In Italien handelt es sich um die neue Cybersicherheitsbehörde Agenzia per la Cybersicurezza nationale. Vor ihrer Gründung im Mai 2021 gab es fünf zuständige Behörden: die Ministerien für wirtschaftliche Entwicklung, Infrastruktur, Wirtschaft, Gesundheit und Umwelt, die jetzt „sektorspezifische Behörden“ sind (Artikel 7 der Gesetzesverordnung 65/2018). Die Cybersicherheitsbehörde ist daher der einzige Kontakt und umfasst auch das italienische CSIRT, das zuvor zum Ressort für Information für die Sicherheit der Republik gehörte (und damit unter den Geheimdienst fiel).

Wie wir in anderen Artikeln erklärt haben, ist die Cybersicherheitsbehörde in vieler Hinsicht autonom. Sie untersteht jedoch der Kontrolle der/des Ministerpräsident*in, die/der die Verwaltung des Sektors sowie die Ernennung des Direktors (Roberto Baldoni) und der Vizedirektorin (Nunzia Ciardi) überwacht. Intern ist diese Agentur in acht Abteilungen unterteilt, die wiederum aus Fachbereichen bestehen. Derzeit soll sie maximal etwa 300 Mitarbeitende beschäftigen und ihr Haushalt für das Jahr 2022 beträgt 41 Millionen Euro. In den nächsten Jahren wird jedoch eine deutliche Erhöhung der Ressourcen erwartet.

> Ab 2026 soll der italienischen Cybersicherheitsbehörde ein Budget von 122 Millionen Euro zur Verfügung stehen.

In Frankreich ist die zuständige Stelle die Agence nationale de la sécurité des systèmes d'information (ANSSI). Wie in Italien ist sie der/dem Ministerpräsident*in untergeordnet. Die französische Behörde untersteht dem Secrétariat général de la défense, einer Stelle, die die/den Ministerpräsident*in bei der Wahrnehmung ihrer/seiner Aufgabe im Zusammenhang mit der Verteidigung und nationalen Sicherheit unterstützt. Die ANSSI wurde im Jahr 2009 per Gesetz gegründet und setzte sich umgehend ehrgeizige Ziele; sie beabsichtigte unter anderem, eine der weltweit führenden Stellen für Cybersicherheit zu werden. Die jüngste Version der französischen Cybersicherheitsstrategie enthält diesen Wortlaut jedoch nicht länger.

Die ANSSI wird von einer Generaldirektion geleitet, die sich aus dem Generaldirektor Guillaume Poupard, dem stellvertretenden Generaldirektor und der Stabschefin zusammensetzt. Der Generaldirektion sind vier Unterdirektionen untergeordnet, die jeweils aus Abteilungen bestehen. Im Jahr 2020 belief sich das Budget der ANSSI (ohne Personalkosten) auf 21 Millionen Euro und die Agentur beschäftigte mehr als 500 Beamt*innen und 100 Nachwuchskräfte.

> Das Budget der ANSSI betrug im Jahr 2020 ohne Personalkosten 21 Millionen Euro.

Auch in Deutschland gibt es eine einzige zuständige Behörde, das Bundesamt für Sicherheit in der Informationstechnik (BSI). Im Gegensatz zu Frankreich und Italien untersteht diese Behörde nicht dem/der Ministerpräsident*in (in diesem Fall dem/der Bundeskanzler*in), sondern ist im Geschäftsbereich der Generaldirektion für Cyber- und Informationssicherheit des Bundesministeriums des Innern angesiedelt. Das Amt wurde bereits im Jahr 1991 gegründet, aber heute werden seine Aufgaben hauptsächlich durch ein Gesetz von 2009 geregelt. Im weiteren Verlauf wurden zusätzliche Bestimmungen verabschiedet, davon eine im Jahr 2015, die viele Elemente der im folgenden Jahr veröffentlichten EU-Richtlinie antizipierte, und eine weitere erst vor wenigen Monaten. Mit dem jüngsten Gesetz beabsichtigt die Bundesregierung, das BSI weiter zu stärken, insbesondere in Bezug auf Verbraucherschutz, Sicherheit für Unternehmen und Mobilfunknetze.

An der Spitze des BSI stehen dessen Präsident Arne Schönbohm und der Vizepräsident. Das Amt ist intern in acht Abteilungen unterteilt, die wiederum 18 Fachbereiche und mehrere Referate umfassen. Sein Haushalt für 2021 betrug etwa 200 Millionen Euro, und das Amt beschäftigte 1550 Mitarbeitende.

> Im Jahr 2021 betrug der Haushalt des Bundesamts für Sicherheit in der Informationstechnik 200 Millionen Euro

Die Informationen über Budgets und Mitarbeitendenzahlen dieser Einrichtungen sind zwar interessant, aber schwer zu vergleichen. Das liegt nicht nur an den unterschiedlichen Quellen, aus denen die Daten stammen, und den abweichenden Methoden, die zur Datenerhebung verwendet wurden, sondern auch daran, dass für Cybersicherheit in keinem Land eine Organisation allein verantwortlich ist. In diesem Bereich spielen verschiedene Strukturen wie Ministerien, Verteidigung und Geheimdienst wichtige Rollen, weshalb es sehr schwierig ist, den Aufwand für Cybersicherheit der einzelnen Länder zu beurteilen.

Die Beziehung zwischen Verteidigungssektor und Geheimdienst

Wie bereits erwähnt, war vor der Gründung der italienischen Cybersicherheitsbehörde das Ressort für Information für die Sicherheit der Republik (DIS) für deren Aufgaben zuständig. Das neue Gesetz siedelt diese Agentur jedoch außerhalb des Geheimdienstes an, obwohl sie über viele Verbindungen zu diesem verfügt. Die/der für den Geheimdienst zuständige Untersekretär*in der Regierung erhielt inzwischen per Gesetz im Zusammenhang mit Cybersicherheit dieselbe Aufgabe wie die Cybersicherheitsbehörde. Die Koordination mit dem Geheimdienst erfolgt darüber hinaus durch die Präsenz von Geheimdienstvertretenden im Bereich Cybersicherheit, an dem darüber hinaus Beauftragte verschiedener Ministerien beteiligt sind. Unter anderem ist die Präsenz einer/eines Vertreter*in des Verteidigungsministeriums geplant, was wohl die Verbindung zwischen der Behörde und der Organisation für Cyberoperationen (COR) – der für Cybersicherheit zuständigen Stelle unter

dem Kommando der/des Generalstabschef*in – garantiert. In den bisher veröffentlichten Regeln gibt es allerdings keine ausdrückliche Verbindung zwischen der Behörde und der COR.

Das Bundesamt für Sicherheit in der Informationstechnik ist ebenfalls aus dem Geheimdienst entstanden und war Anfang der 1990er Jahre zunächst eine für den technologischen Schutz von Staatsgeheimnissen zuständige Stelle. Im Laufe der Jahre wurde das BSI jedoch völlig autonom. Über das Nationale Cyber-Abwehrzentrum, eine behörden- und institutionenübergreifende Plattform aus verschiedenen Strukturen des Bundes, für die Cybersicherheit relevant ist, bestehen weiterhin Beziehungen zum Geheimdienst. Diese Plattform pflegt auch Beziehungen zur Armee, die in Deutschland auf diesem Gebiet eine wichtige Rolle spielt, denn die Cyber-Abwehr obliegt laut Verfassung der Bundeswehr. Im Jahr 2017 wurde das Kommando Cyber -und Informationsraum (CIR) gegründet, eine Stelle, die als gleichwertig mit den anderen Kommandos der Bundeswehr gilt und für die Sicherheit der Cyber-Abwehr-Infrastruktur und der Waffensysteme verantwortlich ist. Aufgrund der engen Beziehung zwischen Verteidigung und Cybersicherheit unterstützt das CIR bei Bedarf das BSI. Die strengen Einschränkungen, die der Bundeswehr durch die Verfassung auferlegt werden, erlauben es dieser jedoch nur, „Amtshilfe“ zu leisten. Sollte es erforderlich sein, zur Abwehr einer landesweiten Cyberattacke Militärpersonal einzusetzen, schreibt die Verfassung die vorherige Genehmigung durch den Bundestag vor.

Wie vorstehend dargelegt, gehört in Frankreich die ANSSI zum Secrétariat général de la défense. Diese Struktur garantiert die Koordination mit Armee und Geheimdienst. Das Secrétariat général de la défense verfügt in der Tat über verschiedene Zuständigkeiten in den Bereichen Verteidigung und Geheimdienst und übernimmt für die/den Präsident*in des Ministerrats die Leitung, das Vorschlagen, die Koordination und Regulierung allgemeiner Angelegenheiten im Zusammenhang mit Verteidigung und nationaler Sicherheit. Darüber hinaus haben wir gesehen, dass das Secrétariat général de la défense der/dem Präsident*in des Ministerrats gegenüber rechenschaftspflichtig ist. Der Ministerrat ist wiederum auch für die Aktivitäten des inländischen Geheimdienstes und der ausländischen Geheimdienste verantwortlich, obwohl diese jeweils in den Zuständigkeitsbereich des Innen- bzw. des Verteidigungsministeriums fallen.

Links:

Data protection in EU: Comparative Study of National Reports. Lesen

Cyber defence in Nato countries: comparing models. Lesen

Russland möchte deine Daten haben: die Cyberangriffe in der Europäischen Union nehmen zu

Abstract: Der Schatten Russlands schwebte immer schon über den sozialen Netzwerken, aber die Pandemie, die das Leben der Bürger ins Netz verlagert hat, hat die Sicherheitslücken der Unternehmen und Europäischen Institutionen. Es ist deshalb auch keine Überraschung, dass die Cyberangriffe auf kritische Sektoren in Europa sich im Jahr 2020 verdoppelt hat. Und obwohl Brüssel

daran arbeitet, diese Lücken zu schließen, droht die Invasion in der Ukraine den Cyberkrieg noch zu verstärken.

Author: Álvaro Merino (El Orden Mundial)

Link: https://www.europeandatajournalism.eu/eng/About/Other-projects/Panelfit/Panelfit-news/Russia-wants-your-data-cyber-attacks-are-growing-in-the-European-Union

Text:

Am 14. März 2021 wartete Donna-Maria Cullen auf ihren Termin bei der Radiologie, um einen aggressiven Hirntumor zu bekämpfen, als sie einen unerwarteten Anruf erhielt : ein Cyberangriff hatte das Internetsystem des irischen Gesundheitswesens lahmgelegt und ihre Behandlung musste vorübergehend ausgesetzt werden.
Nach einem Jahr intensiven Kampfes gegen das Coronavirus, ist das irische Gesundheitssystem zusammengebrochen, allerdings weder aufgrund der vielen Ansteckungen, noch durch das Chaos der Ausgangssperren, wie man vielleicht erwarten könnte, sondern durch einen unsichtbaren Angriff aus mehreren Hundert Kilometer Entfernung.

Spätere Ermittlungen haben ergeben, dass der Auslöser eine Ransomware (Lösegeld-Trojaner) war oder eine unberechtigte Kenntnisnahme von Daten (Bit-Napping) ausgeführt von Wizard Spider , einer Cybercrime-Bande mit Sitz im russischen Sankt Petersburg, die 14 Millionen Pfund, ca. 17 Millionen Euro, für die Beendigung des Angriffs forderten. Die irischen Behörden versuchten, den Angriff abzuwehren, was die Aussetzung von vielen Tausend Terminen über Monate zur Folge hatte, die Rückkehr zu Papier und Stift in den Gesundheitszentren, eine Filtrierung von vertraulichen medizinischen Informationen von 520 Patienten und Ausgaben in einer Größenordung von ungefähr 100 Millionen Euro.

Dieser Fall ist bei weitem kein Einzelfall, der Angriff auf das irische Gesundheitssystem reiht sich ein in eine Lawine von Cyberangriffen mit dem Ziel, europäische Unternehmen und die EU-Institutionen zu treffen. Russlands Schatten lag immer schon über den sozialen Netzwerken, aber durch die Pandemie haben sich Anzahl und Ausmaß dieser Angriffe immer weiter potenziert.

Die Angriffe durch Malware auf kritische Sektoren in Europa haben sich im Jahr 2020 verdoppelt – 304 Angriffe gegenüber 146 im Jahr 2019 – laut der Europäischen Agentur für Cybersicherheit (Enisa). Die Cyberangriffe auf Krankenhäuser und Gesundheitsnetzwerke sind ebenfalls um 47% gestiegen.

Die neue Normalität – ein fruchtbares Feld für die Cyberkriminellen

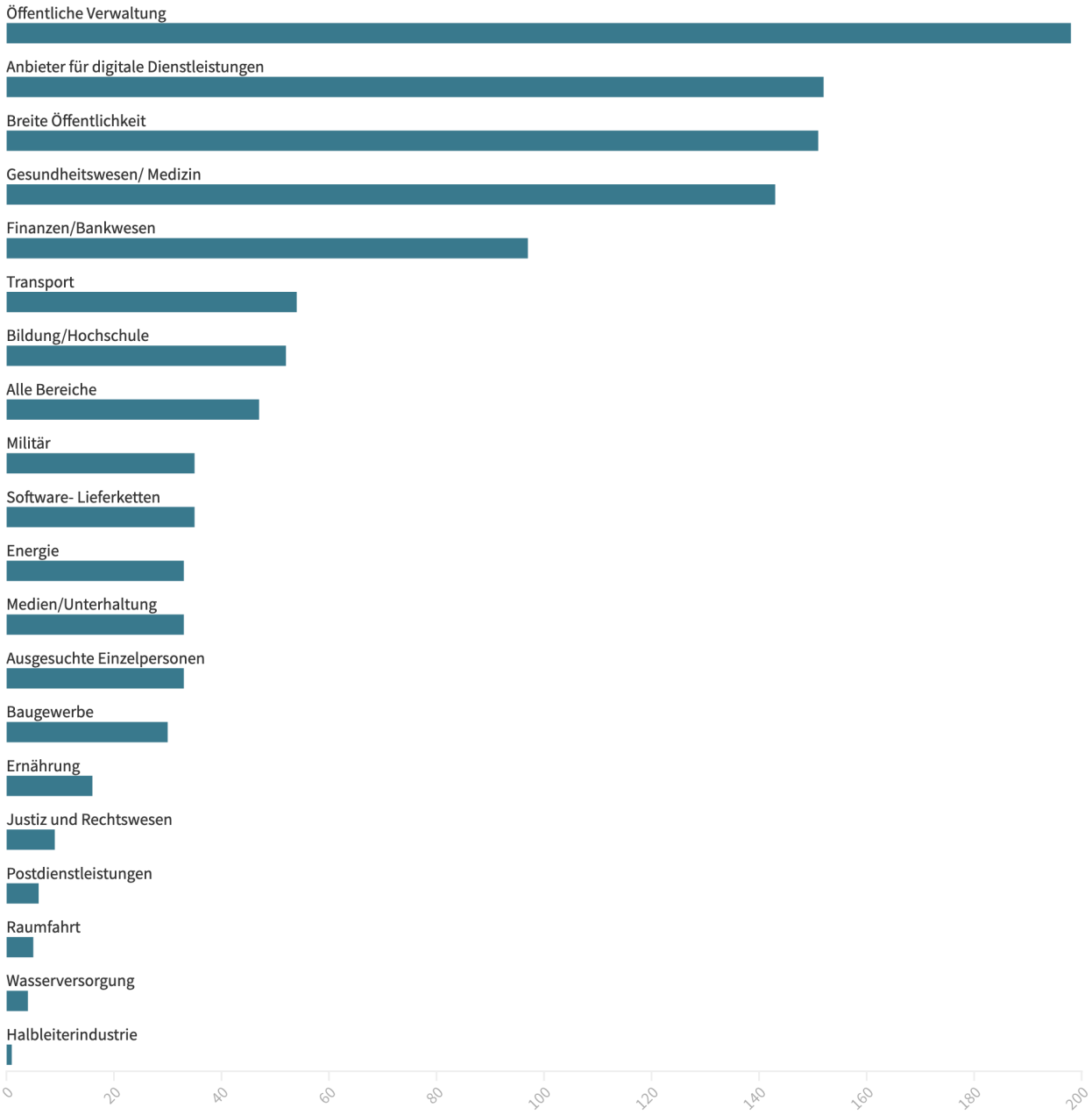
Nachdem die WHO den Pandemiezustand ausgerufen hatte und die Ansteckungen mit dem Coronavirus innerhalb weniger Tage außer Kontrolle gerieten, verlagerte sich das Leben der Europäer ins Internet. Mit einem Mal wurden Homeoffice, Onlineshopping und das Sozialleben vor dem Bildschirm zur Routine. Und obwohl es diese digitalen Lösungen einen kompletten Stillstand der Welt verhinderten und ein Teil des wirtschaftlichen Lebens aufrecht erhalten werden konnte, boten sie der Internetkriminalität gleichzeitig eine goldene Gelegenheit.

Nicht nur das Coronavirus, auch der Wechsel von den traditionellen Infrastrukturen hin zu Cloud-basierten Plattformen, die wachsende Interkonnektivität und das Aufkommen neuer Technologien wie der künstlichen Intelligenz, haben zu einem Anstieg der Cyberangriffe geführt, was „die Kompliziertheit, die Komplexität und die Auswirkungen betrifft“, so die Europäische Agentur für

Cybersicherheit Enisa. In ihrem Bericht aus dem Jahr 2021 verkündete die Agentur, dass „diese Tendenz (die Beschleunigung der digitalen Transformation) die Angriffsfläche für Cyberanschläge noch vergrößert habe und wir als Ergebnis gesehen haben, dass die Anzahl der Internetangriffe auf Organisationen und Unternehmen über die Büroinfrastruktur zugenommen hat“.

Sektoren im Fokus

Cybersicherheitsangriffe, die die Europäische Agentur für Cybersicherheit (Enisa) zwischen April 2020 und Juli 2021 beobachtet hat



Quelle: Enisa Threat Landscape 2021 • Álvaro Merino

Darüber hinaus haben sich die öffentliche Verwaltung, die Lieferketten – die Kaskadenreaktionen auslösen können – und die Gesundheitssysteme seit dem Ausbruch der Pandemie zu bevorzugten Sektoren für die Cyberkriminellen entwickelt. Eine Einrichtung, die einen Angriff dieser Art erfuhr,

war das Universitätskrankenhaus Brünn in Teschechien , welches im März 2020 sogar seine digitale Infrastruktur zu schließen musste, mit der Folge, dass dringende Operationen verschoben werden mussten und Patienten mit schwersten Erkrankungen verlegt werden mussten. Sogar die Europäischen Institutionen selbst wurden im März 2021 zur Zielscheibe eines Cyberangriffes , wobei es keine offensichtliche Sicherheitslücke gegeben hat.

Russland, die permanente Bedrohung

Die Tatsache, dass diese Art von Angriffen anonym erfolgen, macht es sehr schwer, den Feind zu identifizieren und angemessen zu reagieren. Das gilt umso mehr in einem Kontext, wo sich hinter den nicht-staatlichen Gruppen offenbar Staatslenker verbergen, die sich nicht scheuen, diese Art von Angriffen öffentlich anzuprangern.

Obschon es kompliziert ist, die Cyberkapazität eines jeden Landes präzise zu benennen, gibt es international keinen Zweifel daran, dass Russland einer der prominentesten Akteure ist . Auf diese Weise kann Moskau das Internet benutzen, um seine geopolitischen Aspirationen zu verstärken: von der Stärkung seiner Rolle als globale Macht, über die Konsolidierung der Kontrolle über sein Einflussgebiet, bis hin zur Schwächung und Destabilisierung von Organisationen, die es als feindlich einstuft, so wie die EU oder die NATO.

Dafür lassen sich leicht hunderte Beispiele anführen: Deutschland, Italien, Niederlande und Dänemark haben in den letzten Jahren immer wieder gesagt , sie seinen Opfer russischer Cyberangriffe geworden; Frankreich teilte zu Beginn des Jahres 2021 mit, dass einige seiner Großunternehmen, unter anderem Airbus und Orange, zur Zielscheibe von Hackerangriffen mit Verbindungen nach Russland geworden seien; und vergangen September beschuldigte Josep Borrell , der Hohe Vertreter der EU für Außenpolitik Moskau, in die Computersysteme zahlreicher europäischer Politiker, ranghoher Manager von Energieunternehmen und weiterer Bürger mit einer gewissen sozialen Sichtbarkeit eingedrungen zu sein.

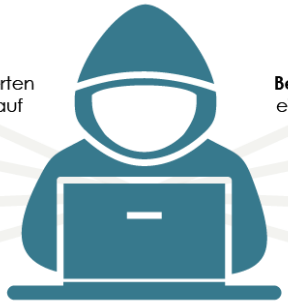
Neben dem Zugang zu sensiblen Daten, suchen die russischen Computerkriminellen

persönliche Informationen von europäischen Bürgern, mit denen sich ein Lösegeld erpressen lässt oder versuchen, das europäische Datenschutzsystem ganz schachmatt zu setzen, was als Beweis für die Verletzlichkeit der europäischen Gesellschaften angeführt wird. Für die Ermittler erweist es sich las sehr schwierig zu beweisen, dass diese Angriffe vom Kreml gedeckt werden, denn bei den meisten Fällen stützen sich die Anschuldigungen auf Indizien, die nicht ausreichend belastbar sind, um von Russland offiziell eine Erklärung zu verlangen.

Cyberkriminalität, eine konstante Bedrohung

Hauptbedrohungen, die von Enisa zwischen 2020 und 2021 benannt wur

1. **Ransomware:** Angreifer verschlüsseln die Daten einer Organisation und fordern Lösegeld für die Wiederherstellung des Zugangs
2. **Malware:** Software soll einen nicht authorisierten Prozess ausführen, der negative Folgen hat auf die Vertraulichkeit, Integrität oder Zugänglichkeit eines Systems
3. **Cryptojacking:** ein Krimineller nutzt insgeheim die Computermacht eines Opfers, um Cryptowährungen zu generieren
4. **Bedrohnungen per E-mail:** eine Vielzahl von Bedrohungen, die stärker die Schwächen der menschlichen Psyche nutzt und in Alltagsroutinen, als die technischen Schwachstellen in der Computerausstattung



5. **Datenbedrohungen:** eine Datenlücke oder Datenleck bei der Weitergabe von sensiblen, vertraulichen oder geschützten Daten an eine nicht vertrauenswürdige Umgebung
6. **Bedrohungen der Verfügbarkeit und Integrität:** eine Vielzahl von Bedrohungen und Angriffen, wovon die Familien Denial of Service (DoS) und Web Angriffe hervorstechen
7. **Falschinformationen:** verbreitet durch die verstärkte Nutzung von Social Media Plattformen und Online-Medien
8. **Nicht-bösartige Bedrohungen:** Bedrohungen, wo die böse Absicht nicht offensichtlich ist, meistens gestützt auf menschliche Fehler und Fehlkonfigurierungen des Systems

Autor:
Álvaro Merino (2022)
Quelle:
Enisa Threat Landscape 2021

EUROPEAN DATA JOURNALISM NETWORK

elordenmundial.com

3. Ungleichgewicht der Macht und Freiheit des Konsenses: Europas digitale Festung

Das Ökosystem der europäischen biometrischen Kontroll- und Überwachungsdaten

Zusammenfassung: Eine Beschreibung der wichtigsten Systeme, die in Europa zur Verwaltung der Mobilität von Personen an den europäischen Grenzen und zwischen den Ländern eingesetzt werden, wobei der Schwerpunkt auf den Aspekten liegt, die an den derzeitigen Mechanismen verbessert werden können.

Autor: Mediterranean Institute for Investigative Reporting (MIIR)

Link: Verfügbar ab dem 26. April 2022

Text:

Die Digitalisierung und Online-Umstellung von immer mehr Aspekten unseres Lebens ist ein langfristiger Trend, der durch die COVID-19-Pandemie beschleunigt wurde. Was jedoch weitgehend unbemerkt bleibt, ist derselbe Trend betreffend der Supermächte in Bezug auf Datenerfassung und Überwachung der EU-Staaten .

Die nationalen Behörden der Mitgliedstaaten, wie Polizei, innere Sicherheitsdienste, Grenzschutz, Einwanderungsbehörden und europäische Einrichtungen wie Europol und Frontex, betreiben groß angelegte Datenerfassungs- und Speicherinfrastrukturen. Unter dem Deckmantel der „nationalen Sicherheit“ wird ein Raum für potenzielle Verletzungen der grundlegenden Menschenrechte geschaffen, und das zu einer Zeit, in der die „militarisierte“ Grenzsicherung bereits zu Gewalt gegen Flüchtlinge, zu Rückschiebungen mit dem Risiko der Rückkehr in unsichere Länder und unmenschliche Bedingungen sowie zu einem alarmierenden Anstieg vermeidbarer Todesfälle geführt hat.

Die Länder schließen die Migrationsrouten – mit der diskriminierenden jüngsten Ausnahme der ukrainischen Flüchtlinge – und zwingen damit Migranten und Flüchtlinge, andere, oft gefährlichere Alternativen zu suchen, und treiben sie in die Arme krimineller Schlepperbanden.

Aber es sind nicht nur physische Mauern, die errichtet werden. Wie das unabhängige Transnationale Institute TNI (Border War Series-Berichte) berichtet, besteht ein wesentlicher Teil der sogenannten „Festung Europa“ aus „virtuellen Mauern“, die Migranten daran hindern sollen, in den Schengen-Raum einzureisen, oder die ihre Bewegungen innerhalb des Raums überwachen. Diese „virtuellen Mauern“ haben viele Formen: von fortschrittlichen Überwachungssystemen, die Migrationsströme überwachen und die Bewegungen von Menschen an (und manchmal auch vor) den Außengrenzen verfolgen, bis hin zu „intelligenten“, interoperablen KI-Datenbanken, die darauf abzielen, Migranten an und innerhalb der Grenzen zu identifizieren, zu erfassen und zu profilieren.

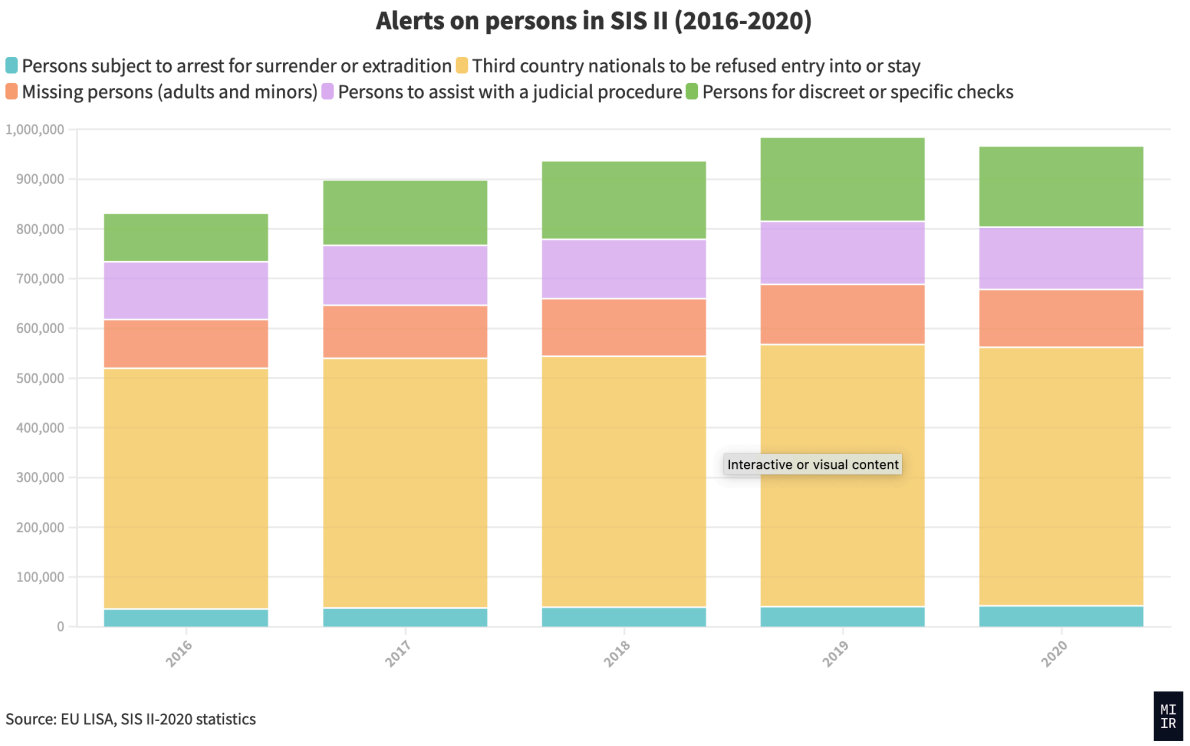
Der gemeinsame Nenner von physischen und virtuellen Mauern ist die soziale Konstruktion des „Menschen auf der Flucht“ als potenzielle Bedrohung für die EU und ihre Mitgliedstaaten. Menschen, die versuchen, die EU zu erreichen und zu betreten, die vor Katastrophen, Gewalt, Krieg oder politischer Verfolgung fliehen, gelten als Risikofaktoren, die bewertet und kategorisiert werden müssen.

Das journalistische Team des MIIR hat im Rahmen des Panelfit-Projekts (Participatory Approaches to a New Ethical and Legal Framework for ICT) die verschiedenen Datenerfassungs- und Überwachungssysteme der EU geprüft sowie ihre Gesetzgebung und die in den verschiedenen Datenbanken gesammelten Daten untersucht, um auf der Grundlage zahlreicher Interviews mit Fachleuten, Forschern, Aktivisten, Anwälten, NROs und Migranten die Risiken für die Menschenrechte zu ermitteln, die auch durch die Interoperabilität dieser Systeme entstehen. Im ersten Teil der Untersuchung geben wir einen kurzen Überblick über die wichtigsten Überwachungssysteme.

Beschreibung der Erfassungssysteme und Personendatenbanken

1. Schengener Informationssystem SIS-II

Die älteste Datenbank. Ihr Zweck ist die Überwachung der Bewegungen von Drittstaatsangehörigen im Schengen-Raum. Sie wurde ursprünglich 1995 eingerichtet und 2013 in ihrer zweiten Generation aktualisiert. In den folgenden Monaten werden die 2018 aufgenommenen Bestimmungen in Kraft treten. Es ist das größte IT-System in Europa und wird in 26 EU-Mitgliedstaaten (Zypern ist nicht dabei, wird aber voraussichtlich beitreten) sowie in der Schweiz, Norwegen, Liechtenstein und Island betrieben. Im Rahmen der SIS-II-Verordnungen werden Daten (Namen, Vornamen, Geburtsdaten und andere alphanumerische Informationen) von Drittstaatsangehörigen, die Gegenstand von Rückführungsentscheidungen sind, Daten über die Verweigerung der Einreise oder des Aufenthalts von Personen im Schengen-Raum sowie Gegenstände (z. B. Autos, Waffen, verlorene Dokumente, Pässe usw.) erfasst und zum Zwecke der polizeilichen und justiziellen Zusammenarbeit verarbeitet. Die Bestimmungen der SIS-II-Verordnung ermöglichen die Anwendung der biometrischen Identifizierung von Personen auf der Grundlage der Gesichtserkennungstechnologie. Sie wird sowohl von den Polizeibehörden als auch von den Einwanderungs- und Asylbehörden verwendet. Wenn eine Person einen Asylantrag stellt, können die Behörden das SIS abfragen, um festzustellen, ob die Person ausgeschrieben ist. Ausgeschrieben werden können Personen, die zur Festnahme oder Überprüfung gesucht werden, Personen, die von den Strafverfolgungsbehörden überwacht werden, Personen, die nicht das Recht haben, in die EU einzureisen oder sich dort aufzuhalten, Personen, die im Rahmen der Rechtshilfe gesucht werden, sowie vermisste Personen (Erwachsene und Kinder).



Das SIS II-System hat 2019 mit 18 Millionen Abfragen pro Tag durch alle zugriffsberechtigten zuständigen Behörden einen Rekord aufgestellt. Diese Zahl ist dreimal so hoch wie die Zahl der Abfragen im Jahr 2014 (6 Millionen Abfragen pro Tag). Bezeichnend für die weit verbreitete Nutzung ist die Einführung des Automatisierten Fingerabdruck-Identifizierungssystems (AFIS) Ende 2020, das Abfragen nach Staaten und über Fingerabdrücke ermöglicht sowie eine automatische Überprüfung und einen Abgleich mit bestehenden Abfragen einführt.

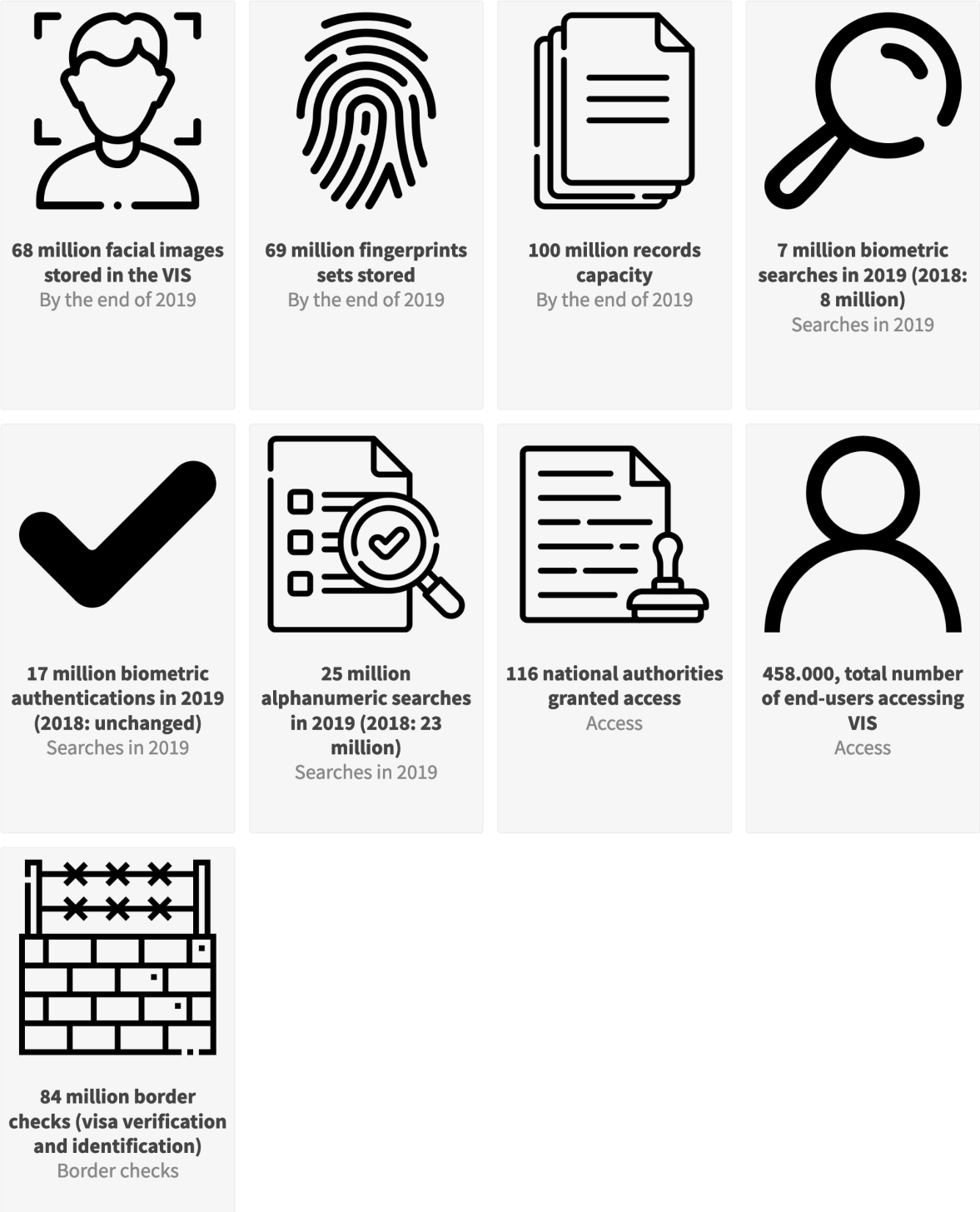
Bezeichnend für die gezielte erweiterte Nutzung des Systems zur Identifizierung von Migranten ohne Papiere ist jedoch, dass von den 964.720 Ausschreibungen im SIS II im Jahr 2020 mehr als die Hälfte Drittstaatsangehörige betrafen, denen die Einreise und der Aufenthalt im Schengen-Raum verweigert worden waren. Dies war über die Jahre hinweg durchgängig der Fall, wie die Tabelle der Ausschreibungen 2016–2020 zeigt.

2. VIS – Visa-Informationssystem

Dieses System wurde ab 2011 schrittweise eingeführt und seine Entwicklung 2016 abgeschlossen. Das System wird von den 30 Schengen-Staaten zusammen mit Bulgarien, Kroatien, Zypern und Rumänien genutzt. Es soll es diesen Ländern ermöglichen, Daten über Visa für kurzfristige Aufenthalte auszutauschen und die Visakontrolle an den Grenzübergängen zu erleichtern. Die zuständigen Asylbehörden können auf das VIS zugreifen. Im Jahr 2018 legte die Europäische Kommission einen Vorschlag zur Überarbeitung des VIS vor, um dessen Anwendungsbereich zu

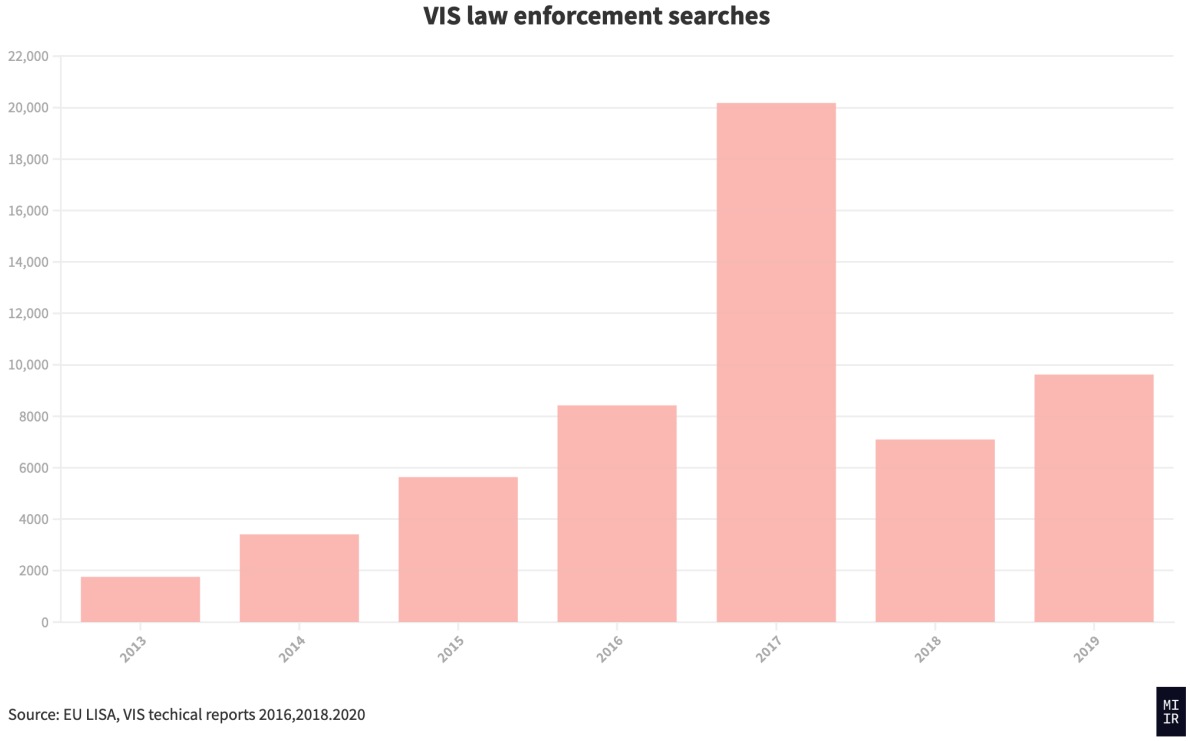
erweitern. Die vorgeschlagenen Regeln legen nahe, dass das VIS auch Daten über Visa für den längerfristigen Aufenthalt enthalten sollte.

VIS: Use of biometrics, searches and access



Das System speichert Fingerabdrücke und ein Foto der Visumantragsteller/-inhaber sowie die in den Anträgen enthaltenen personenbezogenen Daten wie Nachname, Wohnanschrift, Informationen über den Visastatus und Bankdaten (Nachweis der Einzahlung). „Ohne diese Daten wird das Visum nicht erteilt. Dies ist implizit eine Klassendiskriminierung: Wenn man reich ist, kann man reisen, wenn man kein Geld hat, wird kein Visum erteilt („Lowtech-Diskriminierung"). Der einzuzahlende Betrag hängt von den einzelnen Mitgliedstaaten ab", sagt der Forscher Georgios Glouftios.

Die automatisierte biometrische Identifizierung wird im VIS bereits auf der Grundlage der erfassten Fingerabdrücke eingesetzt. 2019 wurden 7 Millionen biometrische Abfragen und 17 Millionen biometrische Identitätskontrollen durchgeführt, letztere hauptsächlich an Grenzstationen. An den Flughäfen überprüfen die Behörden die Fingerabdrücke von Drittstaatsangehörigen, die nach Europa reisen, um sicherzustellen, dass sie mit den Fingerabdrücken übereinstimmen, die in ihrer individuellen Datei im VIS-System gespeichert sind und die vor der Reise eingerichtet werden muss. Die Polizeibehörden können das VIS abfragen, um festzustellen, ob eine Person, die zuvor ein Visum beantragt hat, in kriminelle Aktivitäten verwickelt ist. Das System kann auch von Asylbehörden genutzt werden.



Ein weiteres Element, das die Bedenken der Bürger und Organisationen hinsichtlich des Schutzes der Privatsphäre in Bezug auf diese Systeme noch verstärkt, ist der erweiterte Zugang von Behörden und Personen aller Dienststellen. Es mag stimmen, dass die Behörden in jedem Land, die zum Zugriff auf die Datenbank berechtigt sind, jedes Jahr im EU-Journal veröffentlicht werden. Dies allein reicht jedoch nicht aus, da die Zahl der Endnutzer, die Zugang zu den personenbezogenen Daten des Einzelnen haben können, ungewiss ist. Im VIS-System sind beispielsweise insgesamt 116 nationale Dienststellen und Behörden, einschließlich Strafverfolgungsbehörden, berechtigt, Daten zu erstellen,

zu ändern und zu löschen – und die Zahl der Endnutzer erreicht die astronomische Zahl von 458.000 Mitarbeitern, die alle Zugang zu diesen sensiblen personenbezogenen Daten haben.

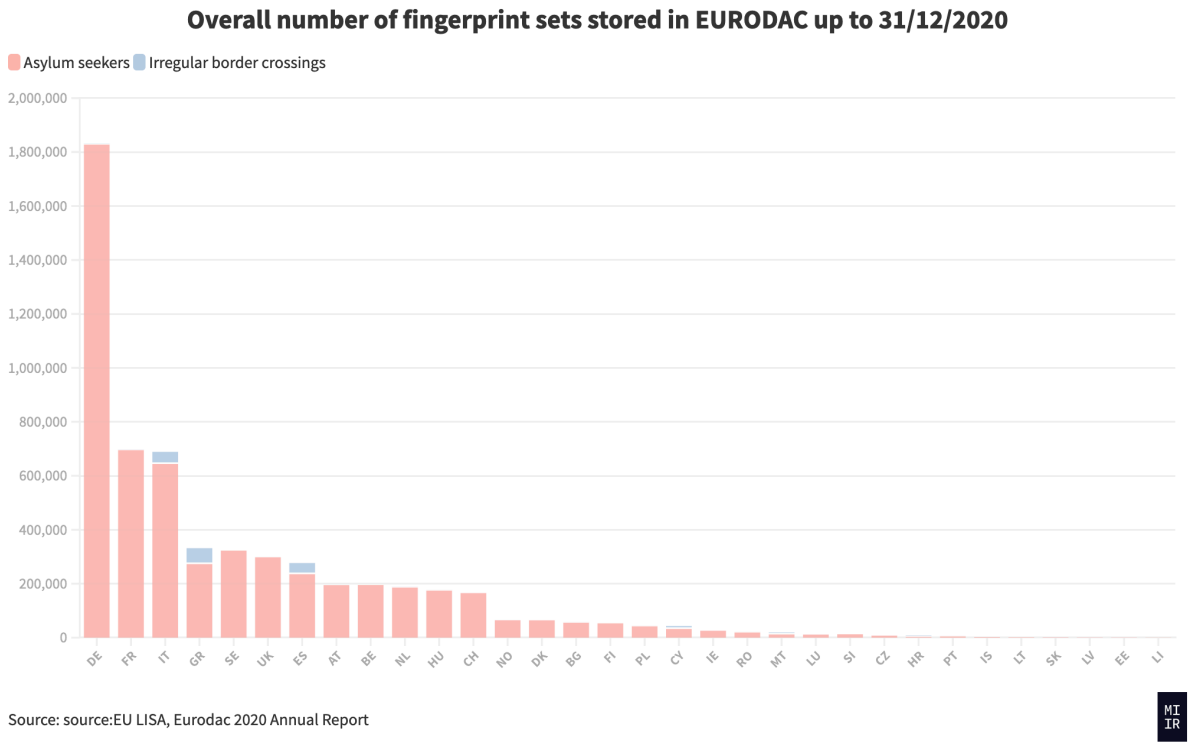
3.Eurodac

Das Europäische System für den Vergleich von Fingerabdrücken von Asylbewerbern (EURODAC) wurde 2003 in Betrieb genommen und war das erste IT-System, das die Speicherung von Fingerabdrücken in einer Datenbank auf EU-Ebene ermöglichte. Ziel des Systems war es, den EU-Ländern die Bestimmung der Zuständigkeit für die Prüfung eines Asylantrags zu erleichtern, indem die Fingerabdrücke von Asylbewerbern und Drittstaatsangehörigen/Nicht-EWR-Bürgern mit einer zentralen Datenbank verglichen werden. Außerdem sollten die Strafverfolgungsbehörden in die Lage versetzt werden, Eurodac unter strengen Auflagen zur Ermittlung, Aufdeckung und Verhütung von terroristischen oder schweren Straftaten zu durchsuchen. Bislang werden nur biometrische Merkmale und nicht einmal der Name einer Person gespeichert. Wenn ein Asylbewerber oder ein Drittstaatsangehöriger/Nicht-EWR-Bürger illegal in einem EU-Land angetroffen wird, kann das EU-Land Eurodac konsultieren, um festzustellen, ob die Person zuvor in einem EU-Land einen Asylantrag gestellt hat oder bereits beim Versuch, illegal in die EU einzureisen, festgenommen wurde.

EURODAC wird derzeit überarbeitet. Die vorgeschlagenen Überarbeitungen sehen die Interaktion von EURODAC mit anderen IT-Systemen der EU in Asyl-, Rückführungs- und Neuansiedlungsverfahren vor. In diesem Zusammenhang wird EURODAC unter anderem für die Kontrolle der Migrationsströme und die Aufdeckung von Sekundärbewegungen unrechtmäßiger Drittstaatsangehöriger eingesetzt werden.

Die Zahlen zeigen jedoch, dass die Erfassung und Speicherung von Fingerabdrücken von Drittstaatsangehörigen oder Staatenlosen ebenfalls gängige Praxis ist. So übermittelten die Mitgliedstaaten im Jahr 2020 insgesamt 644.926 Fingerabdruckdatensätze an EURODAC. 62 % dieser Fingerabdruckdatensätze entsprechen Personen, die internationalen Schutz beantragt haben, 25 % sind Fingerabdrücke von Drittstaatsangehörigen oder Staatenlosen, die sich illegal in einem Mitgliedstaat aufhalten, und 13 % sind Fingerabdrücke der gleichen Gruppen, die illegal die Außengrenze überschreiten.

Der neue Vorschlag würde im Falle der Annahme die Erfassung und Speicherung der Fingerabdrücke von Drittstaatsangehörigen oder Staatenlosen, die sich illegal in Europa aufhalten, verbindlich vorschreiben. Darüber hinaus wird der Umfang der erfassten personenbezogenen Daten radikal erhöht. Die vorgeschlagenen Bestimmungen werden die Erfassung einer Vielzahl biografischer und biometrischer Informationen zusätzlich zu den bereits erfassten Daten ermöglichen, wie z. B. Bilder von Personen, Namen, Geburtsdatum und -ort sowie Staatsangehörigkeit.



Die fast 6 Millionen Fingerabdrücke, die Ende 2020 in EURODAC gespeichert sein werden, stammen nicht nur von Asylbewerbern, sondern auch von Migranten, die von den Aufnahmestaaten als „unrechtmäßige Grenzgänger“ eingestuft werden und die keinen Anspruch auf Zugang zu Asylverfahren haben. Am 31.12.2020, als die Registrierung erfolgte, waren es nur knapp 155.000 (3 %), aber die Fingerabdrücke dieser Kategorie werden automatisch nach 18 Monaten aus der Datenbank gelöscht, im Gegensatz zu denen von Asylbewerbern, die 10 Jahre lang gespeichert werden. So lag der entsprechende Anteil für sie Ende 2016 bei 13 %. Es sei darauf hingewiesen, dass die EURODAC-Datenbank seit Juli 2015 auch für die Polizeidienste der Länder und Europol zugänglich ist, um Straftaten im Zusammenhang mit Terrorismus und schwerer Kriminalität zu verhindern und zu untersuchen.

Es ist bemerkenswert, dass Deutschland, obwohl es kein Erstaufnahmeland wie Italien und Griechenland ist, dennoch die meisten biometrischen Daten unter den 32 Schengen-Ländern zu sammeln scheint. Dies ist darauf zurückzuführen, dass die große Mehrheit der Migranten, die vor allem mit der Flüchtlingskrise 2015 nach Europa kamen, den ersten Asylantrag in Deutschland und nicht in den Ländern an den Einreisestellen der europäischen Grenzen stellen. Im Ranking der biometrischen Speicherung folgen auf Deutschland Frankreich, Italien, Griechenland, Serbien, das Vereinigte Königreich und Spanien.

Auffällig ist auch, dass Griechenland unter den 32 Ländern der „Spitzenreiter“ bei der Erfassung von Fingerabdrücken von Migranten ist, die keinen Anspruch auf Asyl haben. Dies sind 56.000 (d. h. ein Drittel der Gesamtzahl dieser Kategorie in EURODAC) von insgesamt 331.609 Fingerabdrücken, die Griechenland Ende 2020 registriert hat. Der bemerkenswerte erste Platz Griechenlands hängt mit dem

Prozess der Datenerfassung und dem Screening in griechischen Aufnahmezentren für Migranten zusammen, die ins Land kommen.

Die erste offizielle Phase der Registrierung ist neben der Überprüfung der relevanten Dokumente, die die Person mit sich führt (Reisepass, Personalausweis, andere Dokumente), die Untersuchung/Befragung/Vernehmung durch die griechische Polizei oder FRONTEX-Personal, das sogenannte Screening. „Der Zweck dieses Verfahrens ist es, die Identität der Person zu „kalibrieren", d. h. Daten wie Alter, Nationalität, Herkunftsort, Familienbeziehungen. Es wird in Zusammenarbeit mit FRONTEX-Übersetzern durchgeführt", sagt Vassilis Vlassis, ein Post-Doc-Forscher für Überwachungstechnologien an der Universität für Informatik in Kopenhagen. Er hat eine Feldstudie über Asyl- und Screening-Verfahren in den Aufnahmezentren auf Chios und Lesbos durchgeführt. „In meinen Interviews mit Personen, die im VIAL in Chios als Screener tätig waren, stellte sich heraus, dass viele Daten untersucht werden, darunter Sprache, Aussprache, Rechtschreibung, Kleidung, Schmuck und natürlich auch Handyfotos. Diese Daten werden dann bei der Schlussfolgerung des Screeners berücksichtigt. ‚Ich weiß, dass Syrer Mohamad so und nie so schreiben, während Marokkaner es so, aber nie so schreiben', wurde mir gesagt. Instinkt und Intuition spielen auch eine Rolle. Manchmal hat man, sobald sie durch die Tür kommen, sofort eine Meinung, und dann versucht man, sie zu bestätigen, wie einer der Prüfer erläuterte", erzählt Vlasis. Zusammenfassend lässt sich sagen, dass die Art und Weise, wie diese Daten zustande kommen, multifaktoriell ist und starke performative Elemente aufweist, aber dennoch einen entscheidenden Einfluss auf die Zukunft des Migranten haben kann, der in EURODAC aufgenommen wird. „Der Koordinator der FRONTEX-Mission auf den griechischen Inseln im Jahr 2016 sagte mir selbst: ‚Das Ergebnis des Screenings stellt keine wissenschaftliche Tatsache dar. Es ist eine Arbeitshypothese, das Beste, was wir tun können und womit wir arbeiten'", erzählt Vlassis.

4. EES (europäisches Entry/Exit System)

Das EES wurde 2017 eingerichtet und wird voraussichtlich im Mai 2022 voll einsatzfähig sein. Es sammelt Daten über alle Drittstaatsangehörigen, unabhängig davon, ob sie ein Visum beantragen müssen oder nicht. Es erfasst und speichert das Datum, die Uhrzeit und den Ort der Ein- und Ausreise von Inhabern eines Visums für einen kurzfristigen Aufenthalt sowie von Reisenden, die beim Überschreiten der EU-Grenze von der Visumpflicht befreit sind. Das System soll das Passstempelverfahren ersetzen, indem es die Verarbeitung biometrischer Daten von Personen ermöglicht. Es wird auch die Dauer des Aufenthalts einer Person erfassen und automatische Warnungen bei Überschreitung der Aufenthaltsdauer in einem Land auslösen. Die nationalen Strafverfolgungsbehörden und Europol werden auf diese Datenbank zugreifen können.

5. ETIAS – (Europäisches Reiseinformations- und -genehmigungssystem)

Das ETIAS wurde 2018 eingerichtet und soll bis Dezember 2022 voll einsatzfähig sein. Laut EU-Erklärungen handelt es sich um „ein weitgehend automatisiertes IT-System, das eingerichtet wird, um Sicherheitsrisiken, unrechtmäßige Migration oder hohe epidemische Risiken zu identifizieren, die von

Besuchern ausgehen, die in Schengen-Staaten einreisen und nicht der Visumspflicht unterliegen. [...] Drittstaatsangehörige, die für Reisen in den Schengen-Raum kein Visum benötigen, sollten vor der Reise eine Reisegenehmigung über das ETIAS-System beantragen." Dies ist ein weiteres Beispiel dafür, dass die EU Menschen, die nach Europa reisen wollen, als Risikofaktoren behandelt. Das System wird keine biometrischen Daten speichern. Es werden jedoch verschiedene Datenkategorien erfasst, wie z. B. der Nachname des Antragstellers, seine Staatsangehörigkeit, das Land und die Stadt seines Wohnsitzes, seine Wohnanschrift, seine E-Mail-Adresse und Telefonnummer sowie sein Bildungsstatus (Primar-, Sekundar-, Hochschul- oder kein Bildungsabschluss).

In der Praxis wird das ETIAS-System in etwa so funktionieren wie das ESTA-System in den USA.

6. ECRIS-TCN (Europäisches Strafregisterinformationssystem für Drittstaatsangehörige)

Das 2012 eingerichtete ECRIS ermöglicht den effizienten Austausch von Informationen über strafrechtliche Verurteilungen in der EU zwischen den Mitgliedstaaten. Die meisten der ausgetauschten Informationen betreffen europäische Bürger. Das überarbeitete Europäische Strafregisterinformationssystem wird nun eine zentrale Datenbank mit Informationen über Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) umfassen und soll 2022 betriebsbereit sein. In ECRIS-TCN werden sowohl biografische als auch biometrische Daten von verurteilten Drittstaatsangehörigen, staatenlosen Personen und EU-Bürgern, die Drittstaatsangehörige sind und in einem Mitgliedstaat verurteilt wurden, gespeichert. Diese Daten umfassen Kategorien wie vollständige Namen, Geburtsort und -datum, Staatsangehörigkeit, Geschlecht, Identitätsnummern sowie Fingerabdruckdaten, die im Einklang mit den Rechtsvorschriften des Mitgliedstaats während des Strafverfahrens erhoben wurden. Die Gesichtsbilder verurteilter Personen werden ebenfalls in dem System gespeichert, wenn die Rechtsvorschriften des verurteilenden Mitgliedstaats die Erfassung und Speicherung von Gesichtsbildern verurteilter Personen zulassen. Die Datenbank wird über das Internet zugänglich sein, sodass Behörden werden sie mit einem positiven/negativen Suchmechanismus leicht durchsuchen können: Ein positives Suchergebnis wird die Mitgliedstaaten identifizieren, von denen vollständige Strafregisterinformationen über eine bestimmte Person erhalten werden können.

ECRIS wurde rund 3 Millionen Mal pro Jahr für den Austausch von Informationen über frühere strafrechtliche Verurteilungen genutzt. Etwa 30 % der Fälle, in denen Strafregisterinformationen angefordert werden, werden positiv beantwortet.

Laut der Meijers-Kommission, einer Gruppe von Rechtsprofessoren, Forschern, Richtern und Anwälten, die sich dafür einsetzt, dass die europäische Gesetzgebung die Rechtsstaatlichkeit respektiert und die Grundrechte für alle garantiert, ist die ECRIS-TCN-Verordnung die erste

europäische Gesetzgebung, die europäische Bürger, die auch Staatsangehörige eines Drittlandes sind, als Drittstaatsangehörige behandelt.

Interoperabilität der Systeme

Die Server all dieser Systeme befinden sich in Straßburg. Dort werden die Server vom EU-Lisa-Dienst verwaltet. Wenn wir an Grenzkontrollen und Mobilitätskontrollen denken, denken wir normalerweise an Frontex, aber Frontex ist nicht der Hauptakteur bei diesen Datenbanken. EU-Lisa, die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ist seit 2012 tätig und hat ihren Sitz in Tallinn, Estland, aber ihr operatives Zentrum ist in Straßburg. Sie hat die Erprobung des Pilotprojekts Smart Borders und die nachfolgenden Maßnahmen, die Analyse der Ergebnisse und die Berichterstattung über dieses Projekt in enger Zusammenarbeit mit den teilnehmenden EU-Ländern und den europäischen Institutionen koordiniert. EU-Lisa ist für das Betriebsmanagement von EURODAC, SIS II, VIS und das Entry-Exit System zuständig und gewährleistet dabei die Informationssicherheit und den Datenschutz.

2019 verabschiedete die EU zwei Verordnungen, mit denen ein Rechtsrahmen geschaffen wurde, der die Interoperabilität von sechs der oben beschriebenen Datenbanken (VIS, SIS II, Eurodac, Entry-Exit System, ECRIS-TCN und ETIAS) vorschreibt. Ziel ist es, das allgemeine Datenverbundsystem bis Ende 2023 umzusetzen.

Während die Europäische Kommission die Interoperabilität als natürliche Entwicklung darstellt, ist dies in der Praxis nicht der Fall, da viele der bestehenden Datenbanken noch nicht voll funktionsfähig sind.

„Punkt ohne Wiederkehr“

Nach Ansicht des Europäischen Datenschutzbeauftragten würde die Entscheidung des EU-Gesetzgebers, diese Systeme interoperabel zu machen, einen „Punkt ohne Wiederkehr“ bedeuten, mit tiefgreifenden Auswirkungen auf das Recht auf Privatsphäre von Menschen, die in die EU einreisen. Eine neue zentrale Datenbank mit Informationen über Millionen von Drittstaatsangehörigen, einschließlich ihrer biometrischen Daten, würde einen neuen und verbesserten Zugang zu Informationssystemen erhalten.

Vier weitere Datenerhebungsplattformen in der EU werden in den nächsten zwei Jahren in Betrieb genommen oder sollen ihren Anwendungsbereich erweitern. Das Europäische Suchportal (ESP) wird es den zuständigen nationalen und EU-Behörden ermöglichen, wenn diese eine Person nicht identifizieren können oder Zweifel an der angegebenen Identität haben, eine Abfrage zu starten, indem sie biografische oder biometrische Daten an das ESP übermitteln, das dann die sechs Datenbanken gleichzeitig durchsucht. Der Dienst für den Abgleich biometrischer Daten wird aus allen in den zugrunde liegenden Systemen gespeicherten biometrischen Daten Vorlagen erstellen und

speichern. Im Common ID Repository (CIR) wird für jede in den Systemen registrierte Person ein individueller Datensatz gespeichert, der biometrische und biografische Daten enthält. Schließlich wird der Multiple Identity Detector in der Lage sein, Identitäten über alle Systeme hinweg abzugleichen.

Wie in dem von Petra Molnar verfassten Bericht „Technological Testing Grounds“ des EDRI Network und des Refugee Law Lab festgestellt wird, bietet dieser einheitliche Interoperabilitätsrahmen eine günstige Infrastruktur für viele automatisierte Entscheidungsprozesse, die die Menschenrechte gefährden. Statewatch-Direktor Chris Jones, Autor des Berichts „Automated suspicion: the EU's new travel surveillance initiatives“, erklärte dazu: „Der Enthusiasmus der EU-Beamten und der Beamten der Mitgliedsstaaten, neue Techniken und Instrumente bei ahnungslosen Reisenden einzusetzen, ist besorgniserregend, da sie das Risiko der Diskriminierung erhöhen, zu weiteren Fehlentscheidungen führen können und den Regierungen mehr personenbezogene Daten liefern. Die Menschen sollten mehr darüber nachdenken, wie ihre Regierungen mit Ausländern umgehen – sonst könnten auch sie als Verdächtige und nicht als Bürger behandelt werden.“

Bemerkenswert ist auch das völlige Fehlen einer Folgenabschätzung des Gesetzgebers zu den menschenrechtlichen Auswirkungen der neuen interoperablen Systeme sowie zu den Ressourcen und dem Umfang der unabhängigen Behörden, die diese Systeme kontrollieren, um sie zur Rechenschaft zu ziehen.

Eine der Tücken der technologischen Entwicklung besteht darin, dass wir zu der Ansicht neigen, dass sie die Effizienz steigern und dazu beitragen wird, die Ziele zu erreichen, für die sie entwickelt wurde. Allzu oft ist dies jedoch nicht der Fall. Ein erstes großes Problem, das sich stellt, hat mit der Qualität der Daten zu tun, die in einige der oben genannten Datenbanken eingegeben werden. „Einem kürzlich vom Europäischen Rechnungshof veröffentlichten Bericht zufolge gibt es zum Beispiel ein großes Problem mit der Qualität der in das Schengener Informationssystem eingegebenen Daten. Und Qualität kann sich hier sowohl auf biometrische Daten als auch auf alphanumerische Daten beziehen. Es kann zum Beispiel vorkommen, dass ein Polizeibeamter in einem Mitgliedstaat den Namen einer gesuchten Person falsch schreibt, wenn er eine Ausschreibung in das System eingibt, oder den Vornamen einer Person in das Datenfeld für den Nachnamen einträgt“, sagt der Forscher Georgios Glouftios. Wenn eine Person in einer Datenbank mit einem falschen Namen oder anderen Daten von schlechter Qualität registriert wird, können zwei Probleme auftreten. Das erste betrifft falsche Negative: Gesuchte oder verdächtige Personen werden vom System nicht identifiziert, einfach weil ihre Namen nicht korrekt in der Datenbank gespeichert sind. Das andere Problem sind falsch positive Ergebnisse, d. h. die falsche Identifizierung einer Person. Zum Beispiel wird jemand von der Polizei kontrolliert, aus welchem Grund auch immer, und versehentlich sieht sein Name sehr ähnlich oder gleich aus wie eine im System gespeicherte Falschausschreibung. In diesem Fall kann diese Person in Schwierigkeiten geraten, gerade weil das System sie fälschlicherweise als gesuchte Person identifiziert.

„Meiner Meinung nach gibt es drei Hauptprobleme in Bezug auf die Genauigkeit der für die Grenzsicherung eingesetzten Technologien. Erstens: schlechte Datenqualität. Zweitens, die mangelnde Vollständigkeit der Daten. Und drittens, und hier geht es eher um künftige Entwicklungen, verzerrte Daten und potenziell verzerrte Sicherheitsentscheidungen“, sagt Georgios Glouftios.

* Zitat aus „Technological Testing Grounds, Migration Management Experiments and Reflections from the Ground Up“ (EDRi, refugee law lab, November 2020, Autorin Petra Molnar)

Gefangen in einem digitalen Überwachungssystem

Zusammenfassung: Die Auswirkungen von Überwachungssystemen auf schutzbedürftige Bevölkerungsgruppen, Geld für Frontex-Drohnen und die Überwachung der Freizügigkeit von Bürgern innerhalb des europäischen Raums.

Autor: Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

Link: Verfügbar ab dem 26. April 2022

Text:

An einem Morgen im Jahr 2016 überschreitet Erkan, ein türkischer Staatsbürger kurdischer Herkunft, die Schwelle des griechischen Konsulats in Istanbul, um sich an die griechischen Behörden zu wenden. Er wollte ein Visum für die Einreise nach Griechenland beantragen, um aus der Türkei zu fliehen, als das Erdogan-Regime die Verfolgung verschärfte, insbesondere gegen die Führung und die Mitglieder der Oppositionspartei HDP und ihre kurdischen Anhänger. Die griechische Konsularbehörde lehnte den Visumantrag jedoch ab und Erkan war gezwungen, in der Türkei zu bleiben.

Orestiada Evros, 4 Jahre später. Erkan wurde an der griechisch-türkischen Grenze festgenommen, als er versuchte, griechisches Hoheitsgebiet zu betreten, und vor Gericht gestellt. Das Gericht verurteilte ihn zu 4 Jahren Haft ohne Bewährung und einer Geldstrafe von 10.000 Euro aufgrund des Tatbestands der Wiedereinreise in das Land. Erkan war jedoch nicht erneut nach Griechenland eingereist.

Was war geschehen? Vor griechischen Richtern hatte Erkan Asyl in Griechenland wegen der Verfolgung durch das Erdogan-Regime beantragt. Er erfuhr jedoch, dass sein Name auf der nationalen Liste unerwünschter Ausländer (EKANA) und im Schengener Informationssystem (SIS II, dem größten Informationsaustauschsystem zwischen Schengen-Ländern) mit dem Vermerk stand, dass ihm die Einreise für sieben Jahre untersagt worden war. Da er auf diesen Listen stand, wurde er zunächst ins Gefängnis von Komotini und dann ins Gefängnis von Korfu gebracht.

„Wir versuchten herauszufinden, was wirklich geschehen war“, erzählt Erkans Anwältin und Human Rights 360-Anwältin Eugenia Kouniaki. „Mein Mandant war noch nie zuvor nach Griechenland

eingereist und wurde plötzlich wegen der Wiedereinreise verurteilt. Zunächst wandte ich mich an die Polizeibehörden und an den Direktor der Asylbehörde in Athen, der mir antwortete, mein Mandant sei in das EKANA und SIS II aufgenommen worden, weil sein Visum vom Konsulat in Istanbul abgelehnt worden war.“

Der Grund lag ganz einfach in der Funktionsweise des einheitlichen europäischen Visa-Informationssystems (VISA-VIS) und des SIS II. Das griechische Konsulat, das Erkans Antrag bearbeitete, gab die Ablehnung des Visums gleichzeitig in das VIS-System und in das SIS II ein. Dieser Eintrag reichte aus, um ihn ins Gefängnis zu bringen, auch wenn er internationalen Schutz beantragte.

„Selbst als ich darum bat, ihn von der Liste der unerwünschten Personen und aus dem SIS II zu streichen, da Erkan ein Asylbewerber war, weigerte sich die griechische Polizei“, beschreibt Kouniaki. „Abgesehen davon, dass mein Mandant nicht wusste, dass er auf der Liste stand, erhielten wir, als wir versuchten herauszufinden, warum sein Visum 2016 abgelehnt wurde, die vage Antwort 'wegen Fälschung einiger Dokumente'. Als wir versuchten, herauszufinden, welche Dokumente angeblich gefälscht worden waren, konnten wir nicht überprüfen, um welche es sich handelte. Glücklicherweise akzeptierten die Richter in der Berufung, die wir wegen der Verzögerung der Vollstreckung des Urteils einlegten, unsere Argumente, und er wurde nach einem Jahr aus dem Gefängnis entlassen."

Nach all dieser ungerechten Behandlung und Inhaftierung zog er es jedoch vor, das Land zu verlassen, "weil er glaubte, dass er niemals Gerechtigkeit finden würde", so Kouniaki abschließend.

Verbrannte Finger bei der Vermeidung einer Identifizierung in EURODAC

Erkans Geschichte mag ungeheuerlich klingen, aber sie ist leider nicht die einzige, die mit den Folgen von Überwachungstechnologien und biometrischen Datensystemen für Migranten in Verbindung gebracht wird. In dem Bericht „Technological Testing Grounds: migration management experiments and reflections from the ground up“ (EDRi, Refugee Law Lab, November 2020) hat die Autorin Petra Molnar, Rechtsanwältin und Mitglied von EDRi (European Digital Rights), eine Vielzahl von Interviews mit Asylbewerbern in Brüssel gesammelt, die auf ihrem Weg in die Sicherheit Europas mit Mobilitätskontrollsystemen in Berührung kamen.

Caleb, ein verheirateter Mann in den 30ern, beschreibt seine Erfahrungen mit dem Asylverfahren mit den Worten, er fühle sich „wie ein Stück Fleisch ohne Leben, nur mit Fingerabdrücken und Iris-Scans“. Eine andere Migrantin, Esche, beschreibt ihre Begegnung mit Drohnen im Mittelmeer und im Ärmelkanal mit einem erschütternden Zitat, als sie diese am Himmel sah: „Jetzt haben wir fliegende Computer statt mehr Asyl.“

Die unangenehmste Geschichte erzählt Negassi, ein 20-Jähriger aus Äthiopien: „Ich bin müde und will nach England“, sagt er, nachdem er fast zwei Jahre lang ohne Papiere in Brüssel und zuvor fünf Jahre lang in Nürnberg festsaß. Aber er ist nicht zum ersten Mal in Belgien, denn er wurde bereits nach Deutschland abgeschoben, als er in einem Brüsseler Park verhaftet wurde, wo er im Freien schlief. Bei der Erfassung seiner biometrischen Daten durch die belgische Polizei ergaben seine Fingerabdrücke einen Treffer im EURODAC-System, das die Fingerabdrücke von Asylbewerbern speichert und identifiziert und ihn als Erstasylbewerber in Deutschland identifiziert. Aufgrund von Dublin II, wonach das erste Aufnahmeland den Antrag zu bearbeiten hat, wurde er zurückgeschickt.

Negassi räumt ein, dass die Erfassung biometrischer Daten einen Eingriff in den Körper darstellt, fragt aber: „Wie kann ich mich weigern, wenn die Polizei mir Handschellen anlegt, mich auf die Wache bringt und mich zwingt, meine Fingerabdrücke abzugeben“, erklärt er Molnar. Er hat Freunde, die so weit gegangen sind, sich die Finger zu verbrennen, um ihre Fingerabdrücke zu verändern und eine Identifizierung zu vermeiden. „Aber das löst das Problem nicht", meint Negassi, denn eine fehlgeschlagene Identifizierung bedeutet in der Regel eine längere Haftzeit.

„Es gibt einen sehr wichtigen Aspekt, der in der öffentlichen Debatte zu wenig diskutiert wird“, so Petra Molnar, „und zwar die Tatsache, dass diese Überwachungstechnologien Traumata bei Menschen verursachen, die mit der Technologie gar nicht vertraut sind. Die Migranten, mit denen ich gesprochen habe, waren alle der festen Überzeugung, dass sie durch den Kontakt mit diesen Systemen eine rassistische und diskriminierende Behandlung erfahren.“

Aus diesem Grund sei es umso wichtiger, „dass es bei der ausufernden Nutzung dieser Technologien eine Rechenschaftspflicht, Aufsicht und Kontrolle gibt. Wir müssen uns darauf konzentrieren, welche Art von Governance-Strukturen entwickelt werden müssen, um sicherzustellen, dass diese Technologien, die ein Risiko für die Menschenrechte darstellen, den Menschen kein Trauma zufügen.

Die Rechenschaftspflicht scheint jedoch durch die Art und Weise, wie diese Systeme entwickelt werden, nicht verbessert zu werden. Die Beteiligung privater Unternehmen an der Sicherheits- und Verteidigungsindustrie macht die Sache noch komplizierter. Es gibt eine sehr problematische Beziehung zwischen privaten Unternehmen und staatlichen Institutionen, die unter dem Vorwand zusammenarbeiten, dass die Staaten diese Technologien nicht selbst entwickeln können“, betont Molnar. „Daher werden enorme öffentliche Mittel für die Entwicklung dieser Technologien an große Unternehmen vergeben. Aber auch aus rechtlicher Sicht ergibt sich daraus das Problem der sogenannten ‚Verantwortungswäsche‘, wenn etwas schief geht. Wie wir gesehen haben, sagt der Staat in solchen Fällen: ‚Das ist nicht unser Problem, denn wir haben diese Technologie nicht entwickelt.‘ Und das private Unternehmen seinerseits erwidert, dass ‚die staatliche Verwaltung der Instrumente schuld ist.‘“

Die öffentlichen Haushalte für den industriellen Komplex des Migrationsmanagements und der Grenzkontrolle sind jedoch beträchtlich, wie Molnar betont. „Stellen Sie sich vor, das ganze Geld, das in eine so problematische und traumatisierende Technologie fließt, würde in Bildung, Rechtsberatung und Wohnraum investiert. Warum denken die Staaten nicht darüber nach, wie sie das Geld für die soziale Eingliederung einsetzen können, anstatt es in Überwachungstechnologien zu stecken?“

Das Europäische Grenzüberwachungssystem (Eurosur) und das Geld für Drohnen

Das vielleicht interessanteste System für Migrationsfragen ist Eurosur, das Karten sowohl der territorialen/Land- als auch der Seegrenzen erstellt. Es wird von Frontex betrieben und ermöglicht den Austausch von Karten zwischen Staaten über Grenzkontrollen auf See. „Die Entwicklung von Eurosur wurde 2007 eingeleitet, aber es erreichte das Europäische Parlament zum ersten Mal Ende 2012, nachdem Hunderte von Millionen ausgegeben worden waren und das Design fertiggestellt was, was die Institution praktisch vor vollendete Tatsachen stellte. Aufgrund der mangelnden Transparenz wird die Forschung in den zuständigen Direktionen der Europäischen Kommission weitgehend von den Prioritäten des sicherheitsindustriellen Komplexes bestimmt“, berichtet der Journalist Apostolis Fotiadis in seinem Buch „Border Merchants“.

Bei seiner Entwicklung wurde es als „humanitäre Technologie“ angepriesen, ein System, das es den Behörden der einzelnen Mitgliedstaaten ermöglichen würde, Such- und Rettungsaktionen durchzuführen. Die Idee war, dass „wir Karten verwenden und Informationen von Satelliten und auch von Drohnen erhalten, um Migrationsströme, zum Beispiel von Afrika nach Europa, zu erkennen und so Menschen auf See retten zu können.“ Das Problem ist jedoch, dass Eurosur sogenannte Bilder des Grenzvorbereichs erstellt. Dabei handelt es sich um Karten, die sich auf das Gebiet vor der Grenze konzentrieren, bevor ein Schiff an der Seegrenze, zum Beispiel in Griechenland, ankommt. „Die italienischen Behörden können beispielsweise Daten mit den libyschen Behörden austauschen, sodass die libyschen Behörden die Migranten zurücknehmen können. Sie wissen, dass Push-Backs nicht erlaubt sind, also ist die Lösung Pull-Backs. Deshalb wird Libyen finanziert“, erklärt Georgios Glouftios, Dozent an der Universität Trient, dem MIIR.

Bei der Erstellung der Karten des Grenzvorbereichs arbeitet Frontex auch mit dem Satellitenzentrum der Europäischen Union (EU SatCen) zusammen, das Satellitenbilder, Luftaufnahmen und andere damit verbundene Dienste zur Verfügung stellt. In der Eurosur-Datenbank werden auch Vorfälle an den EU-Seegrenzen erfasst, obwohl die Mitgliedstaaten bisher nicht verpflichtet waren, Daten von Vorfällen an Grenzkontrollstellen systematisch und organisiert hochzuladen (dies änderte sich mit einer Durchführungsverordnung im April 2021). Das bedeutet, dass es keine vollständige und systematische Erfassung von Zwischenfällen gibt, was das Gesamtbild der Zwischenfälle an den Außengrenzen trübt. Eine Tatsache, die auch von der Europäischen Kommission im Eurosur-Evaluierungsbericht (September 2018) eingeräumt wird.

Der zweite Bericht von Frontex im Jahr 2018 über den Betrieb von Eurosur verzeichnete mehr als 184.000 Vorfälle im Zeitraum von Dezember 2013 bis Anfang 2018, wobei die überwiegende Mehrheit (147.827) im Zusammenhang mit Migrationsströmen stand.

Events inserted in Eurosur 2013-2018

Eurosur Node	Crisis	Irregular migration	Related crossborder crime	Other	Total events
Member State	66	83,845	20,641	686	105,238
Frontex	80	63,982	12,231	3029	79,322
Total	146	147,827	32,872	3715	184,560

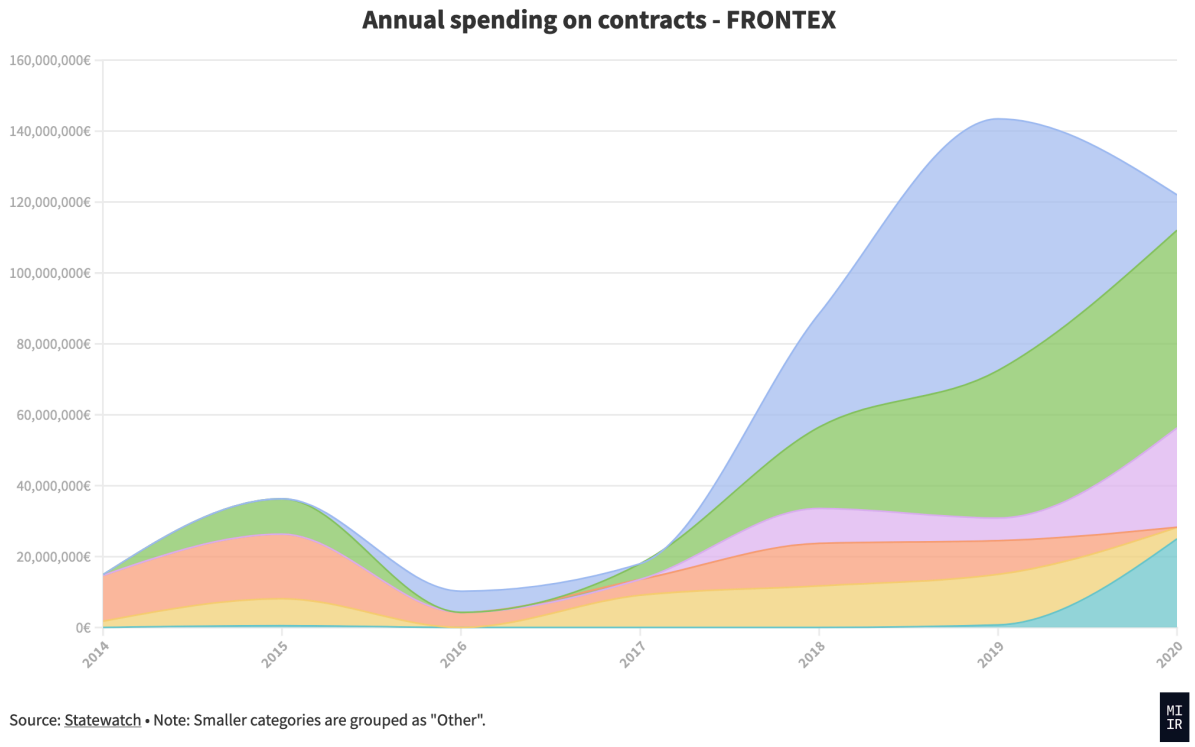
Source: Frontex

Im Februar 2022 kündigte die französische Regierung an, zusätzliche Kameras entlang der Kanalküste zu installieren, um die Überwachung von Migranten zu unterstützen, die auf die Überquerung des Kanals nach Großbritannien hoffen. Die Kosten für die Kameras werden von der britischen Regierung getragen. Im Dezember 2021 lieferte die italienische Marine erneut Container mit Überwachungsausrüstung nach Libyen, um die Migration im Mittelmeer zu überwachen (Quelle: Forschungsmagazin Altreconomia, Ausgabe Februar 2021). Zusätzliche „Kamerafallen“ für Autos und Personen wurden auch an oder in der Nähe der Grenze zwischen Italien und Slowenien entlang der sogenannten Balkanroute aufgestellt.

Augen am Himmel

Frontex bestätigt den Einsatz „einer Reihe von Diensten, die unter Eurosur fallen, d. h. den Rahmen für den Informationsaustausch, der die Verwaltung der europäischen Außengrenzen verbessern soll“ (Quelle: infomigrants.net, „Digital borders: EU increases use of technology to monitor migration“, 18.2.2022). Darin heißt es, dass der größte Teil dieser Überwachung „durch die Luftüberwachung mit bemannten und unbemannten Flugzeugen, mit Satellitenbildgeräten und der Erfassung von Schiffspositionen durch Ortungssysteme“ durchgeführt wird.

Laut einer kürzlich von der gemeinnützigen Organisation Statewatch durchgeführten Untersuchung („Funds for Fortress Europe: spending by Frontex and EU-LISA“, Januar 2022) gibt Frontex den größten Teil seines Jahresbudgets für die Überwachung auf See und aus der Luft sowie für Abschiebungen (Charter- und Linienflüge zur Rückführung von Migranten) aus. Laut einer von Statewatch durchgeführten Datenanalyse hat Frontex zusammen mit der europäischen Agentur EU-LISA (die für groß angelegte Informationssysteme zur Mobilitätskontrolle zuständig ist) zwischen 2014 und 2020 insgesamt 1,9 Milliarden Euro für Verträge mit privaten IT-Unternehmen und der Sicherheits- und Verteidigungsindustrie ausgegeben. Davon wurde etwa eine halbe Milliarde (434 Mio. EUR) von Frontex verwaltet, wobei mehr als 100 Mio. EUR in Verträge mit privaten Unternehmen im Bereich der Luftüberwachung flossen. Dazu gehörte ein 50-Millionen-Euro-Vertrag mit dem Airbus-Konsortium – einem der führenden transeuropäischen Unternehmen in der Luft- und Raumfahrt und der Verteidigungsindustrie – und dem israelischen Unternehmen Albeit, das 85 % der Drohnen der israelischen Armee liefert.



https://public.flourish.studio/visualisation/9014574/

Im gleichen Zeitraum scheint Frontex eine profitable Beziehung zu drei anderen Anbietern von Luftüberwachungsdiensten unterhalten zu haben: der kanadischen CAE Aviation, der britischen Diamond-Executive Aviation (DEA) und der niederländischen EASP Air. Als Konsortium haben sie acht Verträge im Gesamtwert von 57 Mio. EUR abgeschlossen (nicht mitgezählt die Verträge, die sie allein für andere Sicherheits- und Kontrolldienste für Frontex unterzeichnet haben).

Dieser Trend setzt sich auch 2021 fort: 84 Millionen Euro – also ein Sechstel des Jahresbudgets von Frontex – fließen in Luftüberwachungsdienste.

Im Rahmen des Abschiebungsverfahrens hat Frontex mit der polnischen eTravel SA einen 30-Millionen-Euro-Vertrag über die Erbringung von Reisedienstleistungen (Buchung und Ticketausstellung) für die planmäßigen Rückflüge geschlossen. Außerdem hat Frontex mit dem britischen multinationalen Unternehmen Air Charter Service Limited und dem norwegischen Unternehmen AS Aircontact im Bereich Charterflüge für denselben Zweck zusammengearbeitet.

Die in London ansässige Organisation Privacy International veröffentlichte im Juli 2021 ihre Erkenntnisse darüber, dass immer mehr Unternehmen „Satelliten mit der Fähigkeit entwickeln, Daten zu verfolgen und an Grenzbehörden zu verkaufen“. Die Organisation kam zu dem Schluss, dass „eine solche Überwachung zwar Leben retten kann, aber auch Rückschlüsse erleichtern oder zur Verfolgung von Asylbewerbern genutzt werden kann.“

Der Einsatz all dieser Überwachungstechnologien hat auch tiefere Folgen, unterstreicht Antonella Napolitano, Netzwerkkoordinatorin von Privacy International. „Einerseits trägt sie zur Kriminalisierung der Person des Migranten bei und macht ihn gleichzeitig zu einer Datendrehscheibe, vom Beginn der Reise aus dem Herkunftsland bis zur Auswertung der biometrischen Daten in der EU. Ziel ist es, seine Bewegung vollständig aufzuzeichnen und ihn bis zu den nächsten Schritten innerhalb des europäischen Raums zu verfolgen. Und wenn er einmal aufgrund einer falschen Aufzeichnung oder Entscheidung in diesen Systemen verstrickt ist, in denen seine Daten gespeichert sind, verfolgt ihn dieser Fehler für den Rest seines Lebens."

Dieser Gedanke sollte nicht getrennt von der Gefahr betrachtet werden, dass eine solche Überwachung auf das gesamte Spektrum des Reisens ausgedehnt wird, sei es zu touristischen oder beruflichen Zwecken. Außerdem, so Napolitano, „ist gerade die Interoperabilität der Systeme ein gutes Beispiel dafür, wie ein System, das zur Überwachung von Migrationsbewegungen entwickelt wurde, auf alle Menschen ausgedehnt werden kann, da diese Systeme nach und nach auf alle Reisenden, die in den europäischen Raum einreisen, aber auch auf EU-Bürger, die sich innerhalb der EU bewegen, ausgedehnt werden.
Die Tatsache, dass man möglicherweise „standardmäßig als Krimineller" betrachtet wird, ein Konzept, das sich in der Verwaltung von Überwachungstechnologien widerspiegelt, kann niemanden gleichgültig lassen."

Fluggastdatensätze: Überwachung des innergemeinschaftlichen Flugverkehrs

Die Fluggastdatensätze (PNR) dienen der Erfassung aller Daten von Fluggästen, die sich im europäischen Hoheitsgebiet bewegen, unabhängig davon, ob sie aus einem Drittland kommen. Was wird in diesem System erfasst? Name, Staatsangehörigkeit, wann wir gereist sind, von wo aus, wohin, unsere E-Mail-Adresse und unsere Anschrift. Außerdem kann man unsere Reisebegleiter herausfinden, möglicherweise einige Daten im Zusammenhang mit unserem Aufenthalt wie Hotelreservierungen, ob wir aus geschäftlichen oder privaten Gründen gereist sind. Im Extremfall kann es sogar unsere Religion herausfinden, da das System sogar die Mahlzeit aufzeichnet, die wir während des Fluges gegessen haben. Diese Mahlzeit kann „interessante" Fakten über uns enthalten, z. B. wenn wir koscher essen, sind wir Juden, wenn wir kein Schweinefleisch essen, sind wir Muslime. Es kann auch aufzeigen, ob jemand Allergien hat.

Die PNR-Daten sind für die Polizeibehörden der einzelnen Länder zugänglich. „Und genau hier beginnen die Probleme. Es gibt eine europäische Richtlinie darüber, wie personenbezogene Daten über das PNR-System verarbeitet werden können. Diese europäische Gesetzgebung muss in den einzelnen Ländern in nationales Recht umgesetzt werden. Das Problem ist, dass es bei der Umsetzung dieser Richtlinie in verschiedenen Ländern wie zum Beispiel in Griechenland zu Versäumnissen gekommen ist", erklärt Rechtsanwalt Kostas Kakavoulis, Mitglied von Homo Digitalis, dem MIIR. „Die europäische Richtlinie sieht vor, dass jeder Mitgliedstaat eine Behörde einrichtet oder benennt,

die für die Verhütung, Aufdeckung, Ermittlung und Verfolgung schwerer terroristischer Straftaten zuständig ist. Es handelt sich also um eine Behörde, die entweder von Anfang an eingerichtet wird oder bereits existiert und der diese Zuständigkeit übertragen wurde. In Griechenland hat der Gesetzgeber diese Zuständigkeit einer Abteilung innerhalb der Direktion für Informationsmanagement und Analyse der griechischen Polizei übertragen. Wir sprechen also nicht von einer Behörde, sondern von einer Direktion der griechischen Polizei. Es ist absurd, dass die Stelle, die über die Daten verfügt, nämlich die Polizei, von einer Abteilung innerhalb der Polizei Zugang zu diesen Daten verlangt. Wenn sie einer hierarchischen Kontrolle unterliegt oder generell Druck ausgeübt wird, ist es eher zweifelhaft, dass eine Abteilung der griechischen Polizei sich weigern wird, anderen Abteilungen der griechischen Polizei benötigte Daten zur Verfügung zu stellen, selbst wenn eine Weigerung notwendig wäre. In Frankreich ist dies nicht der Fall, da eine spezielle unabhängige Behörde für PNR-Daten eingerichtet wurde. In Griechenland kann jede Polizeibehörde jederzeit und überall unkontrollierten Zugriff auf PNR-Daten erhalten. Es gibt keinerlei Aufzeichnungen darüber, wer welche Daten wann und zu welchem Zweck angefordert hat. Und es gibt auch keine Geheimhaltungsvorschriften für den Zugang. Man muss nur Mitglied der Polizei sein, um auf diese Daten zugreifen zu können."

In Griechenland hebt die Organisation Homo Digitalis (Mitglied von EDRi) in einem offenen Brief an das Parlament hervor, dass „die fraglichen Daten das Bewegungsmuster einer Person offenbaren können, wie z. B. die Reisezeit, den Abfahrts- und Ankunftsort, ihre E-Mail-Adresse und Anschrift sowie die Reisebegleiter einer Person, aber möglicherweise auch damit verbundene Hotelbuchungsdaten usw., wodurch Informationen über geschäftliche oder private Reisen und sogar den sozialen Kreis der Person, wie z. B. Freunde oder Gefährten, offengelegt werden können."

Die Organisation weist darauf hin, dass der 2018 in Griechenland vorgelegte Gesetzesentwurf folgende Probleme umfasste:

- Fehlen eines Systems zur Erfassung des Zugriffs auf PNR-Daten
- fehlende vorherige gerichtliche Kontrolle der Weitergabe von PNR-Daten an Ermittlungsbehörden und andere Behörden
- die Speicherfrist für PNR-Daten ist nicht auf den unbedingt erforderlichen Zeitraum beschränkt

Vier Jahre später sind die gleichen Unzulänglichkeiten immer noch vorhanden.

Die Organisation betonte, dass die übermittelten PNR-Daten von Minderjährigen klar und genau beschrieben werden sollten und dass die übermittelten Daten weder religiöse Überzeugungen noch Informationen über die Gesundheit des Fluggastes preisgeben sollten.

Automatisierung und Überwachung in der Festung Europa

Zusammenfassung: Künstliche Intelligenz und Algorithmen stehen im Mittelpunkt der neuen EU-Mobilitätskontrollregelung. Es werden hochriskante automatisierte Entscheidungen über Menschenleben getroffen. Es handelt sich um einen aufstrebenden, unregulierten Multi-Milliarden-Euro-Markt mit dystopischen „intelligenten“ Anwendungen.

Autor: Kostas Zafeiropoulos, Ioanna Louloudi, Nikos Morfonios (MIIR)

Link: Verfügbar ab dem 26. April 2022

Text:

Ende Juni 2020 wurde Robert Williams, ein afroamerikanischer Einwohner von Detroit, vor den Augen seiner beiden kleinen Töchter am Eingang seines Hauses verhaftet. Niemand konnte ihm sagen, warum. Auf dem Polizeirevier wurde ihm mitgeteilt, dass er als Verdächtiger im Zusammenhang mit dem Raubüberfall auf ein Geschäft im Jahr 2018 galt, da sein Gesicht auf den Überwachungsaufnahmen des Geschäfts zu erkennen war. Die Identifizierung erfolgte auf der Grundlage eines alten Führerscheinfotos. Nach dreißig Stunden Gewahrsam wurde Robert Williams schließlich freigelassen. Das zynische Geständnis der Detroiter Polizeibeamten war entwaffnend: „Der Computer hat wahrscheinlich einen Fehler gemacht.“

Einen ähnlichen Vorfall erlebte im Juni 2019 Michael Oliver, ebenfalls ein afroamerikanischer Einwohner von Detroit, der verhaftet wurde, nachdem sein Gesicht angeblich auf einem Überwachungsvideo erkannt worden war. Er wurde vor Gericht gestellt, wo er schließlich drei Monate nach seiner Verhaftung freigesprochen wurde.

In ähnlicher Weise identifizierte das Programm der Software „Rekognition“ von Amazon in einer Teststudie 28 Mitglieder des Kongresses(!) fälschlicherweise als Personen, die zuvor wegen eines Verbrechens verhaftet worden waren. Die falschen Identifizierungen betrafen überwiegend Schwarze und Latinos. Aber gehen Sie nicht davon aus, dass dies nur in den USA geschieht.

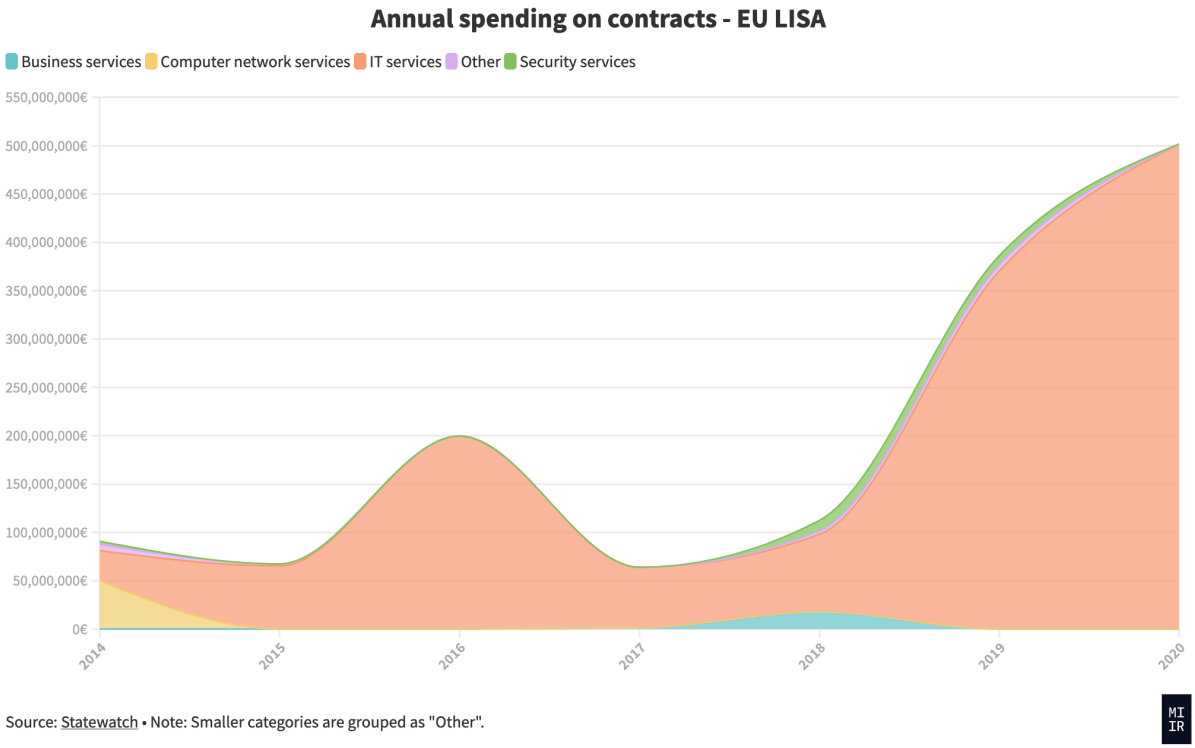
Wie in den beiden vorangegangenen Teilen der MIIR-Forschungsarbeit zum Thema „Europas digitale Festungsmauern“ erörtert wurde, hat die EU als Teil einer neuen Architektur der Grenzüberwachung und Mobilitätskontrolle in den letzten Jahren eine Reihe von Systemen zur Erfassung und Überwachung von Bürgern eingeführt, die sich im europäischen Raum bewegen. Die EU nutzt verschiedene Finanzierungsmechanismen für Forschungs- und Entwicklungszwecke, wobei der Schwerpunkt zunehmend auf Technologien der künstlichen Intelligenz (KI) liegt, die auch biometrische Daten nutzen können. Zwischen 2007 und 2013 (aber mit Projekten, die bis 2020 laufen) war das Siebte Rahmenprogramm (RP7) das wichtigste dieser Programme, gefolgt von Horizont 2020. Mit diesen beiden Programmen wurden EU-Sicherheitsprojekte im Wert von mehr als 1,3 Milliarden Euro finanziert. Für den laufenden Zeitraum 2021–2027 verfügt Horizont Europa über ein Gesamtbudget von 95,5 Milliarden Euro, wobei der Schwerpunkt auf Sicherheitsfragen liegt. Technologien wie automatisierte Entscheidungsfindung, Biometrie, Wärmebildkameras und Drohnen

kontrollieren zunehmend die Migration und betreffen Millionen von Menschen, die unterwegs sind. Die Grenzverwaltung hat sich in der EU und in anderen Teilen der Welt zu einem profitablen Milliardengeschäft entwickelt. Nach einer Analyse von TNI (Border War Series) wird das jährliche Wachstum des Grenzsicherheitsmarktes voraussichtlich zwischen 7,2 % und 8,6 % liegen und bis 2025 ein Gesamtvolumen von 65–68 Mrd. USD erreichen.

Das größte Wachstum verzeichnen die globalen Märkte für biometrische Daten und künstliche Intelligenz (KI). Für den Biometriemarkt selbst wird eine Verdoppelung des Umsatzes von 33 Mrd. USD im Jahr 2019 auf 65,3 Mrd. USD bis 2024 prognostiziert. Ein erheblicher Teil der Mittel ist für den Ausbau der Kapazitäten von EU-LISA (Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht) bestimmt, die eine Schlüsselrolle bei der Verwaltung der Interoperabilität von Datenbanken für die Mobilitäts- und Sicherheitskontrolle spielen soll. Die Arbeiten an diesem Supercomputer werden finanziert von:

- einen Zuschuss aus dem Gesamthaushaltsplan der EU.
- Ein Beitrag der Mitgliedstaaten in Bezug auf das Funktionieren des Schengen-Raums und Eurodac-bezogene Maßnahmen.
- direkte finanzielle Beiträge der Mitgliedstaaten.

Chris Jones, Exekutivdirektor der gemeinnützigen Organisation Statewatch, verfolgt seit mehreren Jahren den Weg des Geldes, der in Brüssel beginnt. Er erklärt, dass „EU-LISA-Projekte in der Regel von Konsortien aus privaten Unternehmen, öffentlichen Einrichtungen und Universitäten durchgeführt werden. Private Unternehmen erhalten die größten Summen, mehr als öffentliche Einrichtungen.“ Eine aktuelle Statewatch-Studie (Funds for Fortress Europe: spending by Frontex and EU-LISA, Januar 2022) zeigt, dass im Zeitraum 2014–2020 rund 1,5 Milliarden Euro an private Auftragnehmer für die Entwicklung und Stärkung von EU-LISA geflossen sind, wobei der größte Anstieg nach 2017 und dem Höhepunkt der Flüchtlingskrise zu verzeichnen war.



https://public.flourish.studio/visualisation/9014422/

Das Überwachungsoligopol

Einer der wichtigsten Verträge im Jahr 2020 im Wert von 300 Millionen Euro wurde zwischen den französischen Unternehmen Idemia und Sopra Steria für die Einführung eines neuen biometrischen Abgleichsystems (BMS) unterzeichnet. Diese Unternehmen erhalten häufig neue Aufträge, da sie Vereinbarungen über die Wartung der Systeme EES, EURODAC, SIS II und VIS haben. Andere Unternehmen, die Verträge in hohem Wert für EU-LISA-bezogene Arbeiten erhalten haben, sind Atos, IBM und Leonardo – im Wert von 140 Millionen Euro – und das Konsortium Atos, Accenture und Morpho (später Idemia), das 2016 einen Vertrag im Wert von 194 Millionen Euro unterzeichnete. Die von Statewatch gesammelten Daten zeigen auch die Zusammenarbeit (in der Regel in Form von Joint Ventures) bei der Erweiterung des EU-LISA-Systems mit Unternehmen mit griechischen Interessen auf, beispielsweise Unisystems SA (im Besitz der Quest-Gruppe des ehemaligen Vorsitzenden des Verbands der griechischen Industriellen Th. Fessa), das 2019 einen Vertrag über 45 Millionen Euro unterzeichnete. Auch European Dynamics SA (im Besitz von Konstantinos Velentzas) ist an einem 2020 vergebenen Auftrag im Wert von 187 Mio. EUR beteiligt, und das in Luxemburg ansässige Unternehmen Intrasoft International SA (früher im Besitz von Kokkalis-Interessen) ist zusammen mit fünf anderen Unternehmen an einem Projekt im Wert von 187 Mio. EUR beteiligt, das ebenfalls 2020 vergeben wurde.

Contracted companies (by contract size) - EULISA

Search...

Company name	Sum of all contracts	Number of contracts	Address
Sopra Steria Benelux SA/NV	604,954,007 €	6	15/23 Avenue Arnaud Fraiteur, Brussels, Belgium
Atos Belgium NV	573,501,690 €	4	DA Vincilaan 5, Zaventem, Belgium
Idemia Identity & Security SAS	302,550,000 €	1	2, place Samuel de Champlain, Courbevoie, France
Accenture NV/SA	271,786,039 €	8	boulevard de Waterloo 16, Brussels, Belgium
Morpho SAS	194,450,000 €	1	11 boulevard Gallieni, Issy-les-Moulineaux, France
ARHS Developments SA	187,000,000 €	1	13 Boulevard du Jazz, Belvaux, Luxembourg
European Dynamics Belgium SA	187,000,000 €	1	15, rue Belliard, Brussels, Belgium
European Dynamics Luxembourg SA	187,000,000 €	1	12, rue Jean Engling, Luxembourg, Luxembourg
European Dynamics SA	187,000,000 €	1	209, Kifissias Ave. & Arkadiou Str, Athens, Greece
Everis Belgique SPRL	187,000,000 €	1	rue de SPA 8, Brussels, Belgium

1 / 5

Source: Statewatch

MI IR

https://public.flourish.studio/visualisation/9468645/

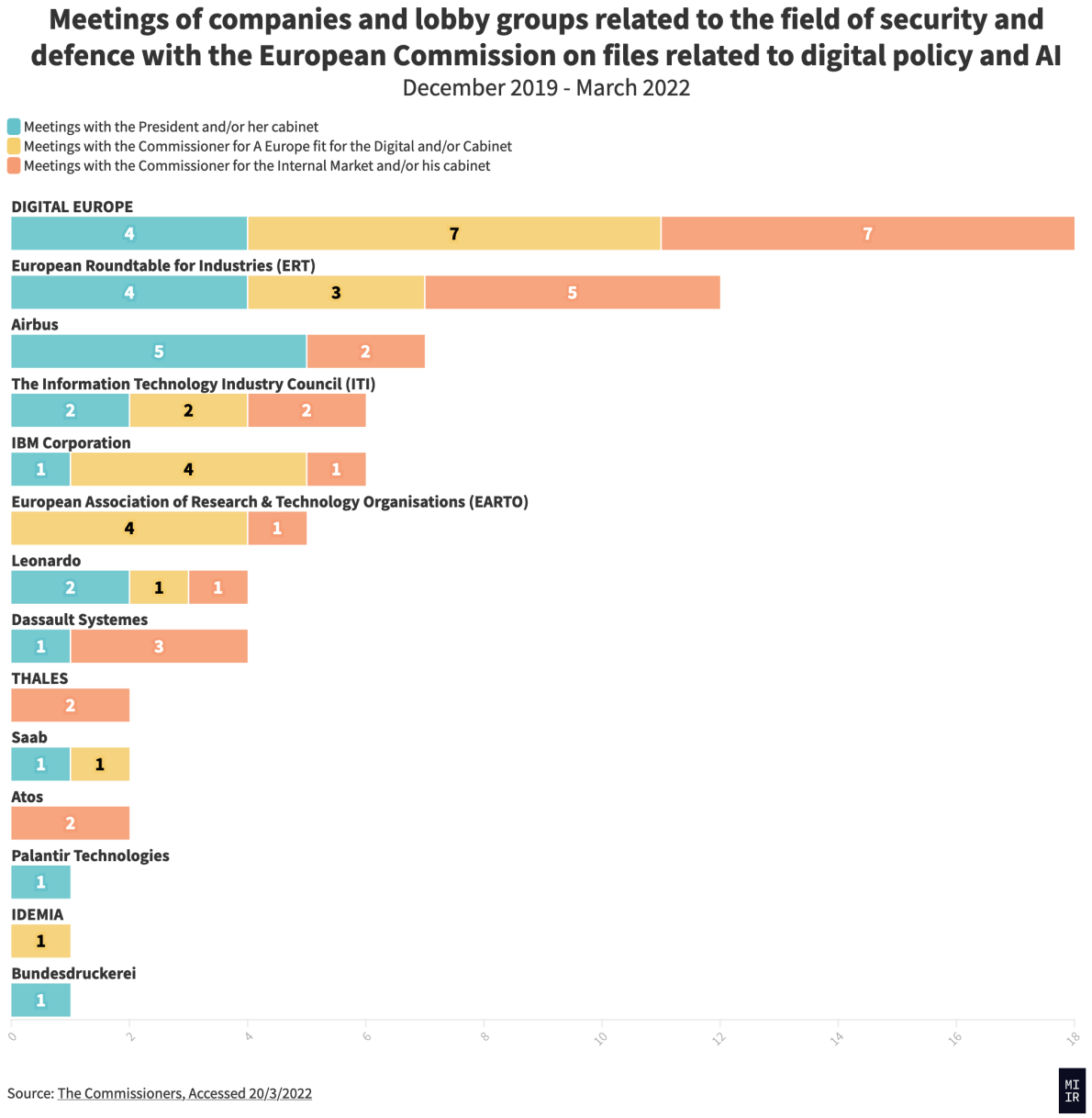
Die Beziehung zwischen EU-LISA und der Industrie zeigt sich auch in der häufigen Durchführung gemeinsamer Veranstaltungen, wie z. B. dem „Runden Tisch mit der Industrie“, der am 16. Juni 2022 in Straßburg stattfinden wird. Dies wird das 15. Treffen dieser Art sein, an dem EU-Gremien, Vertreter von Mobilitätsmanagementsystemen und Einzelpersonen teilnehmen werden. „Es gibt umfangreiche, lange und sehr geheime Verhandlungen zwischen den Mitgliedsstaaten und den Abgeordneten des Europäischen Parlaments, wenn sie etwas in den Datenbanken ändern wollen. Aber wir wissen nicht, welchen Einfluss die Unternehmen, die diese Systeme betreiben, wirklich haben, ob sie das technisch Machbare unterstützen und wie all dies mit dem politischen Prozess zusammenhängt“, sagt Chris Jones von Statewatch. Auch der Inhalt der Verträge, die zwischen den Konsortien und EU-LISA geschlossen wurden, bleibt unbekannt, da er nicht veröffentlicht wird.

Die neuen Grenzen der KI und der Druck auf die EU

Im April 2021 veröffentlichte die Europäische Kommission ihren lang erwarteten Entwurf einer Verordnung über künstliche Intelligenz (AI ACT). Das Konsultationsverfahren wird voraussichtlich einige Zeit in Anspruch nehmen. Dieser wichtige Rechtsakt umfasst mehr als 200 Seiten und wird – unter anderem – eine Verfeinerung der Datenschutz-Richtlinie (Richtlinie 680/2016) sein. Es wird erwartet, dass die Unternehmen und Akteure des Sektors erheblichen Druck ausüben werden, bis der Gesetzentwurf in seiner endgültigen Form dem Europäischen Parlament vorgelegt wird.

Das MIIR hat die Aufzeichnungen offizieller Treffen zu KI- und digitalpolitischen Themen zwischen der Präsidentin der Europäischen Kommission Ursula von der Leyen, Kommissarin Margrethe

Vestager („Ein Europa, das fit ist für das digitale Zeitalter“), Kommissar Thierry Breton (Binnenmarkt) und ihren Mitarbeitern zwischen Dezember 2019 und März 2022 untersucht. Daraus geht hervor, dass sich mindestens 14 Agenturen, Konzerne des Privatsektors und Unternehmenskonsortien aus dem Sicherheits- und Verteidigungssektor in 28 Monaten 71 Mal mit wichtigen Vertretern der Europäischen Kommission getroffen haben, um Fragen der Digitalpolitik und KI zu erörtern. Die meisten Treffen mit den Kommissaren wurden von DIGITALEUROPE abgehalten, einer Organisation, die 78 Unternehmensmitglieder vertritt, darunter große Verteidigungs- und Sicherheitsunternehmen wie Accenture, Airbus und Atos. Es wurde auch festgestellt, dass andere Konsortien starkes Lobbying betreiben, darunter der European Round Table for Industries (ERT), der eine Reihe von Verteidigungs- und Sicherheitsunternehmen wie Leonardo, Rolls-Royce und Airbus vertritt.



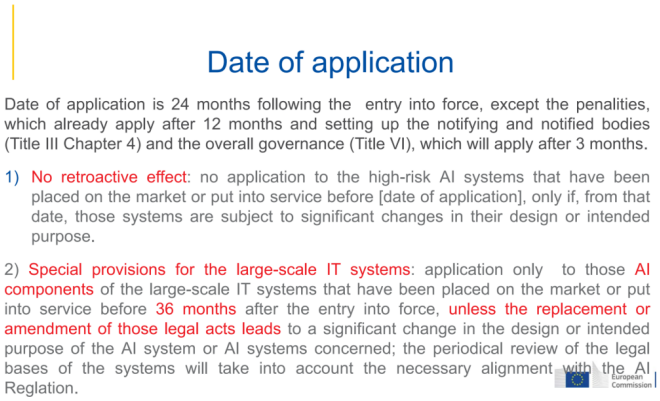
https://public.flourish.studio/visualisation/9083043/

Hochrisikosysteme

Der Vorschlag für eine europäischen Verordnung (COM/2021/206 final), der im April 2021 angenommen wurde, gibt einen guten Überblick über die KI-Systeme und -Anwendungen, die reguliert werden sollen, sowie über die Risiken ihres unregulierten Betriebs an den Eintrittspunkten Europas. Wie bereits erwähnt: „[...] sollten KI-Systeme eingestuft werden, die dazu gedacht sind, von den für Aufgaben in den Bereichen Einwanderungsmanagement, Asyl und Grenzkontrollen zuständigen Behörden als Polygraphen und ähnliche Instrumente, zur Erkennung des emotionalen Zustands einer Person oder zur Bewertung bestimmter Risiken verwendet zu werden, die von natürlichen Personen ausgehen, die in das Hoheitsgebiet eines Mitgliedstaats einreisen oder ein Visum beantragen."

Der kritische Parameter

Der Bereich, in dem „risikoreiche" KI-Systeme eingesetzt werden können, scheint breit gefächert zu sein. Trotz der Hoffnung, dass eine neue Richtlinie ihre Funktionsweise regeln wird, gibt es einen Parameter, der diese Möglichkeit ausschließen könnte. Wie aus einer internen Präsentation im Rahmen der internen Überprüfung der Europäischen Kommission hervorgeht, die im Mai stattfand und von Statewatch ans Licht gebracht wurde, wird die neue Verordnung bei Verabschiedung 24 Monate nach ihrer Unterzeichnung in Kraft treten und nicht für alle Systeme gelten, da sie voraussichtlich nicht rückwirkend für die Systeme gelten wird, die vor dem Datum des Inkrafttretens auf dem Markt sind.



„Es ist so, als würde man sagen: ‚Ja, wir sollten den Einsatz von künstlicher Intelligenz und maschinellem Lernen auf verantwortungsvolle Weise kontrollieren. Aber wir werden es nicht für die Systeme tun, die wir bereits bauen, weil … wir andere Ideen für sie haben …'", kommentiert Chris Jones. Das Problem wird auch in der gemeinsamen Erklärung angesprochen, die unter der Schirmherrschaft des EDRI-Netzwerks für digitale Rechte im November von 114 zivilgesellschaftlichen Organisationen veröffentlicht wurde und in der hervorgehoben wird, dass „keine angemessene Begründung für diese Ausnahme von der KI-Verordnung im Gesetzentwurf

enthalten ist oder vorgelegt wird.“ In der Mitteilung fordern sie den Europarat, das Europäische Parlament und die Regierungen der Mitgliedstaaten auf, in den endgültigen Gesetzentwurf Garantien für die Rechenschaftspflicht aufzunehmen, die einen sicheren Rahmen für die Implementierung von KI-Systemen und vor allem den Schutz der Grundrechte der europäischen Bürger gewährleisten.

Roboter-Hunde in Aktion: Algorithmen und alptraumhafte Forschungsprojekte

„Die EU-Institutionen und die Mitgliedstaaten unternehmen große Anstrengungen, um die Zahl der Abschiebungen zu erhöhen. Die EU hat Geld und Ressourcen in diese Datenbanken gesteckt, um im Wesentlichen zu sagen: ‚Wir wollen dazu beitragen, diese Menschen von europäischem Boden zu entfernen‘“, so Chris Jones von Statewatch. In der Tat spielen die Automatisierung und der Einsatz von durch die Industrie geförderten algorithmischen Werkzeugen bereits eine wichtige Rolle an den europäischen Einreisestellen und werfen viele Fragen über die Wahrung der Rechte von Flüchtlingen und Migranten auf. Es ist nicht nur die Profilerstellung, die diejenigen beunruhigt, die diese EU-Projekte kritisieren, sondern auch die Qualität der Daten, auf die sich dieser Prozess stützt. „Es sieht aus wie eine ‚Black Box‘, bei der wir nicht genau wissen, was drin ist“, sagt die Flüchtlingsrechtsexpertin und Anthropologin Petra Molnar, die sich auf die Gefahr einer Automatisierung ohne menschlichen Faktor bei der Entscheidungsfindung konzentriert, wenn es um Menschenleben geht.

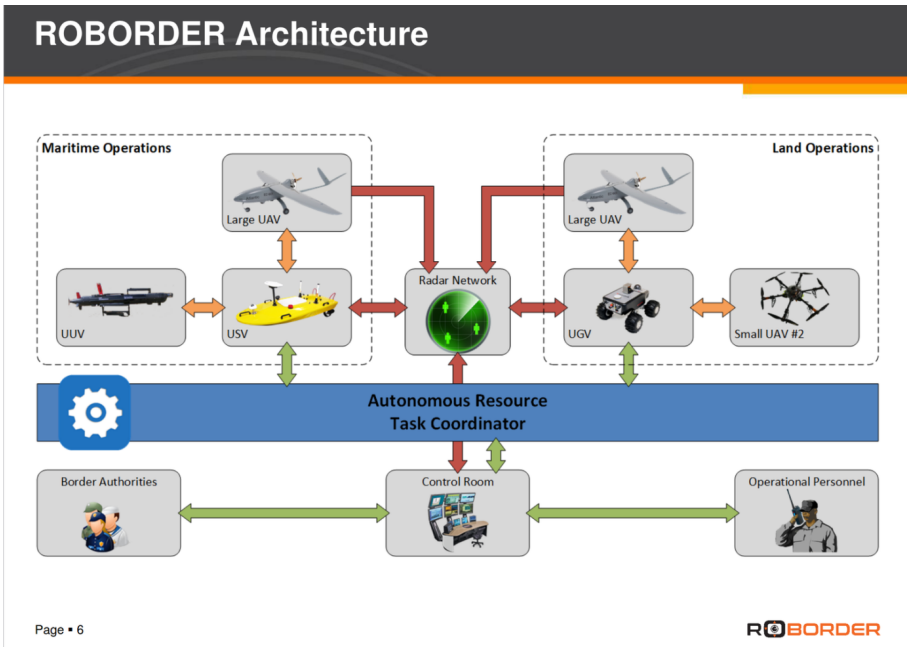
Zu den wichtigsten in den letzten Jahren finanzierten Pilotsystemen gehören Folgende:

iBorderCtrl – „intelligente“ Lügendetektoren: Dieses System kombiniert Gesichtsabgleich und Werkzeuge zur Dokumentenauthentifizierung mit KI-Technologien. Es handelt sich dabei um einen „Lügendetektor“, der in Ungarn, Griechenland und Lettland getestet wurde und bei dem ein „virtueller Grenzschutzbeamter“ eingesetzt wird, der auf das Geschlecht, die Nationalität und die Sprache des Reisenden zugeschnitten ist – ein Beamter, der über eine Digitalkamera Fragen stellt. Das Projekt wurde mit 4,5 Millionen Euro aus dem Programm Horizont 2020 der Europäischen Union finanziert und heftig als gefährlich und pseudowissenschaftlich kritisiert („Sci-fi surveillance: Europe's secretive push into biometric technology“, The Guardian, 10. Dezember 2020; “We Tested Europe's New Lie Detector for Travelers – and Immediately Triggered a False Positive”, The Intercept, 26. Juli 2019).

Es wurde Anfang Juli 2019 unter simulierten Bedingungen in den Räumlichkeiten von TRAINOSE in einem speziell eingerichteten Bereich des Zentrums für Sicherheitsstudien in Athen getestet. Vor der Abreise mussten die Reisenden ein Foto eines Personalausweises oder Reisepasses in eine spezielle Anwendung hochladen. Anschließend beantworteten sie Fragen, die ihnen von einem virtuellen Grenzbeamten gestellt wurden. Eine spezielle Software zeichnete ihre Worte und Gesichtsbewegungen auf, die einem normalen Auge entgangen sein könnten, und berechnete am Ende – angeblich – den Grad der Aufrichtigkeit des Reisenden.

Am 2. Februar 2021 entschied der Europäische Gerichtshof über eine Klage des Europaabgeordneten und Aktivisten Patrick Breyer (Piratenpartei) gegen den Datenschutz dieses Forschungsprojekts, das er als pseudowissenschaftlich und orwellsch bezeichnete.

Roborder (ein autonomer Schwarm heterogener Roboter zur Grenzüberwachung): Ziel ist die Entwicklung eines autonomen Grenzüberwachungssystems mit unbemannten Robotern, darunter Luft-, See-, U-Boot- und Bodenfahrzeuge. Die gesamte Roboterplattform integriert multimodale Sensoren in ein einziges interoperables Netz. Vom 28. Juni bis 1. Juli 2021 fand in Griechenland der letzte Pilotversuch des Projekts statt, an dem das griechische Verteidigungsministerium beteiligt ist.



Foldout: Das 8,1 Millionen Euro teure Forschungsprojekt Foldout macht keinen Hehl aus seinen Zielen: „In den letzten Jahren hat die unrechtmäßige Migration dramatisch zugenommen und ist mit den bestehenden Systemen nicht mehr zu bewältigen.“ Die Hauptidee des Projekts, das in Bulgarien erprobt und in Finnland, Griechenland und Französisch-Guinea eingeführt wird, besteht darin, Bewegungssensoren an Grenzabschnitten zu platzieren, wo das Gelände oder die Vegetation die Erkennung eines illegalen Grenzübertritts erschweren. Bei jeder verdächtigen Bewegung, sei es von Menschen oder Fahrzeugen, besteht die Möglichkeit, eine Drohne zu diesem Punkt zu schicken oder Bodenkameras zur zusätzlichen Überwachung zu aktivieren. Das Konsortium, das das System entwickelt, wird vom Austrian Institute of Technology koordiniert (das 25 Millionen Euro aus 37 europäischen Projekten erhalten hat).

Unter den Organisationen, die sich auf europäischer Ebene für diese Projekte einsetzen, trafen wir EARTO, ein Konsortium von Forschungszentren und Projektbegünstigten in verschiedenen

Bereichen, darunter auch Sicherheit. Dazu gehören KEMEA in Griechenland, die Fraunhofer-Gesellschaft (140 EU-finanzierte Forschungsprojekte, darunter Roborder) und das Austrian Institute of Technology (Foldout).

Viele der Horizon 2020-Forschungsprojekte (Roborder, iBorderCtrl, Foldout, Trespass usw.) wurden von ihren eigenen Autoren als noch „unreif" für eine breite Anwendung beschrieben. Der allgemeine Wandel in der Herangehensweise der Europäischen Union an die Nutzung von KI für die Mobilitätskontrolle und die Verbrechensverhütung lässt sich jedoch an der ständig steigenden Finanzierung durch den Europäischen Sicherheitsfonds ablesen. Ein solches Projekt ist die Bereitstellung tausender mobiler Geräte durch die griechische Polizei, die es ermöglichen werden, Bürger mithilfe von Gesichtserkennungs- und Fingerabdruck-Software zu identifizieren. Die Gesamtkosten des von Intracom Telecom durchgeführten Projekts belaufen sich auf über 4 Millionen Euro und werden zu 75 % aus dem Europäischen Sicherheitsfonds finanziert.

Das Samos-„Experiment"

„Grenzen und Einwanderung sind das perfekte Labor für Experimente. Undurchsichtige, risikoreiche Bedingungen mit einem geringen Maß an Verantwortlichkeit. Grenzen werden zum perfekten Testgelände für neue Technologien, die später in größerem Umfang auf verschiedene Gemeinschaften und Bevölkerungsgruppen angewendet werden können. Das ist genau das, was Sie in Griechenland sehen, oder?" fragt die Rechtsanwältin Petra Molnar. Die Antwort lautet ja, sowohl für den Norden als auch für den Süden des Landes.

Auf der Insel Samos an der südöstlichen Grenze Griechenlands zur Türkei werden in dem neuen Migrantenlager, für das die griechische Regierung gerade Werbung macht, zwei spezielle Pilotsysteme namens YPERION und KENTYROS in Betrieb genommen.

YPERION ist ein Asylverwaltungssystem für den gesamten Bedarf des Aufnahme- und Identifizierungsdienstes. Es verarbeitet nicht nur biometrische und biografische Daten von Asylbewerbern sowie auch von Mitgliedern der NRO, die die entsprechenden Einrichtungen besuchen, und von den Mitarbeitern dieser Einrichtungen. Es soll das wichtigste Instrument für den Betrieb der geschlossenen Aufnahmezentren (CRC) sein, da es für die Zugangskontrolle, die Überwachung der Leistungen für jeden Asylbewerber mit einer individuellen Karte (Lebensmittel, Kleidung usw.) und die Bewegungen zwischen den CRC und den Unterbringungseinrichtungen zuständig sein wird. Das Projekt umfasst die Entwicklung einer Mobiltelefonanwendung, die dem Nutzer personalisierte Informationen zur Verfügung stellt und als elektronischer Briefkasten für das Asylverfahren fungiert, mit der Möglichkeit, personalisierte Informationen bereitzustellen.

KENTYROS ist ein digitales System für die Verwaltung der elektronischen und physischen Sicherheit rund um das Gebäude und innerhalb des Gebäudes unter Verwendung von Kameras und

KI-Algorithmen zur Verhaltensanalyse. Es umfasst ein zentrales Management durch das Ministerium für digitale Governance sowie Dienste wie beispielsweise die Signalisierung von Alarmen bei Grenzverletzungen mithilfe von Kameras (die Thermometrie, Fokussierung und Rotation ermöglichen) und Algorithmen zur Bewegungsanalyse, die Signalisierung von Alarmen bei illegalem Verhalten von Einzelpersonen oder Personengruppen in Versammlungsbereichen innerhalb der Einrichtung und den Einsatz unbemannter Flugsysteme zur Bewertung von Vorfällen innerhalb der Einrichtung ohne menschliches Eingreifen.

„KENTYROS setzt Kameras ein, die in der Lage sind, sich auf bestimmte Personen zu konzentrieren, Kameras, die auch die Temperatur einer Person messen können. Das Wichtigste ist nicht, dass KENTYROS dieses Bild aus Sicherheitsgründen verwendet, sondern dass auch Algorithmen zur Verhaltensanalyse eingesetzt werden, ohne genau zu erklären, was das bedeutet“, sagt Kostas Kakavoulis, Anwalt und Mitglied von Homo Digitalis. Er erklärt: „Ein Algorithmus lernt, auf der Grundlage bestimmter Daten, die wir ihm gegeben haben, bestimmte Schlussfolgerungen zu ziehen. Ein solcher Algorithmus ist in der Lage, zwischen der Tatsache zu unterscheiden, dass Person X möglicherweise ein aggressives Verhalten an den Tag legt, andere Asylbewerber oder Wachleute angreift oder illegal aus der Unterkunft fliehen will. Eine weitere Anwendung von Algorithmen zur Verhaltensanalyse ist die Lügenanalyse, mit der beurteilt werden kann, ob unser Verhalten und unsere Worte etwas widerspiegeln, was der Wahrheit entspricht oder nicht. Dies geschieht hauptsächlich durch die Analyse biometrischer Daten, also der Daten, die wir alle durch unsere Bewegung im Raum, durch unsere körperliche Anwesenheit, durch unser Aussehen und auch durch die Art und Weise, wie wir unsere Hände bewegen, wie wir blinzeln, wie wir gehen, erzeugen. All dies mag unbedeutend erscheinen, aber wenn jemand diese Daten über einen langen Zeitraum sammeln und mit den Daten vieler anderer Menschen in Beziehung setzen kann, kann er zu Schlussfolgerungen über uns kommen, die uns vielleicht überraschen, wie aggressiv unser Verhalten sein kann, wie viel Angst wir haben, wie ängstlich wir sind, ob wir die Wahrheit sagen oder nicht.“ Nach der geltenden Gesetzgebung ist es verboten, personenbezogene Daten ohne die Möglichkeit eines menschlichen Eingriffs zu verarbeiten.

Die Juristin Petra Molnar hat kürzlich die Auswirkungen von KI-Anwendungen auf die Kontrolle von Migrationsströmen untersucht. Sie war in Samos bei der Eröffnung des neuen geschlossenen Aufnahmezentrums. „Mehrere Schichten Stacheldraht, überall Kameras, Fingerabdruckstationen am Drehtor und den Ein- und Ausreisepunkten. Für die Flüchtlinge ist es wie ein Gefängniskomplex. Das werde ich nie vergessen. Am Vorabend der Eröffnung war ich in dem alten Lager in Vathi auf Samos. Wir sprachen mit einer jungen Mutter aus Afghanistan. Sie schob ihre kleine Tochter in einem Kinderwagen und tippte eilig eine Nachricht auf ihrem Telefon, in der stand: ‚Wenn wir dorthin gehen, werden wir verrückt.‘ Und jedes Mal, wenn ich mir die Lager mit diesen Systemen ansehe, wird mir klar, dass sie die Angst verkörpern, die Menschen haben, wenn sie isoliert und Überwachungstechnologien eingesetzt werden, um ihre Bewegungen weiter zu kontrollieren.“

Ärzte ohne Grenzen bezeichnete die neue Struktur in Samos als „dystopischen Albtraum“. Damit waren sie nicht allein. „Das KENTYROS-System zeichnet sich durch den Einsatz hochgradig eingreifender Technologien in den Schutz der Privatsphäre, personenbezogener Daten und anderer Rechte aus, wie z. B. Algorithmen zur Verhaltens- und Bewegungsanalyse, Drohnen und Überwachungskameras. Es besteht die ernsthafte Möglichkeit, dass die Installation der Systeme YPERION und KENTYROS gegen die Rechtsvorschriften der Europäischen Union über die Verarbeitung personenbezogener Daten und gegen die Bestimmungen des Gesetzes 4624/2019 verstößt“, so die NRO Homo Digitalis. Die Hellenic Human Rights Association, HIAS Greece, Homo Digitalis und ein Dozent der Queen Mary University of London, Dr. Niovi Vavoula, haben am 18. Februar 2022 bei der griechischen Datenschutzbehörde (DPA) einen Antrag auf die Ausübung der Untersuchungsbefugnisse und die Abgabe einer Stellungnahme zur Lieferung und Installation der Systeme gestellt. Am Mittwoch, dem 2. März 2022 leitete die Behörde eine Untersuchung des Ministeriums für Einwanderung und Asyl in Bezug auf die beiden fraglichen Systeme ein.

Der Automatisierungsfetisch

„Das Problem besteht darin, dass Behörden und Politiker beginnen, fortgeschrittene Datenanalysen als Faktoren für eine Art objektives und unvoreingenommenes Wissen über Sicherheitsfragen zu betrachten, weil sie diese Aura mathematischer Präzision haben. Künstliche Intelligenz und maschinelles Lernen können jedoch sehr genau die Vorurteile der Vergangenheit reproduzieren und verstärken. Wir sollten nicht vergessen, dass Daten von schlechter Qualität nur zu schlechten automatisierten, voreingenommenen Entscheidungen führen“, sagt der Forscher George Glouftios.

---

[1] Diese wurden zusammengefasst; vollständige Beschreibungen sind in der Finanzhilfevereinbarung enthalten.

[2] Zu Beginn des Projekts waren dies folgende Themen: (1) Einwilligung nach Aufklärung, (2) Kommerzialisierung von Daten und (3) Sicherheits- und Cybersicherheitsfragen.

[3] Verfügbar unter: http://guidelines.panelfit.eu/understanding-data-protection/

[4] Facebook-Post: 159 Personen erreicht; Erster Tweet: 811 Impressions, 2 Likes, 1 Retweet; Zweiter Tweet: 1.841 Impressions, 6 Likes, 7 Retweets; ECSA-Newsletter, Juli 2020: 438 Öffnungen (21,9 % der Abonnenten); ECSA-Mailingliste mit über 600 Einzelpersonen und Organisationen.

[5] Der PANELFIT-Leitfaden für verantwortungsvolle Forschung und Innovation enthält weitere Informationen für diese Gruppe.

[6] Art. 21 der Richtlinie 2013/33/EU (Neufassung der Richtlinie über Aufnahmebedingungen). Siehe: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/vulnerable-person_en

[7] Dieser Leitfaden konzentriert sich zwar auf Europa, aber viele der Arten von Schutzbedürftigkeit treten auch anderswo auf. Gleichzeitig gibt es weitere Ursachen und Arten von Schutzbedürftigkeit außerhalb Europas.

[8] So sind beispielsweise „Flüchtlinge“ eine schutzbedürftige Gruppe, „arm sein“ und „obdachlos sein“ dagegen eine Beschreibung des Zustands einer Person zu einem bestimmten Zeitpunkt und in einem bestimmten Kontext.

[9] Dies steht für lesbisch, schwul, bisexuell, transgender, queer, intersexuell und asexuell.

[10] Siehe: www.theguardian.com/world/2020/may/19/hungary-votes-to-end-legal-recognition-of-trans-people

[11] Die Samen sind das einzige europäische Volk auf der UN-Liste der indigenen Völker.

[12] Siehe: www.iwgia.org/en/sapmi.html

[13] Es gibt kostenlose Online-Tools, die eine Analyse der lichtempfindlichen Epilepsie durchführen; siehe z. B. www.w3.org/TR/WCAG20-TECHS/G15.html; auf der Website von Mozilla gibt es auch einen Abschnitt über barrierefreie Lösungen für Entwickler: https://developer.mozilla.org/en-US/docs/Web/Accessibility/Seizure_disorders