Kompetenzzentrum
Öffentliche IT

FORSCHUNG FÜR DEN DIGITALEN STAAT

DATENACHTSAMKEIT – EIN NEUER(LICHER) BLICK AUF DEN SELBSTDATENSCHUTZ

Selbstdatenschutz bezeichnet Maßnahmen, die Bürger:innen ergreifen können, um ihre Daten und damit sich selbst zu schützen. Die Ermöglichung und Wahrung dieser Selbstbestimmung ist für unsere Gesellschaft wichtig. Das grundlegende Instrument zum Schutz von Privatheit ist Datenschutzregulierung. Da die Entwicklung von Technik und Geschäftsmodellen aktuell dynamischer voranschreitet als eine effektive Datenschutzregulierung, sind zusätzliche Möglichkeiten zur digitalen Selbstverteidigung unverzichtbar. Wir erläutern hier, warum die Förderung und rechtliche Garantie von Maßnahmen zum Selbstdatenschutz notwendig sind.

1. Nutzer:innen kommunizieren über Werbenetzwerke

Die überwiegende Mehrheit digitaler Informations- und Kommunikationsangebote ist werbefinanziert. Da die Werbetreibenden nach möglichst individuellen Werbeformen suchen, ist die Nutzung dieser Angebote mit einer umfassenden Auswertung von Nutzerdaten verbunden. Datenbasierte Profile ermöglichen den Zuschnitt von Inhalten, führen aber zur Bildung von Teilöffentlichkeiten.

2. Komfort macht Nutzer:innen verwundbar

Das Web ist von einem einfachen Informationssystem zu einer universellen Bedienoberfläche im Alltag geworden. Immer mehr Dienste werden ohne Kenntnis der Nutzer:innen personalisiert. Das soll das Nutzungserlebnis verbessern. Dabei ist oftmals unklar, was alles mit den Daten passiert.

3. Datenachtsamkeit ist unverzichtbar

Der Umgang mit den eigenen Daten im Netz erfordert eine bewusste Abwägung von Nutzen und möglichen Konsequenzen. Auf der einen Seite gibt es einfache Strategien, um die Spuren im Web zu minimieren, wie z. B. Datensparsamkeit und Unterbrechung von Kontinuität. Auf der anderen Seite steht eine Entscheidung zugunsten von Komfort und Nutzbarkeit. Datenachtsamkeit lädt dazu ein Gewohnheiten im Umgang mit Daten regelmäßig zu hinterfragen und neue Routinen zu etablieren.

4. Pseudonyme trennen digitale Rollen und Kontexte

Für die Wiedererkennung von Personen reicht oft das Zusammenführen weniger Datenpunkte aus. Über die Nutzung verschiedener Pseudonyme wird die Verknüpfung von Daten erschwert. Zugleich drückt sich darin der Nutzerwille aus, unterschiedliche Rollen und Informationskontexte voneinander zu trennen.

5. Verschlüsselung von Anfang an

Verschlüsselung ist ein Schutzmechanismus, der den Zugriff auf Daten einschränkt und die Vertraulichkeit von Daten und Information gewährleistet. Verschlüsselung muss ein obligatorischer Bestandteil eines Internetdienstes auf Stand der Technik sein. Nachträglich hinzugefügt schöpft Verschlüsselung ihr Potential nicht aus – wenn sie denn überhaupt genutzt wird.

6. Datenachtsamkeit braucht informierte Bürger:innen – und einen fördernden Staat

Nicht jede Organisation geht mit den Daten von Bürger:innen verantwortungsvoll um. Mit Datensparsamkeit, der Unterbrechung von Kontinuität, der Nutzung von verschlüsselten Diensten und Pseudonymen stehen den Bürger:innen generell wirksame, alltagstaugliche und zukunftssichere Strategien zum Schutz ihrer Daten zur Verfügung. Der Staat muss diese Maßnahmen ermöglichen und aktiv fördern und dadurch den Machtausgleich zwischen Organisationen und Nutzer:innen weiter voranbringen.

SELBSTDATENSCHUTZ – UNIVERSELL RELEVANT

Die Grundidee des Selbstdatenschutzes gibt es nicht erst seit der Digitalisierung und dem modernen Datenschutz. Verschleierungstechniken wie die Verwendung von Pseudonymen sind für Künstler:innen und Schriftsteller:innen eine alte Kulturtechnik, die u. a. dazu dient, die Zuordnung bestimmter Informationen zu einer natürlichen Person zu erschweren oder zu verhindern. In einer riskanten Gegenwart oder ungewissen Zukunft kann so die individuelle Sicherheit erhöht werden. Natürlich wurden Verschleierungstechniken auch immer schon von Personen eingesetzt, die sich vor einem legitimen Strafverfolgungsinteresse der Allgemeinheit schützen wollten. Das Thema Selbstdatenschutz bewegt sich in diesem Spannungsfeld zwischen legitimen und illegitimen Interessen. Für die digitale Welt geht es darum, die erzielten Güterabwägungen zu diesem Konflikt aus dem Analogen zu übertragen.

Datenschutz und Selbstdatenschutz sind unterschiedliche Ansätze mit einem gemeinsamen Ziel. Das Bundesverfassungsgericht etablierte 1983 das Recht auf informationelle Selbstbestimmung, wonach das unkontrollierte Erheben, Verarbeiten, Speichern und Weitergeben von personenbeziehbaren Daten Menschen in ihrer Selbstbestimmung einschränken. Es wurde argumentiert, dass die Unklarheit darüber, wer wann welche Informationen über die eigene Person hat, zu Verhaltensanpassungen führen kann. Entsprechend würden nicht nur die individuellen Entfaltungschancen beeinträchtigt, sondern auch das Gemeinwohl, da die Möglichkeit zu selbstbestimmtem Handeln die Grundlage für die Mitwirkungs- und Handlungsfähigkeit der Bürger:innen am Gemeinwesen bilde.

Mit der Charta der Grundrechte der Europäischen Union wurde dieses implizite Grundrecht EU-weit explizit verankert und jüngst durch die Datenschutzgrundverordnung (DSGVO) ausgestaltet. Ein Kernprinzip dieses Datenschutzrechts ist der Einwilligungsvorbehalt. Dieser stellt eine Art Brücke zwischen dem Datenschutzrecht und dem Selbstdatenschutz dar. Das Datenschutzrecht reguliert das Verhältnis zwischen den Daten verarbeitenden Organisationen (Internetfirmen, Plattformen, Dienstanbietern u. a. sowie dem Staat selbst) und den Betroffenen. Es zielt darauf ab, die vorhandene Machtasymmetrie auszugleichen.

Beim Selbstdatenschutz geht es darum, die Rechte an den eigenen Daten wahrzunehmen und über ihre Weitergabe selbstbestimmt zu entscheiden. Selbstdatenschutz baut entsprechend auf Datenschutzregulierungen auf, geht aber über diese hinaus und ergänzt sie. Dort, wo die Rechtmäßigkeit der Datenverarbeitung an eine Einwilligung gebunden ist, ist ein bewusster Selbstdatenschutz sogar Voraussetzung für die Wirksamkeit der Datenschutzregulierung. Im Kontext immer datenintensiverer Technologien und Anwendungen kommt gerade dieser Verbindung eine steigende Bedeutung zu.

Die Wirkung der bestehenden Datenschutzarchitektur ist im Hinblick auf den tatsächlichen Schutz persönlicher Daten begrenzt. Der Einwilligungsvorbehalt verliert an Wirksamkeit, wenn die Zustimmung zur Datenverarbeitung zu einer unhinterfragten Routine wird. Das gilt insbesondere für verbreitete Dienste, die aus Sicht der Einzelnen für eine soziale Teilhabe notwendig sind und die ihre Nutzung an umfassende, nur begrenzt modifizierbare Verarbeitungsrechte knüpfen. Kritisch ist auch, dass die Verknüpfung von Daten sowohl durch Betreiber als auch neugierige Einzelne aufgrund derzeitig dominierender IT-Architekturen und Dienste erleichtert wird. Internetfirmen sammeln und verwerten Daten in industriellem Ausmaß. Wenn beispielsweise eine Pseudonymisierung durch das Verknüpfen verschiedener Profile aufgehoben werden kann, verfehlt ein Recht auf Pseudonymisierung, wie es in § 13 Abs. 6 Telemediengesetz verankert ist, seinen Zweck. Eine Lösung hierfür wäre, die rechtliche Datenschutzarchitektur mit der technischen zu verknüpfen und Dienste mit datenschutzfreundlichen Grundeinstellungen zum Standard zu machen. Es gibt eine Reihe solcher Privacy-Enhancing-Technologies (PETs; siehe Kasten), die Datenspuren vermeiden oder zumindest verringern sowie anonyme oder verkettungssichere Kommunikation über das Internet ermöglichen. Diese technischen Lösungen bringen für den praktischen Einsatz Limitierungen mit sich und bedürfen für ihre Wirksamkeit rechtlicher Garantien.

Dieser Impuls zielt darauf ab, ein Grundverständnis für die Relevanz von Selbstdatenschutz zu ermöglichen und universelle Prinzipien vorzustellen, auf denen ein effektiver Selbstdatenschutz aufbaut. Gesetzliche Regulierung unterstützt und garantiert diesen notwendigen Machtausgleich zwischen Nutzer:innen und Daten verarbeitenden Organisationen.

1. NUTZER:INNEN KOMMUNIZIEREN ÜBER WERBENETZWERKE

Das Internet zeichnet sich durch ein breites und vielfältiges Angebot an Informations- und Kommunikationsdiensten aus. Viele Angebote sind für Nutzer:innen kostenfrei, obwohl ihre Bereitstellung teils mit großem Aufwand verbunden ist. Diese Diskrepanz wird durch die Monetarisierung von Nutzerdaten aufgelöst. Manche Daten sind für die Funktionalität bestimmter Angebote notwendig. Es werden aber regelmäßig mehr Daten erhoben, als für das Kernangebot notwendig wäre. Dazu zählen auch solche Daten, die (bei ihrer Verknüpfung) unerwünschte Rückschlüsse auf die Nutzer:innen ermöglichen. Hinzu kommt, dass auch in ihrem initialen Kontext notwendige Daten oft losgelöst von ihrem ursprünglichen Zweck weiterverwertet werden. Die vielfältigen Verwertungsmöglichkeiten von Daten machen deren Erfassung für Dienstanbieter besonders interessant. Hervorzuheben sind in diesem Zusammenhang die Weitervergabe von Daten an Dritte und der Datenhandel.

Die meisten Daten werden für Werbezwecke erhoben. Dabei geht es auf der einen Seite darum, Werbeangebote zielgruppengerecht zuzuordnen, und auf der anderen Seite darum, die eigenen Angebote entsprechend anzupassen. Im Wettstreit der Websites um die Zeit der Nutzer:innen wird durch Personalisierung Aufmerksamkeit gebunden. Längere Aufmerksamkeit bedeutet eine höhere Anzahl an schaltbarer Werbung und gleichzeitig wird wiederum die Menge an generierten Daten gesteigert. Vereinfacht gesagt: Nutzer:innen kommunizieren über Werbenetzwerke.

Das möglichst zielgerichtete Zuschneiden von Informationen, Angeboten und Werbung war im Marketing und PR-Bereich bereits vor der Digitalisierung üblich (Microtargeting). Wichtige Werkzeuge in diesem Zusammenhang sind diverse Formen von Empfehlungssystemen. Ihnen liegt die Annahme zugrunde, dass Personen sich anhand von verfügbaren Indikatoren nach ihren Interessen und Präferenzen gruppieren lassen. Aus der Auswertung vorherigen Nutzerverhaltens lassen sich Empfehlungen generieren, auf die mit einer höheren Wahrscheinlichkeit (durch einen Klick, einen Kauf oder anderweitigen Konsum) reagiert wird. Die aufgrund der schieren Menge an Daten mögliche Feinauflösung erzeugt so im Hinblick auf das Konsumverhalten ein Manipulationspotenzial, das in vordigitalen Zeiten undenkbar war.

Nach ähnlichen Prinzipien funktioniert auch die personalisierte Auswahl von Informationsangeboten, die auch in anderen Bereichen (wie Politik und Gesellschaft) Anwendung findet. Hier wird eine Gefahr sichtbar: Werden den Nutzer:innen nur solche Informationen gezeigt, die ihren Interessen und ihrem bislang gezeigten Verhalten entsprechen, treffen sie seltener auf Inhalte, die ihren Positionen widersprechen oder die neu für sie sind. So entstehen Filterblasen, denen zugeschrieben wird, die gesellschaftliche Polarisierung zu befördern.

Es ist notwendig, Bürger:innen zu ermächtigen, ihre für konkrete Zwecke freigegebenen Daten dauerhaft kontrollieren zu können. Die hierfür erforderliche Möglichkeit der expliziten Datenfreigabe besteht derzeit nur eingeschränkt. So haben beispielsweise Versuche von Browser- und Plug-In-Herstellern, vor ungewollter Datensammlung zu schützen, hauptsächlich ein technisches Wettrüsten zwischen ihnen und den Betreibern werbefinanzierter Angebote ausgelöst.

Hier könnte »*Ihre*« Werbung stehen

Personen, die diesen Impuls gelesen haben, interessierten sich auch für

Anonymisierung

Internettracking

2. KOMFORT MACHT NUTZER:INNEN VERWUNDBAR

Das Web und Smartphones sind inzwischen universelle Bedienoberflächen für unseren Alltag geworden. Wir informieren uns online über die neuesten Nachrichten, nutzen Echtzeit-Routenplanung für Verkehrsmittel oder steuern Funktionen unserer Wohnung über Clouddienste. Mit dem Smartphone haben sich Reichweite und Komfort dieser Funktionen weiter gesteigert und endgültig durchgesetzt. Zur Kehrseite dieser Entwicklungen gehören umfangreiche Datensammlungen und Bewegungsprofile. Oftmals ist unklar, welche Informationen aus ihnen oder ihrer Verknüpfung gewonnen werden und welche Auswirkungen dies für die Nutzer:innen hat. Im schlimmsten Fall werden sie angreifbar, wenn Daten unerwünschte Rückschlüsse ermöglichen (z. B. Daten von Gesundheitsplattformen).

Viele digitale Funktionen werden erst durch Anpassung an unsere Lebensumstände nutzbar. In jedem Fall macht die Personalisierung von Diensten ihre Nutzung komfortabler. Dabei entstehen aber auch Nutzerprofile, die viel über uns verraten. Geschieht das für uns transparent, so können wir uns gezielt damit auseinandersetzen und Vertrauen aufbauen. Wichtig ist, das Geschäftsmodell zu verstehen: Zahlen Nutzer:innen (auch) mit ihren Daten? Und was passiert eigentlich mit den Daten, wenn das Geschäftsmodell geändert oder der Dienst verkauft wird?

Ein Dilemma wird sichtbar: Einerseits möchten Nutzer:innen kostenfreie Angebote in Anspruch nehmen und sind möglicherweise dafür bereit, mit ihren Daten zu zahlen. Als Datenspender:innen können Nutzer:innen dazu beitragen, Angebote zu verbessern oder überhaupt erst zu ermöglichen (bspw. Stauerkennung auf Basis von Mobilitätsdaten). Andererseits werden Nutzer:innen immer gläserner, wenn sie ihre Daten und Nutzerprofile nicht unter Kontrolle behalten können.

Um zu verstehen, wie bei der Webnutzung Daten gesammelt werden können, muss man die Technik betrachten: Inhalte auf Webseiten stammen aus verschiedenen Quellen und Zugriffe auf das Web sind zunächst zustandslos, d. h. der Aufruf einer Webseite ist unabhängig vom Aufruf davor. Soll jedoch eine Webseite auf vorherigen Aktionen basieren (bspw. beim Füllen eines Warenkorbs), so muss der aktuelle Zustand mitgeführt werden, zum Beispiel durch einen individualisierten Weblink oder ein Cookie.

Tracking nutzt diese und andere Mechanismen zur Sammlung von Aktivitätsdaten: Über einen personalisierte Weblink kann erkannt werden, welche Wirkung eine E-Mail-Kampagne entfaltet, und ein Cookie kann verraten, für welche Themen-Webseiten wir uns interessieren. Damit ermöglicht es personalisierte Suchergebnisse und Werbung und erleichtert die Monetarisierung der Daten. Problematisch ist, dass die meisten Tracking-Methoden nur schwer erkannt werden können und damit auch schwer zu kontrollieren sind. Cookies werden im Browser gespeichert, unsichtbare Elemente auf der Webseite oder gezielt eingebaute Tracker von Werbenetzwerken sind auf den ersten Blick nicht zu erkennen und nur über Mechanismen des Browsers und Erweiterungen wie Werbeblocker zu kontrollieren. Das ÖFIT-White-Paper »Internettracking« erläutert die technischen Details.

Eine neuere Variante des Trackings bietet die Werbe-ID. Diese wird dem Endgerät oder dem Nutzerkonto automatisch zugeteilt und stellt ebenfalls eine Personalisierung dar, die zur Profilbildung in Werbenetzwerken dient. Allerdings ist sie für die Nutzer:innen sichtbar und bietet daher Einflussmöglichkeiten.

Privacy-Enhancing-Technologies (PETs) beruhen auf den Grundsätzen von Daten- und Selbstdatenschutz, wie Datensparsamkeit, Pseudonymisierung, Unterbrechung von Kontinuität und integrierte Verschlüsselung. Diese Prinzipien können bereits im Design von IT-Systemen bzw. Diensten berücksichtigt werden (Privacy by Design) und als datenschutzfreundliche Einstellungen in Diensten vorgegeben werden (Privacy by Default). Eingesetzt werden PETs beispielsweise bei Browsern, die spurenarmes Surfen unterstützen (derzeit z. B. Firefox), datenschutzfreundlichen Suchmaschinen, die keine personenbezogenen Informationen sammeln oder teilen, nicht nachverfolgen und kein Profil anlegen (derzeit z. B. Startpage oder DuckDuckGo), und schließlich Messengerdiensten und E-Mail-Anbietern, die nur technisch erforderliche personenbezogene Daten erheben.

3. DATENACHTSAMKEIT IST UNVERZICHTBAR

Die informationelle Selbstbestimmung wird folglich in vielen Bereichen neu herausgefordert. Bürger:innen können durch Datenachtsamkeit Schutzroutinen entwickeln und so diesen Herausforderungen begegnen. Dies geschieht über eine bewusste Abwägung der Angemessenheit einzelner Schutzmaßnahmen für konkrete Kontexte. Neben den Chancen, die sich in vielen Bereichen der Gesellschaft, wie z. B. in der Verwaltung, in Forschung und Entwicklung oder in bestimmten Alltagsanwendungen, aus dem sinnvollen Einsatz von Daten ergeben können, birgt eine unautorisierte Datenweitergabe Risiken für die Einzelnen ebenso wie für die Gesellschaft als Ganzes. Bei jeder Datenweitergabe stehen den individuellen Zwecken oder den damit verfolgten Gemeinwohlinteressen die Risiken von Privatheitsverletzungen und Datenmissbrauch gegenüber. Die Unterscheidung »gute Daten, schlechte Daten« kann dabei bezogen auf die Verwendung nur kontextabhängig getroffen werden. Der Ethik-Kodex aus der »Hackerszene« nimmt seit den 1980ern hierauf Bezug und fordert: »Öffentliche Daten nützen, private Daten schützen«.

Die hier beschriebenen Prinzipien des Selbstdatenschutzes sind universell gültig und folgen dem Grundsatz der Datenachtsamkeit. Sie sind eng miteinander verbunden und können entweder ergänzend oder alternativ zueinander eingesetzt werden.

Datensparsamkeit ist einerseits ein Gestaltungsprinzip für Dienste und Anwendungen. Übertragen auf einzelne Nutzer:innen heißt das andererseits: Es sollten immer nur die personenbezogenen Angaben gemacht werden, die für die jeweilige Anwendung unbedingt erforderlich sind. Die Reduzierung der Daten zielt ab auf optionale Angaben (z. B. in Formularen oder beim Anlegen von Benutzerprofilen) und die Vermeidung verzichtbarer Daten sammelnder Dienste (z. B. auf die Teilnahme an Gewinnspielen).

Datensparsamkeit lässt sich u. a. durch die Modifikation von Browser-, App- und Geräteeinstellungen erreichen (z. B. die Deaktivierung der Standortbestimmung oder der Kamera- bzw. Mikrofonfunktionen). Damit kann verhindert werden, dass bestimmte Daten ohne Zustimmung verarbeitet werden können. Die Änderungen können im Bedarfsfall wieder rückgängig gemacht werden. Die Modifikation von Browsereinstellungen (z. B. eine differenzierte Einwilligung zu Cookies) erfordert jedoch ein gutes Allgemeinverständnis für die Funktionalität der Anwendung. Auch erfahrene Nutzer:innen stoßen hier schnell an ihre Grenzen. Datenachtsamkeit allein kann Tracking nicht verhindern (z. B. die Weitergabe von Daten an Facebook durch das bloße Laden des Like-Buttons, der auf vielen Websites eingebettet ist, und unabhängig davon, ob die Nutzer:in über ein Facebook-Profil verfügt). Lässt sich die Nutzung von Diensten nicht vermeiden, so besteht seit Inkrafttreten der DSGVO die Möglichkeit, eigene Daten im Nachhinein löschen zu lassen.

Eine zweite wichtige Säule des Selbstdatenschutzes ist die Unterbrechung von Kontinuität. Durch die Modifikation von Einstellungen und andere Maßnahmen werden Verknüpfungsmöglichkeiten von personenbezogenen Daten verringert. Das regelmäßige Löschen von Cookies ist eine einfache Möglichkeit, die Bezüge zu vergangenem Verhalten zu unterbrechen. Dasselbe gilt für das Zurücksetzen der Werbe-ID. Hiermit wird der Bezug zu einem Nutzungsprofil und den bis dahin gesammelten Daten gekappt. Allerdings werden auf diesem Wege nicht die Daten selbst gelöscht, sondern die bestehende Verknüpfung zur Datensammlung beendet und ein neues Profil angelegt. Nutzer:innen erhalten so ein wenig Kontrolle über ihre Daten zurück.

Kontinuität kann auch durch den Wechsel zwischen Webbrowsern für verschiedene Aktivitäten unterbrochen werden. Dabei ist jedoch zu beachten, dass es große Unterschiede in der Datenschutzfreundlichkeit der Konfigurierung von Browsern gibt. Es können aber auch Browsererweiterungen wie Werbeblocker und andere Plug-ins genutzt werden, die Schutzfunktionen bieten.

Datensparsamkeit kann auch durch die Entscheidung für Dienste mit PETs (siehe Kasten) erreicht werden. Nicht alle Angebote sind im Gegensatz zu Daten sammelnden Diensten kostenfrei. Bei der Entscheidung für oder gegen kostenpflichtige Dienste ist es für Bürger:innen generell schwierig, die versteckten Langzeitkosten von kostenfreien Angeboten einzuschätzen, z. B. wenn Werbeprofile zu personalisierten und intransparenten Preisen von beworbenen Produkten führen. Mittlerweile haben auch die großen Internetkonzerne Privatheit für sich als Wettbewerbsstrategie entdeckt und bieten vereinzelt spurenarme Dienste als Serviceleistung an. Es ist allerdings nicht zu erwarten, dass Technologieunternehmen aus Selbstverpflichtung Datenschutzinteressen nachkommen, solange die Nutzung dieser Daten zum Kern ihres Geschäftsmodells gehört.

4. PSEUDONYME TRENNEN DIGITALE ROLLEN UND KONTEXTE

Die Verwendung von Pseudonymen bei der Nutzung von Diensten ist eine weitere Strategie, um Verknüpfungsmöglichkeiten von Daten zu verringern und Kontinuität zu unterbrechen. Pseudonyme sind damit ein Gegenentwurf zu Versuchen, das Individuum vollständig zu erfassen. Sie ermöglichen Nutzer:innen, verschiedene Rollen und Kontexte im Netz voneinander zu trennen. Die Entscheidung für ein Pseudonym kommt damit einer Willenserklärung gleich, Datenräume bewusst voneinander trennen und Daten im Sinne der informationellen Selbstbestimmung zweckgebunden nutzen zu wollen.

Pseudonymisierung kann an verschiedenen Stellen ansetzen. Bei der Selbst-Pseudonymisierung wird der Klarname durch ein Pseudonym ersetzt. Durch die Wahl des Pseudonyms können die Nutzer:innen selbst steuern, welche Rückschlüsse sie zulassen möchten und welche nicht. Beispielsweise kann das Pseudonym Alter oder Wohnort offenlegen oder überhaupt keine Rückschlüsse auf die konkrete Person ermöglichen.

Einsatzmöglichkeiten bestehen bei der Einrichtung pseudonymer Accounts zur Nutzung von Diensten (wie in öffentlichen Internetforen) ebenso wie für die private Kommunikation via Messenger oder E-Mail. Nutzer:innen können durch die Verwendung verschiedener Pseudonyme Kommunikationskontexte trennen, wie es beispielsweise bereits für die Separation von privater und beruflicher Kommunikation üblich ist. Durch eigene Beiträge lässt sich unter verschiedenen Nutzernamen Reputation aufbauen, ohne die Rollen und Kontexte miteinander verknüpfen zu müssen oder partiell die eigene Identität (z. B. Geschlecht, ethnischer Hintergrund oder Religion) preiszugeben. Das erschwert den Daten verarbeitenden Organisationen eine umfängliche Profilbildung. Pseudonymisierung kann auch durch die Entscheidung für PETs (siehe Kasten) erreicht werden. Mit der Pseudonymfunktion des elektronischen Personalausweises wurde eine datenschutzfreundliche Implementierung durch den Staat zur Verfügung gestellt. Pseudonyme können auch von Treuhandsystemen verwaltet werden, die eine Beziehung zwischen Nutzer:innen und einer dritten Partei herstellen. Auch bei qualifizierten elektronischen Signaturen, wie sie z.B. im E-Commerce verwendet werden und die über einen unverwechselbaren Signaturschlüssel Rechtssicherheit herstellen, können Pseudonyme verwendet werden.

Die Wirksamkeit von Pseudonymen hängt davon ab, ob und wie die Daten durch Einstellungen in Endgeräten, Kommunikationsnetzen und bei Dienstanbietern miteinander verknüpft werden und für wen eine Zuordnung zu anderen Referenzdaten und Profilen möglich ist. Dies muss u. a. im Zusammenhang mit anderen Identifikatoren gesehen werden (Login, Browsereinstellungen, Cookies oder JavaScript).

Die Strafverfolgung im Internet ist nach wie vor ein Hauptkritikpunkt gegen Pseudonyme, wie sich in der Diskussion um die Klarnamenpflicht zeigt. Bei wiederkehrenden Vorfällen, wie Hasskommentaren oder Betrugsversuchen, wird regelmäßig auf den Abbau von Hemmschwellen durch den Schutz vermeintlicher Anonymität verwiesen. Pseudonyme schützen allerdings auch vor politischer Verfolgung. Die Gesetzeslage sieht bereits jetzt vor, dass Pseudonyme im Prozess der Strafverfolgung natürlichen Personen zugeordnet werden können müssen. Technisch können Pseudonyme von den Internetanbietern oder großen Plattformen bereits jetzt wirksam aufgelöst werden. Eine gesetzliche Verschärfung erscheint demnach unnötig und wäre gegen das Prinzip der informationellen Selbstbestimmung abzuwägen.

Auch das kürzlich veröffentlichte Gutachten der Datenethikkommission misst der Pseudonymisierung eine hohe Bedeutung bei und spricht sich sogar für strafbewehrte Verbote von De-Anonymisierung aus.

Darüber hinausgehende Möglichkeiten des technischen Selbstdatenschutzes (wie die weitgehende Anonymisierung von Internetdiensten) setzen deutlich höhere digitale Kompetenzen und ein optimales Zusammenwirken von Endgeräten, Kommunikationsnetzen und Dienstanbietern voraus. Mehr Informationen über die Re-Identifizierbarkeit anonymisierter Daten durch die Kombination von Datenpunkten aus verschiedenen Datenbeständen finden sich im ÖFIT-White-Paper »Anonymisierung – Schutzziele und Techniken«.

5. VERSCHLÜSSELUNG VON ANFANG AN

Verschlüsselung verhindert, dass digitale Inhalte durch unautorisierte Dritte gelesen und ausgewertet werden können. Damit wird sie zum Werkzeug für den Selbstdatenschutz: Erforderliche Daten werden gegen unbefugte Zugriffe oder Auswertungen geschützt. Ziel ist nicht nur die Wahrung der Vertraulichkeit der Information selbst, sondern auch die Vertraulichkeit des Zugriffs auf eine Information (bspw. Verhindern von Rückschlüssen aus dem Besuch von Webseiten).

Neben der individuellen Verschlüsselung von Datenträgern spielt die Verschlüsselung von Kommunikation eine wichtige Rolle. Für die verschlüsselte Übertragung ist zuvor ein Austausch von Schlüsseln notwendig. Asymmetrische Verschlüsselung macht diesen Vorgang auch ohne direkten vorherigen Kontakt und damit im großen Maßstab praktikabel: Ein öffentlicher Schlüssel kann verteilt werden und wird zur Verschlüsselung der Nachricht (z. B. von E-Mail-Inhalten) verwendet. Entschlüsselt werden kann die Nachricht nur mit dem dazugehörigen privaten Schlüssel, der ausschliesslich beim Empfänger verbleibt. Die dahinter stehenden technischen Prozesse sind idealerweise vor den Nutzer:innen verborgen.

Für die Alltagspraxis kann man davon ausgehen, dass zeitgemäße Verschlüsselung nicht gebrochen werden kann. Da die Übertragungsstrecke geschützt ist, rücken die Endpunkte in den Mittelpunkt der Betrachtung. Bei einer Ende-zu-Ende-Verschlüsselung gibt es keine weiteren Systeme auf dem Kommunikationsweg, die die Kommunikation zwischenzeitlich vollständig entschlüsseln. Nur bei einer Verschlüsselung am Anfang des Kommunikationswegs ist sichergestellt, dass es keine zusätzlichen kryptografischen Schwachpunkte gibt. Andererseits müssen in diesem Fall die Endpunkte der Kommunikation ihrerseits besonders geschützt werden. Damit wird klar, dass Verschlüsselungsfunktionen eine ganzheitliche Systembetrachtung verlangen.

Trotz Skandalen und Informationskampagnen setzt sich Verschlüsselung als individuelle Maßnahme zum Selbstdatenschutz nicht durch. Insbesondere die eigenständige oder nachträglich hinzugefügte Verschlüsselung bei Speicherung und Übertragung von Daten wird wenig genutzt. Der Aufwand ist hoch und setzt bei der Übertragung von Daten die Mitwirkung anderer voraus. So sind z. B. seit Langem einfach zu nutzende Erweiterungen zur klassischen E-Mail verfügbar, die jedoch im Alltag allenfalls im professionellen Umfeld genutzt werden. Verschlüsselung ist in der Breite dort als Strategie durchschlagskräftig, wo sie von Anfang an integraler und standardmäßig genutzter Bestandteil des Angebots ist. Praktisch alle Messenger-Anwendungen und Webangebote nutzen heute verschlüsselten Datentransport.

Selbstdatenschutz bedeutet also im Bereich Verschlüsselung für die Nutzer:innen vor allem die Auswahl der richtigen Produkte, die standardmäßig verschlüsseln und komfortabel nutzbar sind. Sie müssen ein durchdachtes Sicherheitskonzept ohne Hintertüren aufweisen und vor allem auch kurzfristig auf (nahezu unvermeidliche) Sicherheitslücken reagieren können. Da diese Sicherheitsmaßnahmen für Laien schwer einzuschätzen sind, müssen die Nutzer:innen Anbietern und Produkten vertrauen können. Schon kleinere gesetzliche Einschränkungen der Sicherheit von Verschlüsselung können diese Schutzmöglichkeiten drastisch reduzieren.

Weiterführende Informationen:

Allgemeine Sicherheitsthemen: www.bsi-fuer-buerger.de

Sichere Nutzung von Smartphone und Tablet: www.mobilsicher.de

Überblick über Datenschutzaufsichtsbehörden: www.stiftungdatenschutz.org/aufsichtsbehoerden

Aufbereitung für Kinder, Jugendliche, Eltern und Pädagog:innen: www.klicksafe.de, www.youngdata.de

Vereine und Initiativen, die Selbstdatenschutzmaßnahmen fördern: www.digitalegesellschaft.de, www.selbstdatenschutz.info, www.digitalcourage.de, www.cryptoparty.in

Differenziert nach Nutzergruppen: www.sicher-im-netz.de

Zur technischen Vertiefung: www.privacy-handbuch.de

6. DATENACHTSAMKEIT BRAUCHT INFORMIERTE BÜRGER:INNEN – UND EINEN FÖRDERNDEN STAAT

Digitale Datenspuren bergen nicht nur Risiken, sondern auch Chancen. Die Notwendigkeit einer Abwägung darüber ist nicht neu, wird aber kontinuierlich vor neue Herausforderungen gestellt. Aktuell dienen Daten vorwiegend als Rohstoff für Geschäftsmodelle, sie können – richtig genutzt – aber auch der Allgemeinheit zugute kommen.

Mit den im Impuls beschriebenen Maßnahmen zum Selbstdatenschutz – Datensparsamkeit, Unterbrechung von Kontinuität und Nutzung von Pseudonymen – stehen den Bürger:innen generell wirksame, alltagstaugliche und zukunftssichere Strategien zur Verfügung. Der Staat sollte diese Handlungsmöglichkeiten rechtlich garantieren und aktiv fördern.

Damit mehr Bürger:innen diese Strategien der Datenachtsamkeit in der Zukunft gezielt einsetzen, braucht es:

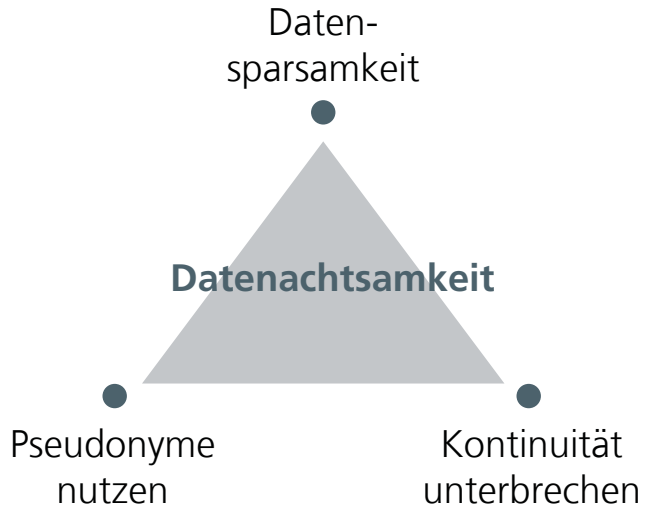
- Aufklärung über die Zusammenhänge der Datenverwertung
- Informationen über Selbstdatenschutzstrategien
- Hinweise auf datenschutzfreundliche Technologien

Voraussetzungen für Selbstdatenschutz sind:

- Ausbau digitaler Bildungsangebote und Aufklärungskampagnen für alle Altersgruppen
- Förderung datenschutzfreundlicher Technologien (z. B. wirksamer Verschlüsselung)
- Rechtliche Gewährung und Unterstützung digitaler Selbstbestimmung

Informationelle Selbstbestimmung ist Schutzpflicht des Staates. Im Kontext komplexer internetbasierter IT-Systeme und -Anwendungen lässt sich die Idee eines freiheitlich-demokratischen Gemeinwesens nur dann verwirklichen, wenn der Staat die Voraussetzungen hierfür schafft. Das Datenschutzrecht bleibt das zentrale Instrument für den Machtausgleich zwischen Organisationen und Bürger:innen und für den Schutz von Informationskontexten. Die DSGVO ist hierfür ein aktuelles Beispiel. Gleichzeitig sollten den Bürger:innen weiterhin angemessene Handlungsmöglichkeiten zum Selbstdatenschutz eingeräumt werden Das gilt insbesondere für die Bereiche, in denen der Schutz der informationellen Selbstbestimmung (noch) nicht ausreichend gewährleistet ist.

Die Möglichkeiten des Selbstdatenschutzes dürfen jedoch nicht zu einer Verlagerung der Verantwortlichkeit des Staates auf den Einzelnen führen. Datenachtsamkeit ist eine wirksame Strategie gegen die unerwünschte Nutzung von Daten, reicht jedoch für eine umfassende Garantie der informationellen Selbstbestimmung nicht aus. Datenachtsamkeit ist nur gemeinsam mit unterstützender Datenschutzregulierung wirksam.



Autor:innen
Dr. Karoline Krenn, Jens Tiemann,
Simon Sebastian Hunt
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

Gefördert durch:
Bundesministerium des Innern, für Bau und Heimat

Fraunhofer FOKUS

Foto: pixabay, nvtrlab [kre 1019]