DRITTER GLEICHSTELLUNGSBERICHT

# Daten und Grundrechte

**Themenblatt 13**

## Datensammlung und Diskriminierung

Können Sie sich noch ein Leben ohne Smartphones oder Internet vorstellen? Kontakte zu Freund∗innen halten, online einkaufen, Filme anschauen, auf Stellen bewerben, Wohnungen suchen. Bei allen Aktivitäten im Netz, besonders in den Sozialen Medien, werden Daten über unser Verhalten gesammelt: Was geben wir in Suchfelder und Formulare ein? Was klicken wir an? Was schauen wir wann von welcher Rechneradresse wie lange an?

Es gibt inzwischen viele Gesetze und technische Vorkehrungen, um das unkontrollierte Datensammeln zu minimieren: Wir können als Nutzer∗innen Cookies ablehnen, mit deren Hilfe Werbetreibende auf Webseiten erkennen können, ob ein bestimmter Rechner schon mal auf der Webseite war, wo er vorher war oder was angeklickt wurde; Webseiten mit Kontaktformularen müssen verschlüsselte Internetverbindungen nutzen, damit Dritte die Verbindung nicht mitlesen können; Anbieter∗innen sozialer Plattformen müssen Passwörter verschlüsselt abspeichern.

Solche Regeln sind nötig, da die Möglichkeiten, zu allen möglichen Zwecken riesige Datenmengen über Menschen zu sammeln und auszuwerten, bei Staat, privaten Unternehmen oder Individuen immer neue Begehrlichkeiten für die Verwendung dieser Daten, u. a. für Kontrolle und Überwachung wecken. Die unkontrollierte Sammlung und Verwendung von Daten kann zudem zu Diskriminierung, Ausgrenzung und neuen Formen der Gewalt führen:

- Lesben, Schwule, Bisexuelle, trans- und intergeschlechtliche Menschen (LSBTI) werden in Sozialen Medien wie YouTube und TikTok häufig Opfer von Diskriminierung. TikTok zensierte etwa Hashtags, die auf LSBTI-Themen schließen ließen. Videos von LSBTI-Künstler∗innen wurden auf YouTube mehrfach gesperrt, weil automatische Filter sie als gefährlich oder anstößig markierten. Die so entstandene Ausgrenzung ist eine Form der Diskriminierung.

- Smart-Home-Geräte wie Kamerasensoren in Küchengeräten können z. B. zur Überwachung anderer Personen im Haushalt genutzt werden und diese in ihrer Privatsphäre verletzen.

- Mit unbemerkt laufenden Spionage-Apps („Stalkerware“) können z. B. Ex-Partner∗innen aus der Ferne überwacht werden. Betroffene sind so ständiger Angst vor Verfolgung und potentiell unberechenbaren Eskalationen von Gewalt gegen sie ausgesetzt.

**Geschlechtergerechte Digitalisierung kann nur gelingen, wenn Datenschutz und Diskriminierungsschutz zusammengedacht werden.**

AUS DEM INHALT

## Datenschutz und IT-Sicherheit im Recht

Das Grundgesetz (GG) beinhaltet das Recht auf Datenschutz und IT-Sicherheit. Das Bundesverfassungsgericht hat aus dem Recht auf die freie Entfaltung der Persönlichkeit in Art. 2 Abs. 1 GG und der Pflicht zur Wahrung der Menschenwürde in Art. 1 Abs. 1 GG zwei weitere Grundrechte hergeleitet:

» Das **Recht auf informationelle Selbstbestimmung** wurde bereits 1983 mit dem sogenannten Volkszählungsurteil geschaffen. Das Bundesverfassungsgericht stellte damals fest, dass die individuellen Entfaltungschancen einzelner Bürger*innen bedroht seien, wenn diese nicht mehr wüssten, wer was wann über sie wisse, dies speichere und irgendwann verwende. Menschen agierten nicht mehr selbstbestimmt, wenn sie sich überwacht fühlten. In einem freiheitlichen demokratischen Gemeinwesen sei dies jedoch die Funktionsbedingung für Handlungsfähigkeit und Mitwirkungsfähigkeit der Bürger*innen.

» Das **Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** begründete das Bundesverfassungsgericht 2008 als Ausprägung des allgemeinen Persönlichkeitsrechts. Das Gericht reagierte damit auf die gewachsenen Möglichkeiten des Staates, Bürger*innen durch informationstechnische Systeme zu überwachen. Anlass war die unbemerkte Online-Durchsuchung durch Geheimdienste.

In Deutschland bietet das Standard-Datenschutzmodell des AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein ausführliches Methodenhandbuch für Datenschutz-Folgenabschätzungen: https://www.datenschutzzentrum.de/sdm/

Diese Grundrechte sollen es allen Menschen ermöglichen, an einer Gesellschaft teilzuhaben, die zunehmend von Prozessen der Digitalisierung beeinflusst wird. Sie sind zum einen Abwehrrechte der Bürger*innen gegen den datensammelnden Staat. Zum anderen verpflichten sie den Staat, die (Datenschutz-)Rechte der Bürger*innen gegenüber privaten Dritten, z. B. Unternehmen, sicherzustellen. Im Grundgesetz sind weitere den Schutz privater Daten betreffende Rechte verankert, z. B. das Brief-, Post- und Fernmeldegeheimnis in Art. 10 GG oder der Schutz der Wohnung in Art. 13 GG. Auf europäischer Ebene enthalten die EU-Grundrechtecharta (GRCh) und die Europäische Menschenrechtskonvention Rechte zum Schutz des Privat- und Familienlebens und privater Kommunikation.

Die europäische Datenschutz-Grundverordnung (DSGVO) spezifiziert die technischen und organisatorischen Maßnahmen zur Verarbeitung personenbezogener Daten. Hierbei müssen Grundsätze eingehalten werden: u. a. Transparenz, Zweckbindung, Datenminimierung, Vertraulichkeit und Integrität. Letztere werden z. B. durch IT-Sicherheitsmaßnahmen wie Daten-Backup-Strategien, Verschlüsselung und digitale Signaturen sichergestellt. Nationale Datenschutzbehörden prüfen z. B. über eine Datenschutz-Folgenabschätzung, ob die DSGVO von Datenverarbeitenden eingehalten wird.

Diese bestehenden Rechte dürfen nicht ins Leere laufen. Die Sachverständigenkommission für den Dritten Gleichstellungsbericht der Bundesregierung empfiehlt daher:

**Vorgaben der DSGVO einschließlich enger Zweckbindungen proaktiv um- und durchsetzen**

» Von Instrumenten ausgreifender staatlicher und privater Datenauswertung (beispielsweise Vorratsdatenspeicherung, Profilbildung, weitreichende Datenaustauschverfahren, Einrichtung zentraler Datensammelstellen) ist abzusehen. Für die Datenverwendungen sind enge Zweckbegrenzungen abzusichern, auch über die DSGVO hinaus. Die zentrale Datenspeicherung mit vielfältigen Weiterverwendungsmöglichkeiten ist abzulehnen. Weitere wichtige Maßnahmen sind: strikte Opt-In-Lösung für (unbemerkte) Datenauswertungen; Verpflichtung und Haftung der Softwarehersteller*innen bezüglich Einhaltung von DSGVO und ePrivacy-Verordnung; Privacy-by-Design; effektive und benutzer*innenfreundliche Do-not-track-Vorkehrungen; Ende-zu-Ende-Verschlüsselung; klare Begrenzung von Profiling und Scoring; Verbot personalisierter, dynamischer Werbung und Preisbildung.

**Vergabe öffentlicher Aufträge an Datenschutz und IT-Sicherheit orientieren**

» In die Vergabepraxis und -vorgaben der öffentlichen Hand ist aufzunehmen, dass digitalisierte Dienste, Produkte, Soft- und Hardware diskriminierungsfrei sind und dass sie mit Datenschutz und IT-Sicherheit nicht nur konform sind, sondern beides fördern.

**IT-Sicherheit stärken**

» Bundes- und Landesregierungen und staatliche Einrichtungen haben darauf hinzuwirken, dass die Bedeutung von Authentizität, Vertraulichkeit und Zugriffsschutz erkannt und umgesetzt wird. Dies beinhaltet: Initiativen der EU zum Schutz der IT-Sicherheit zu unterstützen; kryptografischen Schutz vor unberechtigtem Zugriff zu verstärken; Forschung im Bereich der angewandten IT-Sicherheit und des Datenschutzes finanziell und strukturell auszubauen sowie den Einbau gezielter Sicherheitslücken für staatliche Zwecke zu verhindern.

## Schutz vor Diskriminierung braucht Datenschutz

Das Grundgesetz schreibt in Art. 3 die Gleichberechtigung von Frauen und Männern und den Schutz vor Diskriminierung fest. Art. 3 Abs. 2 und 3 GG schützen vor unmittelbarer und mittelbarer Diskriminierung u. a. wegen des Geschlechtes, der Abstammung, der Sprache, Heimat und Herkunft oder aus rassistischen Gründen. Art. 3 Abs. 2 Satz 2 GG verpflichtet den Staat zudem, die tatsächliche Durchsetzung der Gleichberechtigung zu fördern und aktiv auf die Beseitigung von Nachteilen hinzuwirken. Diese Pflichten wirken sich auch im Datenschutz aus, denn die besonderen Grundrechte in Art. 3 Abs. 2 und 3 GG konkretisieren das Recht auf eine freie Entfaltung der Persönlichkeit und die Pflicht zur Wahrung der Menschenwürde in Art. 2 Abs. 1 i. V. m. Art. 1 GG. Datenschutz muss also auch den Schutz vor (geschlechtsbezogener) Diskriminierung und die Gleichberechtigung von Frauen und Männern gewährleisten. Dies bedeutet z. B. auszuloten, wie der Schutz vor Diskriminierung in Datenschutz-Folgenabschätzungen einfließen kann. Solche Folgenabschätzungen sind beispielsweise nötig, wenn Betriebe neue Softwaresysteme einführen wie etwa Personalmanagementsysteme, die erhebliche Diskriminierungsrisiken bergen.

Die Stiftung Datenschutz hält fest: „Datenschutz- und Antidiskriminierungsrecht verfolgen sehr ähnliche und in Teilen sogar die gleichen Ziele. Es geht darum, gesellschaftliche Machtasymmetrien auszugleichen und zu regulieren. Beide wollen die freie Entfaltung der Persönlichkeit gewährleisten und Individuen vor Fremdzuschreibungen schützen. Es geht um den Schutz der einzelnen Person, aber auch um gesamtgesellschaftliche Freiheit und (Chancen-)Gleichheit."
Bislang werden Datenschutz, Schutz vor Diskriminierung und Gleichberechtigung in der Politik, der Verwaltung und der Wissenschaft allerdings jedoch selten zusammengedacht.

2013 wurde die Stiftung Datenschutz von der Bundesregierung gegründet und soll als unabhängige Institution den Datenschutz in der Praxis fördern. Sie setzt sich auch mit dem Zusammenhang von Datenschutz- und Antidiskriminierungsrecht auseinander: https://stiftungdatenschutz.org/themen/datenschutz-und-antidiskriminierungsrecht

Die Sachverständigenkommission fordert daher:

**Forschung intensivieren**

» Die Forschung im Bereich der Realisierung von Grundrechten im Zuge der Digitalisierung muss gefördert und hierbei auf Ungleichheitskategorien wie das Geschlecht fokussiert werden.

**Institutionen der Wahrung von Datenschutz und IT-Sicherheit für Diskriminierungsaspekte sensibilisieren und entsprechend ausstatten**

» Aufsichtsbehörden und Datenschutzbeauftragte sind gezielt dafür zu sensibilisieren, dass Datenschutz auch und insbesondere dem Schutz und der Teilhabe benachteiligter Gruppen – etwa Menschen, die dem heteronormativen Geschlechtermodell nicht entsprechen – dient. Bei der Beurteilung von Datenverarbeitungsprozessen sind entsprechende Auswirkungen einzubeziehen. Die zuständigen Behörden sind entsprechend auszustatten.

**Umfassende Kontrolle algorithmischer Systeme sicherstellen und dabei Diskriminierungsrisiken berücksichtigen**

» Aufgrund der Vielfalt möglicher Ursachen diskriminierender Effekte beim Einsatz algorithmischer Systeme sind umfassende Kontrollen und Datenschutz-Folgenabschätzungen notwendig. Hierbei muss nicht nur die Auswertung durch Algorithmen (Algorithmenkontrolle) sowie die darauf aufbauende Entscheidung des algorithmischen Systems (Outputkontrolle) kontrolliert werden, sondern auch die Datenbasis eines algorithmischen Systems (Inputkontrolle). Dies gilt insbesondere bei automatisierten Profilbildungen und Überwachungen, unabhängig davon, ob staatliche oder private Akteur*innen ein algorithmisches System einsetzen.

## Weitere Rahmenbedingungen für Datenschutz und Diskriminierungsfreiheit

### Bildung für mehr Datenschutz

Um unsere personenbezogenen Daten im Alltag zu schützen, benötigen wir entsprechende Kompetenzen. Es ist wichtig, dass wir von klein auf ein Bewusstsein dafür entwickeln, welche Gefahren in Smartphone-Apps lauern, auf welche Weise sie unser Verhalten manipulieren oder überwachen oder wie die Diensteanbietenden von den Daten profitieren, die wir hinterlassen.

### Geschützte soziale digitale Räume, besonders im Bildungsbereich

Zur erläuterten Verbindung von Daten- und Diskriminierungsschutz gehört auch, dass Menschen diskriminierungsfrei Zugang zu Diskursen in den Sozialen Medien haben. Internetdienste müssten demnach den Schutz persönlicher Daten absichern. Auf vielen Plattformen wie z. B. Instagram, TikTok, Twitter oder Facebook wird der Zugang jedoch mit Daten erkauft (Daten-gegen-Dienst-Modell). Die Plattformen sind nur vermeintlich kostenfrei. Sie verdienen an der intransparenten Erhebung, Zusammenführung, Rekombination, Auswertung und Weitergabe persönlicher Daten. Besonders brisant ist es, wenn in Bildungseinrichtungen solche Dienste genutzt werden, weil öffentliche gemeinwohlorientierte IT-Infrastrukturen fehlen.

Die Sachverständigenkommission empfiehlt daher:

**Bildung ausbauen, die Datenschutz und IT-Sicherheit gerecht wird**

» Bildung zu Datenschutz und IT-Sicherheit ist über den gesamten Lebensverlauf hinweg zu vermitteln, d. h. in der frühen Bildung, in den Schulen sowie in Angeboten der Aus- und der allgemeinen Weiterbildung; die Empfehlung richtet sich auch an den Bund für den Bereich der beruflichen Weiterbildung.

**Datenschutz- und IT-Sicherheitskonforme Dienste und Produkte fördern, besonders im Bildungsbereich**

» Öffentliche Institutionen sollten eine am Gemeinwohl orientierte, geschlechtergerechte sowie intersektionalitätsbewusste Plattform digitaler Grundversorgung und politischer Partizipation bereitstellen. In Schulen und Bildungseinrichtungen sind Anwendungen einzusetzen, die Datenschutz und IT-Sicherheit gewährleisten und eine Weitergabe der Daten von Schüler*innen und Lehrkräften sowie eine Vernetzung mit kommerziellen sozialen Netzwerken verhindern. Empfohlen wird die Bereitstellung und Nutzung von Open-Source-Anwendungen. Alternativen zum Daten-gegen-Dienst-Modell sind gezielt zu fördern, damit alle Menschen an der Digitalisierung teilhaben können – frei von der Sorge um Diskriminierung, Ausspähung und mangelnden Schutz.


### Zum Weiterlesen

» Kapitel B.IV.3 im Gutachtenteil des Dritten Gleichstellungsberichts der Bundesregierung, abzurufen unter https://www.bmfsfj.de/gleichstellungsbericht

» Die Bundesverbraucherzentrale bietet zahlreiche praktische Tipps, um den Schutz der eigenen Daten sicherzustellen: https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz

» Der Newsletter „Sicher Informiert“ des Bundesamts für Sicherheit in der Informationstechnik klärt auf über aktuelle Gefahren wie Maschen des Identitätsdiebstahls oder im Netz kursierende Betrugs- und Schadsoftware und kann kostenfrei abonniert werden: https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/buerger-cert-abos_node.html

IMPRESSUM:

Themenblatt verfasst von der Geschäftsstelle Dritter Gleichstellungsbericht
V.i.S.d.P.: Institut für Sozialarbeit und Sozialpädagogik e.V.
Geschäftsstelle Dritter Gleichstellungsbericht der Bundesregierung
Sebastian Scheele und Dr. Ulrike Spangenberg (Leitung)
Lahnstraße 19, 12055 Berlin
www.dritter-gleichstellungsbericht.de
Stand: Dezember 2021
Erscheinungsjahr: 2021

ISS Gemeinnütziger e. V.

Gefördert vom:
Bundesministerium für Familie, Senioren, Frauen und Jugend