Datenschutzkonzept

Digitale Gesellschaft
2023

Vorgestellt am Datenschutzfestival
vom 03.11.2023

Datenschutzkonzept

Einleitung

Die fortschreitende Digitalisierung und die rasante Weiterentwicklung von Technologien bringen sowohl Chancen als auch Gefahren mit sich. Insbesondere die Vernetzung von grossen Datenbeständen sowie der Einsatz von «künstlicher Intelligenz» beeinträchtigen die Persönlichkeitsrechte der Menschen. Die Nachwahlbefragung zum E-ID-Referendum hat speziell gezeigt, dass Datenschutz zu einem zentralen Anliegen für die Bevölkerung geworden ist.

Viele Menschen fühlen sich durch die Digitalisierung überfordert. Bestärkt wird das daraus entstehende Unwohlsein durch die fast wöchentlich zu lesenden Berichte über Datenverluste. Dies schwächt das Vertrauen in den Umgang mit Daten. Das Vertrauen in der Bevölkerung ist jedoch von entscheidender Bedeutung, sollen neue Möglichkeiten der digitalen Demokratie und für E-Government, aber auch neue digitale Geschäftsmodelle geschaffen werden. Das selbe gilt für sogenannte Datenräume, in der eine «Sekundärnutzung» von Personendaten über den ursprünglichen Zweck hinaus möglich werden soll.

Um das nötige Vertrauen zu schaffen, braucht es einen sorgsamen Umgang mit Daten, der auf einem zielgerichteten und wirksamen Datenschutz basiert. Datenschutz und Datennutzung sind entsprechend kein Widerspruch – im Gegenteil: sie bedingen einander.

Datenschutzgesetz und Bundesverfassung

Der Zweck des Datenschutzgesetzes ist gemäss Art. 1 der «Schutz der Persönlichkeit und der Grundrechte der natürlichen Personen, über die Daten bearbeitet werden». Dieser Zweckartikel ist sehr offen und allgemein formuliert. Dabei bleibt unklar, was konkret geschützt werden soll. Gemäss dem dem Datenschutzgesetz zugrundeliegenden Art. 13 Abs. 2 der Bundesverfassung (BV) hat jede Person «Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten». Dieses verankerte Missbrauchsparadigma sorgt dafür, dass erst eine Reaktion auf den bereits erfolgten Missbrauch möglich wird und die Beweislast bei den betroffenen Individuen liegt. Eine solche Einschränkung des Wortlauts auf den Missbrauch ist für ein Grundrecht ungewohnt, welches normalerweise erst über Art. 36 BV eingeschränkt wird.

Der Wortlaut von Art. 13 Abs. 2 BV wird entsprechend als zu eng kritisiert. Vielmehr sieht die Rechtsprechung darin ein Recht auf informationelle Selbstbestimmung enthalten. Dieses bezeichnet das Recht der Individuen, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen zu können. Das Recht auf informationelle Selbstbestimmung klingt eingängig, ist gesetzlich aber nur schwach abgestützt und lässt sich in der Praxis nur limitiert einfordern. Überwiegende Interessen der Datenbearbeiter:innen oder gesetzliche Pflichten schränken es deutlich ein. Weiter gibt es die Kritik, als individuelles Recht die Verantwortung den Betroffenen zu überlassen; sei es, sich durch Cookie-Banner zu klicken, die richtigen Datenschutz-Einstellungen zu finden oder sich gegen übergriffige Praktiken zu wehren.

Datenschutz betrifft aber nicht nur einzelne Individuen, sondern auch die Gesellschaft als Ganzes. So ist bei einer Wahlmanipulation, also der Manipulation von Menschen und Menschengruppen zur Beeinflussung eines Wahlergebnisses, die Auswirkung auf das Individuum gering, der gesellschaftliche Schaden unter Umständen aber enorm.

Angesichts dieser Defizite ist es erforderlich, den Datenschutz zu überdenken und ein neues Konzept als Grundlage zu entwickeln. Datenschutz ist kein Selbstzweck. Dafür ist es zunächst notwendig, klar zu definieren, wovor das Datenschutzrecht Menschen tatsächlich schützen soll. Diese Schutzziele und das daraus resultierende Konzept sollen sicherstellen, dass den Individuen und der Gesellschaft als Ganzes aus den Datenbearbeitungen keine Nachteile erwachsen. Gleichzeitig sollen sie dafür sorgen, dass der Raum für Innovation offen bleibt.

Schutzziele

Ausgehend von der Kritik am zu wenig spezifischen Zweck des Datenschutzgesetzes und seinem unklaren Schutzbereich müssen konkrete Schutzziele formuliert werden. Es ergeben sich folgende sieben Schutzziele:

I. Schutz vor Manipulation

Mit dem Schutz vor Manipulation sollen die individuelle Entscheidungsfreiheit und die demokratische Willensbildung geschützt werden.

Unter Manipulation zu verstehen ist die absichtliche, gezielte und in der Regel verdeckte Einflussnahme auf die Entscheidung einer anderen Person, um deren Selbstkontrolle und Entscheidungskraft zu unterlaufen. Die Manipulation kann zu einem Nachteil für die betroffene Person führen. Sie zielt, unter Ausnützung menschlicher Schwächen auf eine Steuerung des Verhaltens von Individuen oder Gruppen. Vulnerable Menschen sind besonders stark gefährdet.

II. Schutz vor Diskriminierung

Datenbearbeitungen dürfen nicht diskriminierend sein. Eine Diskriminierung liegt vor, wenn eine Person rassistisch [1] oder aufgrund geschützter Merkmalen wie Herkunft, Geschlecht, Alter, Sprache, soziale Stellung, Lebensform, religiöse, weltanschauliche oder politische Überzeugung oder körperliche, geistige oder psychische Behinderung ohnesachlichen Grund unterschiedlich behandelt wird.

Regulierungen zum Schutz vor Diskriminierung finden sich vereinzelt in Gesetzen wie im Strafrecht (Art. 261bis StGB), im Gleichstellungsgesetz (GlG) oder im Behindertengleichstellungsgesetz (BehiG). Diese Bestimmungen haben allerdings nicht direkt die Diskriminierung durch Datenbearbeitungen zum Gegenstand. Der zivilrechtliche Persönlichkeitsschutz schützt vor Persönlichkeitsverletzungen (Art. 28 ff. ZGB), doch steht Diskriminierung nicht im Zentrum. Deshalb vermögen bestehende Regelungen nicht genügend vor Diskriminierung durch Datenbearbeitungen zu schützen.

III. Schutz vor Überwachung und Recht auf Anonymität

Mit dem Schutz vor Überwachung soll sichergestellt werden, dass die persönliche Freiheit und die Persönlichkeitsentwicklung (Art. 10 Abs. 2 BV), die freie Meinungsäusserung (Art. 16 BV) und weitere Grundrechte wie insbesondere die Versammlungsfreiheit (Art. 22 BV) und die Privatsphäre (Art. 13 BV) gewährleistet sind. Dafür ist insbesondere wichtig, dass keine Abschreckungseffekte («chilling effects») bei der Wahrnehmung der Grundrechte eintreten.

Das Recht auf Anonymität gewährleistet die Bewegungsfreiheit, um sich im öffentlichen Raum grundsätzlich anonym bewegen und verhalten zu können.

IV. Schutz vor Beeinträchtigung der Gesundheit sowie der Lebens- und Entwicklungschancen

Mit dem Schutz vor Beeinträchtigung der psychischen und physischen Gesundheit sowie der Lebens- und Entwicklungschancen soll sichergestellt werden, dass Menschen nicht durch eine (falsche) Beurteilung durch Automated Decision-Making Systeme (ADMS, künstliche Intelligenz) geschädigt werden. Dies beinhaltet das Recht auf eine (Neu-)Beurteilung durch ein Individuum sowie bei Beurteilungen bei denen dies nicht möglich ist, zusätzliche Schutzmassnahmen, wie höhere Sorgfaltspflichten oder eine Zertifizierung.

V. Recht auf Transparenz und Pflicht zur Sorgfalt

Mit dem Recht auf Transparenz muss für betroffene Personen klar genug ersichtlich sein, welche Daten bearbeitet werden. Dazu gehört ein substanzielles Mitbestimmungsrecht. Dafür muss eine verständliche Erkennbarkeit der Datenbearbeitung und eine Möglichkeit zu einem einfach wahrzunehmenden Widerspruchsrecht am selben Ort gegeben sein. Die Datenbearbeiter:innen müssen eine Rückverfolgbarkeit bei Weitergabe der Daten, eine Korrektur- und Widerspruchsmöglichkeit sowie einen Löschanspruch im Rahmen der substantiellen Mitbestimmung gewährleisten. Der Einsatz von Automated Decision-Making Systemen (ADMS, künstliche Intelligenz) muss erkenntlich sein.

Grundvoraussetzung eines effektiven Datenschutzes ist Datensicherheit. Die Datenbearbeiter:innen haben mit der Pflicht zur Sorgfalt nach anerkannten Regeln der Technik sicherzustellen, dass die Datensicherheit gewährleistet ist und Verletzungen effektiv verhindert werden.

VI. Recht auf Vergessenwerden

Das Recht auf Vergessenwerden soll sicherstellen, dass Informationen nicht dauerhaft zur Verfügung stehen und damit eine Resozialisierung möglich ist. Die Permanenz und Ubiquität von Daten widerspricht der Funktionsweise der menschlichen Wahrnehmung, welche selektioniert und vergisst. Mit dem Urteil des Europäischen Gerichtshofs (EuGH), wonach nicht an der Quelle gelöscht werden muss, sondern dort, wo die Information auffindbar ist, wird dem Rechnung getragen («Google Spain»-Urteil).

VII. Schutz der offenen Gesellschaft und freien Demokratie

Von Datenbearbeitungen können nicht nur Individuen betroffen sein, sondern auch die Gesellschaft als Ganzes und die freie Demokratie.

Eine offene Gesellschaft ist durch Social Scoring gefährdet. Social Scoring basiert auf Überwachung und Kontrolle und führt zu Gleichschaltung. Eine funktionsfähige und stabile Demokratie erfordert eine pluralistische, von staatlichem Dirigismus freie Gesellschaft.

Die freie Demokratie ist gefährdet, wenn durch gezielte Informationen oder das bewusste und massenhafte Verbreiten von (Falsch-) Informationen zum Ziel der Manipulation Wahlbeeinflussung stattfindet. Wenn Botschaften zielgerichtet und individuell auf einzelne Personengruppen zugeschnitten werden (und keine Transparenz darüber besteht, welche Informationen ausgespielt werden), entsteht die Gefahr, dass der Diskursraum fragmentiert wird. Das kann zu einer Verzerrung der öffentlichen Meinung führen. Der Zugang zu verschiedenen Informationen und Perspektiven muss gewährleistet sein, um eine vielfältige und pluralistische Meinungsbildung im demokratischen Prozess zu ermöglichen.

Abschreckungseffekte («chilling effects»), wonach Menschen aufgrund von Überwachung oder der Angst vor unerwünschten Konsequenzen ihre Grundrechte nicht mehr wahrnehmen, sollen verhindert werden. Ein effektiver Datenschutz schafft die notwendige Vertrauensbasis, um sicherzustellen, dass die Menschen ihre Grundrechte wie Meinungsfreiheit oder Versammlungsfreiheit ausüben können, ohne befürchten zu müssen, überwacht und sanktioniert zu werden. Dies ist eine Voraussetzung, dass eine liberale Demokratie bestehen kann.

Konzept

Basierend auf den Schutzzielen ergibt sich ein Konzept für einen zielgerichteten und wirksamen Datenschutz, der Vertrauen schafft und Innovation fördert. Das Konzept stellt dabei die Einhaltung und Durchsetzung der Schutzziele ins Zentrum und löst sich vom Prinzip der Einwilligung zur Datenbearbeitung und der Zweckbindung. Geregelt wird der Umgang mit Daten und nicht Personendaten an sich. Das Konzept beinhaltet Grundsätze zur Datenbearbeitung, ein absolutes Verbot für bestimmte Datenbearbeitungen, eine substantielle Mitbestimmung der Betroffenen sowie Bestimmungen zur Durchsetzung des Konzepts.

Grundsätze

Datenbearbeitungen sollen unter Einhaltung der Schutzziele ohne Einwilligung möglich sein. Datenbearbeiter:innen müssen daher als Ausgleich die Interessen der Betroffenen wahren und dafür sorgen, dass die Datenbearbeitung keine ungewollten Folgen für die Individuen und die Gesellschaft haben. Die Datenbearbeitungen dürfen das Funktionieren einer offenen demokratischen Gesellschaft nicht gefährden. Weiter müssen sie die Vorgaben zur Transparenz, zur substantiellen Mitbestimmung und zur Datensicherheit einhalten. Innerhalb dieses Rahmens sollen Datenbearbeitungen unabhängig einer Zweckbindung möglich sein.

Als Grundsätze gelten:

- Private und staatliche Datenbearbeitungen müssen die Schutzziele für die Individuen und die Gesellschaft wahren.
- Staatliche Datenbearbeitung braucht zwingend eine klare gesetzliche Grundlage, aus der eindeutig hervorgeht, welche Daten zu welchem Zweck und wie bearbeitet werden.

Verbot

Grundsätzlich genügt für die Rechtmässigkeit von Datenbearbeitungen, dass die Einhaltung der Schutzziele sichergestellt ist (und bei staatlicher Datenbearbeitung eine klare gesetzliche Grundlage besteht). Datenbearbeitungen, welche ein grosses Risiko für Individuen oder die Gesellschaft bergen und die Schutzziele nicht gewährleisten können, sind jedoch absolut verboten und können nicht gerechtfertigt werden. Dazu gehören insbesondere biometrische Massenüberwachung (z.B. Gesichtserkennung im öffentlichen Raum), anlasslose Überwachung und Social Scoring.

Substantielle Mitbestimmung

Das Recht auf informationelle Selbstbestimmung ist in der Praxis limitiert. Es stehen daher die Datenbearbeiter:innen in der Pflicht, die Interessen der Betroffenen zu wahren und die Schutzziele einzuhalten. Eine Datenbearbeitung im Rahmen der Grundsätze unter Einhaltung der Schutzziele ist ohne Einwilligung möglich. Datenbearbeitungen müssen jedoch sicher und für die Betroffenen erkennbar sein sowie eine substanzielle Mitbestimmung gewähren, worunter insbesondere eine Möglichkeit zu einem einfach wahrzunehmenden Widerspruchsrecht gegeben sein muss.

Durchsetzung

Unter Einhaltung der Schutzziele können Daten und insbesondere auch Personendaten unbeschränkt bearbeitet werden. Werden die Schutzziele jedoch nicht eingehalten, so ist dies ein Verstoss gegen die Regulierung, und die Datenbearbeitung ist unzulässig. Die Gewährleistung der Schutzziele muss folglich durch wirksame Sanktionen und Mechanismen zur Durchsetzung sichergestellt werden. Insbesondere die Inkaufnahme von grösseren Risiken und eine systematische Verletzung der Grundsätze, Verbote und der substantiellen Mitbestimmung führen zu einer empfindlichen Strafe. Gegenüber Wissenschaft, zivilgesellschaftlichen Organisationen, Medien und Behörden besteht ein umfassendes Auskunftsrecht. Verbände und Aufsichtsbehörden haben ein Klagerecht. Bei Erfolg vor Gericht müssen Verbände ihrem Aufwand entsprechend entschädigt werden. Eine Beweislastumkehr soll der Machtasymmetrie gegenüber den Datenbearbeiterinnen entgegenwirken. Die Möglichkeit zur Überprüfung von Entscheiden beim Einsatz von Automated Decision-Making Systemen (ADMS, künstliche Intelligenz), beispielsweise per Datenzugang, muss gegeben sein.

Auswirkungen

Das Konzept führt unter Einhaltung der Schutzziele zu einem zielgerichteten und wirksamen Datenschutz. Datenbearbeiter:innen werden verstärkt in die Pflicht genommen, die Interessen der betroffenen Personen und der Gesellschaft zu wahren. Individuen haben ein substantielles Mitbestimmungsrecht. Das Vertrauen in die Datennutzung und die Datenbearbeitung wird gestärkt.

[1] In der Verfassung (Art. 8 Abs. 2 BV) und im Gesetz (Art. 261bis StGB) wird für die Diskriminierungsdefinition der Begriff «Rasse» verwendet. Das Wort suggeriert ein Menschenbild, das auf der Vorstellung unterschiedlicher menschlicher «Rassen» basiert und steht für eine lange Geschichte rassistischer Gewalt. Damit steht die Verwendung des Begriffs in einem unauflösbaren Widerspruch mit dem Zweck der Bestimmung, wonach eigentlich rassistische Diskriminierung bekämpft werden soll (s.u. https://www.institut-fuer-menschenrechte.de/themen/rassistische-diskriminierung/begriff-rasse; https://www.amnesty.de/glossar-fuer-diskriminierungssensible-sprache).