Datenschutz und Datenschutzkompetenz

Im Zuge der technologischen Entwicklungen gewinnt das Thema Datenschutz immer mehr an Bedeutung. Auch im Zuge der aktuellen Situation rund um das Coronavirus und die Nutzung einer App zur Erfassung von möglichen Personenkontakten über Sandortdaten des Smartphones, wird in Bezug auf den Datenschutz diskutiert.

Was Datenschutz ist, wie man sich als NutzerIn selbst datenschutzkompetent verhält und welche Werkzeuge zum Datenschutz existieren, erfahren Sie in diesem Artikel.

Datenschutz in Deutschland und Europa

Laut der Duden Online Definition (2019) beschreibt Datenschutz, den Schutz von Bürgern und Bürgerinnen vor Beeinträchtigungen ihrer Privatsphäre durch das unbefugte erheben, speichern und weitergeben von Daten, die ihre Person betreffen. Im speziellen beschäftigt sich der Datenschutz mit dem Schutz personenbezogener Daten. Unter personenbezogenen Daten versteht man jene Daten, die eine Person identifizierbar machen, wie bspw.: Name, Adresse, Geburtstag oder Telefonnummer (Kap. 1 Art. 4 Abs. 1 DSGVO). Darüber hinaus existieren personenbezogene Daten, die besonders sensibel sind, weswegen diese oftmals auch als sensible Daten bezeichnet werden. Zu ihnen gehören unter anderem Informationen zur ethnischen Herkunft, der politischen Meinung, zu genetischen Daten, Gesundheitsdaten oder Daten, die Auskunft über die sexuelle Orientierung einer Person geben (Kap. 2 Art. 9 DSGVO).

Im Rahmen verschiedener Verordnungen ist geregelt, welche Daten in welchem Maße und durch wen verarbeitet werden dürfen. In Deutschland regelt neben der Datenschutzgrundverordnung (DSGVO) bzw. der Europäischen Datenschutzgrundverordnung (EU-DSGVO) auch das Bundesdatenschutzgesetzt (BDSG) die Verarbeitung personenbezogener Daten. Bei der DSGVO handelt es sich um eine Verordnung, die den Datenschutz in der Europäischen Union einheitlich regeln soll. Das BDSG hingegen stellt eine Ergänzung dar, die lediglich für Deutschland gilt und nicht im Widerspruch mit der DSGVO stehen darf. Das BDSG spezifiziert und ergänzt die DSGVO (BFDI 2020a). Sowohl die DSGVO als auch das BDSG sind seit dem 25. Mai 2018 anwendbar.

Das Recht von Bürgerinnen und Bürgern, über die Verwendung und Preisgabe ihrer persönlichen Daten zu bestimmen, wird bereits im Grundgesetz formuliert. Dabei stellen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 2 des Grundgesetztes das allgemeine Persönlichkeitsrecht dar, welches 1973 durch das Bundesverfassungsgericht in den ersten Lebach-Urteilen definiert wurde. Das allgemeine Persönlichkeitsrecht umfasst dabei die freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) sowie den Schutz der Menschenwürde (Art. 1 Abs. 1 GG).

Beitrag online abrufbar unter: https://informationskompetenz.blog.uni-hildesheim.de/datenschutz-und-datenschutzkompetenz/

Art. 2 Abs. 1 GG:

„Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

Art. 1 Abs. 1 GG:

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

Darüber hinaus stellt das allgemeine Persönlichkeitsrecht eine Ausprägung des Rechts auf informationelle Selbstbestimmung dar, welches Grundrecht anerkannt ist (Volkszählerurteil 1983). Dieses leitete sich unter anderem aus Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention ab:

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz."

Das BDSG und die DSGVO schützen das Grundrecht auf informationelle Selbstbestimmung. Geschützt werden, demnach nicht nur Daten, sondern auch die Freiheit des Menschen selbst darüber zu entscheiden, wer, was, wann und in welcher Situation über einen weiß (BFDI 2020b).

Herausforderungen und Chancen

Beschränkte sich der Datenschutz zu großen Teilen früher auf zentrale Einrichtungen, die Daten sammelten und austauschten, stehen wir durch die Nutzung des Internets vor täglich steigenden Herausforderungen. Internetdienste, wie bspw. Suchmaschinen, Soziale Medien und Instant-Messaging-Dienste werden heutzutage von vielen Personen, die Daten produzieren, genutzt. Dabei steigt auch die Verantwortung des einzelnen Nutzers, der seine Daten oftmals bereitwillig den obengenannte Internetdienste zur Verfügung stellt (BFDI 2020a).

Datenschutzkompetenz aus Nutzersicht: Ergebnisse der Online-Diskussion

Online-Datenschutz ist ein wichtiges Themenfeld. Im Kontext des Projekts Informationskompetenz und Demokratie ist insbesondere die Frage der dazu erforderlichen Kompetenzen auf Nutzerseite interessant. Auf der Eröffnungstagung wurde angeregt zu diesem Thema Informationen bereitzustellen und das Themenfeld zu diskutieren. In der Online-Diskussion vom 25. - 28. November 2019 konnten NutzerInnen ihre Perspektive darlegen. Dabei wurden folgende Leitfragen genutzt, um die Beiträge zu strukturieren:

- Was verstehen Sie unter einer Online-Datenschutzkompetenz?
- Was muss man wissen, um online datenschutzkompetent zu sein? Wie verhält sich ein datenschutzkompetenter Nutzer in Bezug auf Online-Tracking und das eigene Posting-verhalten im Internet?
- Wann lohnt sich Datenschutzkompetenz, wann nicht? Warum verhalten wir uns oft nur wenig datenschutzkompetent? Ist nur derjenige, der Tracking blockt und wenig postet datenschutzkompetent?
- Wie haben wir unser Wissen zur Privatheit im Internet erworben? Wie sollte man es erwerben? Wer müsste es vermitteln und wie sollte dies geschehen?

In der Online-Diskussion wird deutlich, dass die Teilnehmenden das Thema Datenschutz als sehr aktuell einschätzen, wie auch nachfolgendes Zitat aufzeigt:

> *„Das Thema um den Datenschutz im Netz war noch nie so wichtig wie in der heutigen Zeit." (Kevin)*

Im Folgenden werden die Ergebnisse der Online-Diskussion inhaltlich unterteilt dargelegt.

Bewusstsein und Wahrnehmung von Risiken

Teilnehmende der Online-Diskussion führen an, dass sich NutzerInnen oftmals nicht darüber bewusst sind, welche Datenspuren sie hinterlassen und wie viele persönliche Informationen sie im Internet veröffentlichen und gesammelt werden. Als Grund dafür wird bspw. ein nicht datenschutzkompetentes Verhalten angeführt und das nicht vorhandene Bewusstsein über mögliche Gefahren, wie bspw. das folgende Zitat aufzeigt:

> *„Heutzutage beschäftigen sich viele Internetnutzer viel zu wenig mit dem Datenschutz, Leichtsinn und Ahnungslosigkeit führen zu vielen versteckten Gefahren für die Nutzer." (Sima C.)*

Insbesondere die Nutzung von Trackern auf Webseiten, die Nutzerprofile erstellen und weiterverkaufen, werden als Risiko wahrgenommen, mit dem man sich aus Nutzersicht auseinander setzten sollte. Auch beim Online-Shopping oder der normalen Internetsuche werden Daten gesammelt, mit denen die Präferenzen der NutzerInnen ermitteln und analysiert werden können. Die erstellten Nutzerprofile können anschließend zu kommerziellen Zwecken, der Markforschung und Werbeplatzierung verwendet werden.

> *„Mehr und mehr Seiten im Internet werden mit Trackern ausgestattet, um Profile zu erstellen, die dann wiederverkauft werden". (Kevin)*

Die Gefahren, die mit einer geringen Datenschutzkompetenz einhergehen werden unterschätzt, da die Bedrohungen nicht sichtbar sind. Gar wird das Brechen eines datenschutzkompetenten Verhaltens oftmals erzwungen, wenn ich bspw. Cookies zur Nutzung einer Webseite zustimmen muss.

> *„So wird einem mittlerweile auf fast jeder Website angezeigt, dass sie Cookies verwenden, doch um alle Funktionen nutzen zu können oder aber die Seite überhaupt sehen zu können (da manche Cookiemeldungen die ganze Seite bedecken), bin ich gezwungen, diesen zuzustimmen, sodass ich letztendlich doch wieder keine Wahl habe.“ (Juliane K.)*

Darüber hinaus nennen Teilnehmende bspw. Hackerangriffe, Identitätsdiebstahl, Virenbefall und unreflektiertes Verhalten auf Sozialen Medien als mögliche Gefahren. Insbesondere jüngere NutzerInnen, die nach dem Wunsch Beliebtheit und Anerkennung zu erlangen handeln, teilen möglicherweise Bilder oder Inhalte auf Sozialen Netzwerken, und sind sich über zukünftige Konsequenzen nicht bewusst.

> *„Das Veröffentlichen von Persönlichen Daten wie Fotos, Adressen aber auch eigenen Interessen auf verschiedenen Webseiten (Facebook, Instagram, Twitter …) haben viele Konsequenzen. Für Anerkennung und Beliebtheit sind viele (vor allem jüngere) Nutzer bereit, ihre Privatsphäre herzugeben.“ (Sima C.)*

Des Weiteren sind Profile öffentlich und ermöglichen es so jedem auf die Inhalte zuzugreifen. So können sich online veröffentlichte Daten ggf. negativ bei der Jobsuche oder ähnlichem auswirken.

> *„Das alles kann sich irgendwann auf der Suche nach einem Arbeitsplatz, auf den Arbeitgeber auswirken. Wenn die Einträge mit dem realen Namen verknüpft sind, können diese ohne Schwierigkeiten per Suchmaschine aufgespürt werden, dass ist vielen nicht bewusst.“ (Nur S.)*

Eine Annahme ist, dass sich NutzerInnen nicht genug mit dem Thema Datenschutz auseinandersetzen.

Risiken bei Apps

Einige Apps auf dem Smartphone, iPad oder Laptop sammeln bspw. Standortdaten. Diese werden mit vorherigem Einverständnis abgefragt. Stimmt man der Standortabfrage nicht zu, können teilweise einige Funktionalitäten oder gar die vollständige App nicht genutzt werden.

NutzerInnen treffen die Entscheidung des Datenzugriffs meist wenig informiert. Des Weiteren seien oftmals lange unverständliche Texte bei der Zustimmungsabfrage ein Hindernis.

> *„Obwohl viele Sachen wie z.B. der Zugriff auf den Standort mittlerweile abgefragt werden und man dessen explizit zustimmen muss, denke ich, dass viele Nutzer einfach auf "Zustimmen" klicken, da man entweder keine weiteren Informationen dazu erhalten kann, was das bedeutet, oder aber sich durch 5 Seiten eng beschriebenen Text quälen muss, für dessen Verständnis man zuvor ein Informatikstudium absolviert haben müsste." (Juliane K.)*

Hinzukommt, dass oftmals nicht ersichtlich wird, warum der Zugriff bspw. des Standortes bei der Verwendung einer Taschenlampen App notwendig ist. Des Weiteren stellen TeilnehmerInnen der Diskussion auch die großen Internetakteure, wie Google und Facebook sowie App-Betreiber in die Verantwortung die Privatsphäre ihrer Nutzer zu schützen.

Wann ist man Datenschutzkompetent?

TeilnehmerInnen führen an, dass man dann Datenschutzkompetenz ist, wenn man bewusst und achtsam mit seinen persönlichen Daten im Internet umgeht.

> *„Datenschutzkompetenz bedeutet für mich, ein bewusster und achtsamer Umgang mit persönlichen Daten und Privatsphäre." (Sima C.)*

Aus Nutzersicht beschreibt die Kompetenz die Fähigkeit seine eigenen Daten zu schützen. Dabei ist das Wissen über die im Internet gebräuchlichen Mechanismen, Kenntnisse über mögliche Gefahren und Wissen darüber, wie man auf diese Gefahren reagieren kann, unabdinglich. NutzerInnen sollten genau abwägen, welche Informationen sie preisgeben und welche Folgen dies haben kann. Im Mittelpunkt der Diskussion stand, bezogen auf die Datenschutzkompetenz, vor allem ein bewusster und reflektierter Umgang mit persönlichen Daten. Dabei sei Wissen über die Vermeidung von Online-Tracking und die Vermeidung von unsicheren Seiten ebenfalls nützlich.

> *„Wer sich richtig verhalten will, sichert alle seine Geräte gegen Tracker ab und vermeidet unsichere Seiten." (Kevin)*

Datenschutzkompetente Nutzer würden, aus Sicht der Nutzer, verschiedene Werkzeuge verwenden, um der Verfolgung im Netz entgegen zu wirken.

Informationen zum und Lernen über Datenschutz

Eine Empfehlung der Teilnehmenden, um mehr über Datenschutz zu erfahren, ist die Einholung von Informationen bei Anbietern, die auf das Thema spezialisiert sind. Des Weiteren

werden als Verantwortliche für die Aufklärung zu datenschutzrelevanten Themen die Politik sowie die Institution Schule und Lehrer genannt. Das Thema Datenschutz sollte gerade bei jungen Nutzern präsenter platziert werden, denn bereits Grundschüler sind im Besitz eines Smartphones.

> *„Ich denke ebenfalls, dass Menschen schon im Kindesalter, […] spätestens ab der Grundschule, mit Datenschutz konfrontiert werden sollten." (Sonja K.)*

Schüler sollte ein verantwortungsbewusster im Umgang mit digitalen Medien erlangen und auf mögliche Risiken aufmerksam gemacht werden.

Tipps zum persönlichen Datenschutz

Passwörter

Verwenden Sie sichere Passwörter, die aus einer Kombination aus Zahlen, Sonderzeichen, Groß- und Kleinschreibung besteht. Achten Sie dabei darauf, dass Sie für unterschiedliche Accounts je ein separates Passwort verwenden.

Browserauswahl und -einstellungen

Es existiert eine Vielzahl an verschiedenen Internetbrowsern, wie bspw. Google Chrome, Safari, Firefox, Opera, Microsoft Edge oder Brave. Internetbrowser öffnen UserInnen die Tür ins Internet. Die verschiedenen Browser unterscheiden sich jedoch in Bezug auf ihre Sicherheit und den Schutz der Daten ihrer NutzerInnen. Einige Browser, wie Firefox und Brave, verfügen bspw. standardmäßig über einen integrierten Tracking-Schutz. Bereits bei der Wahl ihres Browsers können Sie demnach Einfluss auf den Schutz ihrer Daten nehmen.

Des Weiteren können Browsererweiterungen, wie Werbeblocker und zusätzliche Trackingblocker installiert werden. Diese verhindern u. a. die Verfolgung ihres Suchverhaltens und unerwünschte Werbung. Beispiele für Browsererweiterungen finden Sie in den Werkzeugen zum Datenschutz.

Darüber hinaus können Sie in ihrem Internetbrowser Voreinstellungen treffen, die das Surfen im Internet sicherer machen. Bspw. kann das Abspeichern von Cookies untersagt bzw. eine Löschung der Cookies nach Abschluss der Browsersitzung aktiviert werden. Bei Cookies handelt es sich um Textdateien, die Daten zum Nutzerverhalten speichern und an Server übermitteln. Des Weiteren sollten die Passwörter nicht im Browser gespeichert werden. Verwenden Sie stattdessen bspw. eine Passwortverwaltungssoftware.

Soziale Plattformen

Überlegen Sie sich vor einer Registrierung jeweils genau, warum Sie sich auf diesem Netzwerk anmelden möchten. Nach einer Anmeldung stehen Ihnen im Einstellungsbereich des Sozialen Netzwerks jeweils verschiedene Privatsphäreeinstellungen zur Verfügung. Arbeiten Sie diese sorgfältig durch. Eingestellt werden können bspw. die Sichtbarkeit von Kontaktdaten und ob eine Anzeige in Suchmaschinen erfolgen soll oder nicht.

Suchmaschine

Mit Hilfe von Suchmaschinen sind gesuchten Informationen schnell gefunden. Eine Gefahr für den Nutzer besteht jedoch darin, dass einige Suchmaschinen über Suchverläufe, IP-Adressen und Tracking oftmals viele Daten über ihre Nutzer erfassen und diese bspw. für die Einblendung von nutzerbasierten Werbeanzeigen oder zur Analyse und kommerziellen Zwecken verwenden. Neben der Suchmaschine Google existieren noch andere Suchmaschinen, die oftmals mehr Schutz vor dem Tracking des Nutzerverhaltes bieten. Ein Beispiel für eine Suchmaschine, die Wert auf den Datenschutz ihrer Nutzer legt ist DuckDuckGo. Diese Suchmaschine sammelt weder ihre IP-Adresse, Nutzerdaten noch speichert sie ihre Suchhistorie.

Werkzeuge zum Datenschutz

Werkzeug	Typ	Funktion	Verfügbarkeit
Ghostery	Browsererweiterung	- Blockiert Werbung und Tracker - Tracker können manuell ent-/blockiert werden - Verfügt über Smartblocking - Webseiten können als vertrauenswürdig und eingeschränkte Webseiten eingestuft werden - Selbsterklärend	Kostenfreie und kostenpflichtige Version verfügbar
AdBlocker	Browsererweiterung	- Blockiert Werbung und Tracker - Tracker können manuell ent-/blockiert werden - Webseiten können als vertrauenswürdig und eingeschränkte Webseiten eingestuft werden - Detailansicht blockierter Tracker	Kostenfreie und kostenpflichtige Version verfügbar
AbBlock Plus	Browsererweiterung	- Blockiert Werbung und Tracker - Filterlisten können selbst angepasst und bearbeitet werden	Kostenfrei

		ebenso, wie Tracking- und Malwarelisten - Benutzerfreundlich	
Scriptsafe	Browsererweiterung	- Blockiert/stoppt JavaScripts - Standort, Like-Buttons werden ausgeblendet Nutzern wird angezeigt, wer Informationen von einem haben möchte - Nicht benötigte Elemente werden deaktiviert - Blockierung von Scripten kann zu Darstellungsfehlern und eingeschränkter Nutzbarkeit führen - verfügt über Smartblocking	Kostenfrei
Avira	Virenschutzprogramm	- Virenscanner scannt Datenverkehr im System und schlägt bei Auffälligkeiten Alarm - Virenprogramm stellt täglich neue Virendefinitionsdateien zur Verfügung - Prüft Dateien selbstständig	Kostenfrei, kann durch kostenpflichte Pakete erweitert werden
Kaspersky	Sicherheitsprogramm u. a. Virenschutzprogramm	- Je nach Paket unterschiedliche Leistungen - U.a. Virenscanner, bietet auch Internet Security zum Schutz der Privatsphäre etc.	Kostenpflichtig, jedoch kostenlose Testversionen der Sicherheitssoftware verfügbar
FireFox Browser	Webbrowser	- Steht für Privatsphäre und Datenschutz - Blockiert Tracker - Nicht auf Geräten vorinstalliert	Kostenfrei
Cliqz	Suchmaschine und Webbrowser	- Suchmaschine: mit der eine Schnellsuche im Internet durchgeführt wir - Arbeitete mit einem eignen Web-Index - Schütz vor Trackern und besitzt einen eingebauten Werbeblocker - Bei der Suche kann individuell eingestellt werden, ob Cookies, Werbung und Tracking aktiviert werden soll	Kostenfrei

		- Datenschutz steht im Mittelpunkt	
DuckDuckGo	Suchmaschine	- Verwendet verschiedene Dienste um Suchergebnisse zu generieren - Sammelt keine Nutzerdaten - Keine Speicherung von IP-Adressen, Suchhistorie - Nur die Cookies sind aktiv, die benötigt werden um Suchvorgang reibungslos zu gestalten - Legt viel Wert auf Privatsphäre	Kostenfrei, verfügbar für Android, IOS
Signal	Instant Messaging Dienst	- Schutz der Privatsphäre der Nutzer hat höchste Priorität - Kein Tracking, keine Werbung - Ende-zu-Ende Verschlüsselung - Unabhängiger Anbieter - Weniger verbreitet als WhatsApp	Kostenfrei, verfügbar für Android, IOS sowie Desktopversion vorhanden
Telegram	Instant Messaging Dienst	- Schutz der Privatsphäre der Nutzer hat höchste Priorität - Kann auf Android, iPhone und iPad genutzt werden - Ende-zu-Ende Verschlüsselung bei Geheimchat - Zugriff auf Nachrichten ist von mehreren Geräten aus möglich - Kostenlos, ohne Werbung und gebührenfrei - Weniger verbreitet als WhatsApp	Kostenfrei, verfügbar für Android, IOS sowie Zugriff über Browser
Posteo	E-Mailprovider	- Anonymer Mail-Account - Server stehen in Deutschland und unterliegen somit deutschen Datenschutzgesetzten (und werden mit Ökostrom betrieben) - Keine Speicherung der IP-Adresse - Verschlüsselung der Nachrichten - Werbefrei	1€/Monat
FileVault 2	Festplattenverschlüsselung	- Schützt vor unautorisiertem Zugriff auf Daten	Kostenfrei für Mac

		- Zu finden in den Systemeinstellungen unter Sicherheit - Bei Aktivierung wird Wiederherstellungsschlüssel festgelegt - Eine Anmeldung auf dem Mac ist nun nur mit dem Account-Passwort möglich - Leicht einzurichten Beim Vergessen des Passwortes ist weder das anmelden auf dem Mac möglich noch der Zugriff auf seine Daten	

Literatur

Bundesdatenschutzgesetzt (BDSG). Online verfügbar unter: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html, letzte Verifizierung 14.04.2020.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI) (2020a): BDSG und DSGVO – Garanten der informationellen Selbstbestimmung. Online verfügbar unter: https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/Das-BundesdatenschutzgesetzSichertPers%C3%B6nlichkeitsrechte.html, letzte Verifizierung 01.04.2020.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI) (2020b): Was ist Datenschutz? Online verfügbar unter: https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html, letzte Verifizierung 01.04.2020.

Datenschutzgrundverordnung (DSGVO). Online verfügbar unter: https://dejure.org/gesetze/DSGVO, letzte Verifizierung 14.04.2020.

Europäischen Menschenrechtskonvention. Online verfügbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063764, letzte Verifizierung 14.04.2020.

Grundgesetzt (GG). Online verfügbar unter: https://www.gesetze-im-internet.de/gg/BJNR000010949.html, letzte Verifizierung 14.04.2020.

Bundesverfassungsgerichts (BVerfG): Lebach-Urteil vom 5. Juni 1973.

Bundesverfassungsgerichts (BVerfG): Volkszählerurteil vom 15. Dezember 1983.

Förderhinweis

Dieser Artikel wurde im Rahmen des Projekts »Informationskompetenz und Demokratie (IDE): Bürger, Suchverfahren und Analyse-Algorithmen in der politischen Meinungsbildung« erstellt. Das Projekt wird durch das Niedersächsische Ministerium für Wissenschaft und Kultur im Rahmen der Ausschreibung „Zukunftsdiskurse“ aus Mitteln des Niedersächsischen Vorab gefördert.