„Das Geschäftsmodell heißt: Werbung anzeigen“

Im Gespräch mit Datenschutzexperte Daniel Lohninger

Daniel Lohninger, Christian Kitter, Jenny F. Schneider
Medienradar 05/2022

Das Thema Datenschutz ist spätestens seit Inkrafttreten der DSGVO stark in den Vordergrund gerückt, aber für viele Internetnutzer:innen kaum greifbar. Insbesondere wenn es darum geht, seine eigenen Daten besser zu schützen, können viele Menschen gar nicht einschätzen, wovor genau sie ihre Daten schützen sollen. Daniel Lohninger ist für die NGO epicenter.works tätig, die sich für Grund- und Freiheitsrechte im digitalen Zeitalter und einen sorgsamen Umgang mit den Chancen und Risiken der Technik einsetzen. Medienradar spricht mit ihm über Algorithmen, Filterblasen und vermeintliche Sicherheit durch Datenspeicherung sowie darüber, wie Jugendliche für das Thema sensibilisiert werden können.

Warum ist Datenschutz in den letzten Jahren überhaupt ein Thema geworden?

Es gibt das Menschenrecht auf Schutz der Privatsphäre und des Familienlebens. Das ist in der Europäischen Menschenrechtskonvention verankert, die die Grundlage für all unsere Gesetze und unser Zusammenleben bildet. Da geht es darum, dass jeder Mensch ein Recht auf Privatsphäre hat – auf seinen höchstpersönlichen Bereich, also sein Privatleben, sein Familienleben – und dass diese primär vor staatlichen Eingriffen geschützt wird. Nun gibt es dank der rasanten technischen Entwicklungen immer mehr Möglichkeiten, in das Privatleben von Menschen reinzuschauen und Daten darüber zu sammeln. Viele Firmen und auch staatliche Player haben Interesse daran, diese Technologien in eine Richtung weiterzuentwickeln, um möglichst effektiv Daten über das Privatleben von Personen sammeln zu können. Daher gibt es den Datenschutz.

> *„Beim Datenschutz geht es nicht darum, Daten zu schützen, sondern die Privatsphäre der Menschen zu schützen.“*

Wir befinden uns mitten in der Digitalisierung. Videotelefonie, Online-Kommunikation und Möglichkeiten des kollaborativen Arbeitens mit digitalen Technologien sind für uns selbstverständlich geworden. Das ist per se nichts Schlechtes, aber dadurch entsteht eine Menge an Daten, wo das Sammeln der Daten und das Grundrecht auf Privatsphäre gegeneinander abgewogen werden sollten: wie notwendig ist das Sammeln der Daten, wofür werden sie gesammelt und um welche Daten handelt es sich überhaupt?

Für Datenschützer sind das keine neuen Themen. Wir warnen schon seit vielen Jahren davor, dass das Sammeln von Daten auch Probleme nach sich zieht und dass diese Daten natürlich nie hundertprozentig sicher sind, sondern es Datenskandale geben wird: Daten tauchen irgendwo auf, wo sie nicht auftauchen sollen oder werden von verbrecherischen Organisationen oder Leuten genutzt, die sich daran bereichern wollen. Da immer mehr Daten gesammelt werden, passieren solche Skandale jetzt auch immer öfter und tauchen als Thema verstärkt in den Medien auf.

Was denken Sie: Warum würden Kinder und Jugendliche einem Eisverkäufer keine persönlichen Informationen anvertrauen, haben im Gegensatz dazu aber im Netz keine Bedenken, ihre Daten preiszugeben?

Evolutionär betrachtet wurden wir Millionen Jahre darauf vorbereitet einzuschätzen, wie wir mit Menschen umgehen, die uns von Angesicht zu Angesicht gegenüberstehen. Eine Firma wie Instagram ist aber etwas Unpersönliches ohne Gesicht. Für den Einzelnen erschließt sich nicht, wofür die Daten genutzt werden, wie sie zusammengeführt werden und was unsere Profildaten über uns erzählen. Die Gefahr wird nicht thematisiert, sie ist einfach sehr abstrakt und nicht fassbar. Und mal abgesehen von personalisierter Werbung spüre ich nicht sofort direkte Auswirkungen dieser Datensammlung. Ich sehe nicht, dass diese Daten mit anderen Firmen geteilt werden, ich sehe nicht, dass ich Fotos nicht mehr löschen kann – auch wenn ich glaube, dass ich sie gelöscht habe.

Die Vorteile der ganzen Apps und Services sind aber enorm, weswegen viele dieser Apps kaum noch wegzudenken sind. Überwiegen die Vorteile der Datenspeicherung dann nicht auch einfach den Nachteilen?

Die Technologie ist per se nicht schlecht und das Angebot der Apps oft sehr gut. Zudem sind die Apps ja auch so gemacht, dass sie sehr viel Spaß machen, damit man dort möglichst viel Zeit verbringt. Die Auswirkungen der Datenspeicherung sind dabei für den Einzelnen schwer greifbar. Das ist auch dadurch begründet, dass die Information, was gespeichert wird und wie die Daten weitergegeben und genutzt werden, oft bewusst verschleiert wird.

Tatsächlich hat die Datenspeicherung auch noch viele gesamtgesellschaftliche Auswirkungen, die noch abstrakter sind und vom Einzelnen bei der alltäglichen Nutzung kaum erfasst werden können. Wenn beispielsweise Gesundheitsdaten über alle Menschen nicht mehr geschützt werden und diese früher oder später – wenn auch unabsichtlich – öffentlich werden, dann würde unser Gesundheitssystem mit Versicherungen nicht mehr funktionieren. Denn dann

könnte es sein, dass man einfach keine Versicherung mehr bekommt, wenn man eine genetische Vorerkrankung hat – zumindest nicht mehr zu denselben Konditionen. Es geht daher beim Datenschutz nicht nur um die Freiheit von jedem Einzelnen, sondern vor allem um die Auswirkungen auf leicht angreifbare Gruppen wie Minderheiten oder die Gesellschaft als Ganzes.

Viele Firmen wie Meta Platforms (ehem. Facebook Inc.) legen sogar Daten über mich an, wenn ich deren Anwendungen gar nicht nutze. Dies geschieht durch die Erstellung sogenannter Schattenprofile, wenn Freunde Facebook nutzen und dabei automatisch Daten über mich an die Firma weitergeleitet werden. Häufig speichern Unternehmen zudem nicht nur meine Handlungen in der App, sondern setzen Trackingcookies und Analysetools ein, mit deren Hilfe sie mein Verhalten auf fast jeder Website, auf der ich unterwegs bin, beobachten. Ich bin mir gar nicht sicher, ob die jungen Menschen sich bewusst sind, was alles an Datenspeichermöglichkeiten ausgeschöpft wird von den Unternehmen. Das geht soweit, dass ich an Tastaturanschlägen Gemütszustände ablesen kann. Wie soll ich da noch die Auswirkungen erfassen, wenn ich solche Methoden nicht kenne und gar nicht weiß, was eigentlich alles über mich an Daten erfasst wird.

Algorithmen wird vorgeworfen, uns zu beeinflussen und in Filterblasen gefangen zu halten, die uns nur einseitig informieren. Ist das problematisch? Bzw. bewegen wir uns in der realen Welt nicht auch in einer gewissen Blase, die wir selbst geschaffen haben?

Ein Algorithmus ist erstmal nur eine Handlungsanweisung. Wir sprechen hier aber von ganz bestimmten Algorithmen auf Social-Media-Plattformen und solchen Algorithmen, die mir zum Beispiel Informationen vorauswählen. Da entstehen dann sogenannte Filterblasen: mir werden nur noch Informationen angezeigt, die meine Meinung bestärken. Wir wissen, dass die Timelines der Apps so gebaut sind.

Natürlich leben wir auch in der realen Welt immer in einer gewissen Blase – sei das jetzt unsere berufliche Blase oder die unseres Privatlebens, wo wir uns auch nur mit gewissen Leuten umgeben, die uns ähnlich sind oder ähnliche Interessen haben. Aber im realen Leben ist diese Blase natürlich gewachsen, während die Social-Media-Plattformen zum Großteil so gebaut sind, dass sie hier nicht irgendetwas Natürliches abbilden wollen, sondern sie verwenden Algorithmen, um ihr Geschäftsmodell zu fördern.

Das Geschäftsmodell heißt: Werbung anzeigen. Um viel Werbung anzeigen zu können, muss ich die Leute möglichst lange in der Software halten und sie dazu bringen, dass sie sie lange nutzen. Dazu werden sämtliche Maßnahmen getroffen, um möglichst viele Botenstoffe in meinem Gehirn zu aktivieren, damit es mir viel Spaß macht, diese App zu nutzen und ich sie nur schwer wieder weglegen kann.

Und das funktioniert auch sehr gut. Es gibt Leute, die das besser kontrollieren können und einen sehr gezielten Umgang damit haben, aber auch andere, die das weniger gezielt machen. Aber prinzipiell ist es so gebaut, dass es funktioniert.

In der Filterblase zu stecken heißt nicht, dass ich absolut keine anderen Informationen mehr bekomme. Mir sollte einfach bewusst sein, dass die Inhalte nicht nur nach meinen Interessen geordnet und gefiltert sind, um mir die beste Information zu bieten, sondern oft um mich zu beeinflussen. Ich sollte bewusst meinen Medienkonsum hinterfragen. Das ist bei Zeitungen nicht anders, auch da sollte ich mir überlegen, welche Zeitungen ich eigentlich lese, wer dahintersteht und ob ich vielleicht auch mal was anderes lesen möchte.

Von einigen Kritiker:innen wird die Filterblase infrage gestellt, da ihrer Meinung nach auch in gefilterten Inhalten durchaus verschiedene Meinungen abgebildet werden ...

Ein positiver Aspekt des Internets ist, dass ich dort Leute von überall auf der Welt treffen und mich zu unterschiedlichen Meinungen schnell austauschen kann. Ich finde problemlos Gleichgesinnte, selbst wenn ich ein totales Nischeninteresse habe.

Aber Portale wie Facebook, TikTok oder Instagram sind eben nicht so gebaut, dass ich auf möglichst viele verschiedene Meinungen treffe, sondern dass ich nur in meiner Meinung bestätigt werde. Das löst bei mir aus, dass ich mich dort wohlfühle und möglichst lange bleibe. Das große Problem ist auch nicht die Vorauswahl selbst, sondern die Art und Weise der Vorauswahl, die nicht transparent ist. Datenschützer fordern daher von den Firmen, dass sie ihre Algorithmen transparent machen, damit nachvollziehbar ist, wie ausgewählt wird. Aber das ist momentan noch deren Geschäftsgeheimnis.

> *„Das große Problem ist nicht die Vorauswahl selbst, sondern die Art und Weise der Vorauswahl, die nicht transparent ist.“*

Nun ließe sich argumentieren, dass wenigstens in den Nutzerkommentaren verschiedene Meinungen abgebildet werden. Aber die Kommunikation im Internet funktioniert eben anders und auch Nachrichtenportale leben davon, dass sich möglichst viele User auf ihrem Portal bewegen, um die Werbeeinnahmen zu steigern. Die Kommentare, die mir als Erstes angezeigt werden, sind nicht etwa diejenigen, die eine sachliche Diskussion fördern, sondern solche, die am meisten Emotionen auslösen. Und das sind oft Kommentare, in denen wirklich derbe Sprache genutzt wird. Das sorgt für Konflikte und mehr Nutzer, die wiederum darauf reagieren. Die Kommentarfunktion hat also oft eine ganz andere Intention als die der Diskursförderung.

Im Zusammenhang mit der Datenspeicherung fällt häufig das Argument der Sicherheit – so auch beim Thema Vorratsdatenspeicherung, welches vor ein paar Jahren diskutiert wurde. Was genau war problematisch an der ursprünglich mal beschlossenen Vorratsdatenspeicherung?

Die Vorratsdatenspeicherung ist ein gutes Beispiel für eine Form von übermäßiger staatlicher Überwachung. Vorratsdatenspeicherung heißt, dass Firmen per Gesetz großflächig und allumfassend bestimmte Daten über ihre Kunden bzw. Nutzer sammeln müssen. Diese müssen dann für einen gewissen Zeitraum von mehreren Monaten oder Jahren aufbewahrt werden, damit die Kriminalpolizei im Fall eines Verbrechens darauf zugreifen kann. Das können Bewegungsdaten, Kommunikationsdaten oder Metadaten sein, zum Beispiel wer mit wem wann gesprochen hat. Auch wenn der Kommunikationsinhalt dadurch nicht erfasst wird, so lassen sich anhand der Metadaten sehr gut (auch psychologische) Profile erstellen und viele Aussagen über Personen treffen.

> *„Der Bürger hat ein Recht darauf, unbeobachtet zu sein. Er hat das Recht, ein Buch zu lesen, ohne dass der Staat weiß, welches Buch das ist."*

Nachdem vor ein paar Jahren von der EU eine Vorratsdatenspeicherung zunächst beschlossen wurde, gab es 2014 das Urteil vom Europäischen Gerichtshof, dass eine Vorratsdatenspeicherung nicht mit dem Recht auf Privatsphäre vereinbar ist.[1] Der Grund: In einem demokratischen Rechtsstaat liegt die Rechtfertigungslast beim Gesetzgeber, also bei der Regierung – und nicht beim Bürger. Der Bürger hat ein Recht darauf, unbeobachtet zu sein. Er hat das Recht, ein Buch zu lesen, ohne dass der Staat weiß, welches Buch das ist. Er hat das Recht, die Nacht woanders zu verbringen, ohne dass der Staat weiß, wo er die Nacht verbracht hat. Das heißt also, es muss zuerst ein Anlass im Einzelfall, wie ein vermuteter Gesetzesverstoß, da sein, und erst dann ist es gerechtfertigt, dass der Staat eingreift und Untersuchungen anstellt. Aber eben nicht im Vorfeld allumfassend für alle Bürger. Das hat dann mit einem demokratischen und liberalen Rechtsstaat nichts mehr zu tun, da gleitet man ab in eine Diktatur.

Befürworter:innen der Vorratsdatenspeicherung argumentieren immer wieder, dass Verbrecher:innen dadurch schneller überführt würden – und dass Bürger:innen, die gegen kein Gesetz verstoßen haben, schließlich auch nichts zu befürchten hätten …

Im Jahr 2013 hat Edward Snowden aufgedeckt, wie massiv die USA Daten von Bürgern auf der gesamten Welt speichern und nutzen. Er hat zuvor selbst für verschiedene Geheimdienste gearbeitet und hat dann diese Informationen veröffentlicht (NSA-Affäre). Snowden sagte, zu argumentieren, dass man sich nicht um das Recht auf Privatsphäre kümmere, weil man nichts zu verbergen hätte, ist

nichts anderes als zu sagen, dass Meinungsfreiheit nicht wichtig ist, weil man nichts zu sagen hat.

In einem liberalen Rechtsstaat haben Bürger ein Recht auf ihre Privatsphäre, andernfalls gleitet das ab. Natürlich leben wir in einem relativ liberalen Staat und haben eine demokratische Staatsform, aber trotzdem ist es nicht perfekt. Wir wissen, dass es immer wieder Korruption gibt und dass Macht ausgenutzt wird. Und deswegen ist es wichtig, dass man hier Grenzen zieht, weil die sonst immer weiter verschoben werden.

Es ist immer eine Machtverschiebung, wenn Einzelne ganz viel über andere wissen, vor allem wenn der Staat massiv über alle Bereiche seiner Bürger Bescheid weiß. Daher muss es diese versteckten Bereiche – die Privatsphäre – geben, um das Machtgleichgewicht zu erhalten. Wir sprechen hier immer über einen transparenten Bürger statt über einen transparenten Staat, obwohl das eigentlich viel wichtiger wäre, dass wir als Bürger in der Demokratie mehr über die Funktionsträger wüssten – und nicht umgekehrt.

Das Argument der Sicherheit wird gerne aufgegriffen, da Befürworter:innen meinen, dass durch Vorratsdatensammlung unschuldige Bürger:innen besser geschützt werden könnten – insbesondere bei Großveranstaltungen.

Grundlegend werden hier zwei Sachen miteinander verglichen, die man nicht automatisch gegeneinander abwägen kann: Datenschutz und Sicherheit. Aber das sind keine Waagschalen, wo automatisch Sicherheit entsteht, wenn ich Datenschutz wegnehme. Mir ist noch nie eine Studie untergekommen, die definitiv nachweisen kann, dass die Speicherung von Daten oder die Mehrüberwachung zu mehr Sicherheit führen würde. Ganz im Gegenteil: Es gibt viele Studien aus Ländern wie England, wo Videoüberwachung im öffentlichen Raum schon lange sehr massiv eingesetzt wird, die belegen, dass es zu keinem effektiven Rückgang von Kriminalität kommt. Stattdessen werden die Verbrechen zum Teil einfach nur in andere Bereiche verdrängt, wo es keine Videoüberwachung gibt.[2]

> *„Datenschutz und Sicherheit sind keine Waagschalen, wo automatisch Sicherheit entsteht, wenn ich Datenschutz wegnehme.“*

Ich glaube, dass es viel effektiver wäre, sich mit den Gründen von Verbrechen auseinanderzusetzen und andere gesellschaftliche Lösungen zu suchen – Prävention, andere polizeiliche Maßnahmen – als hier einfach mit politischem Aktionismus zu agieren und Datenschutz, die Freiheit der Bürger und damit auch die Sicherheit eines demokratischen Rechtsstaats aufzugeben.

Ganz unabhängig von dem, was der Staat gerne über seine Bürger:innen speichern möchte, gibt es auch massive Datenspeicherung in Bereichen, in denen gar keine Notwendigkeit dafür bestünde, zum Beispiel bei Gesundheits-Apps. Unter dem Vorwand, die Gesundheit zu fördern, werden Unmengen an Gesundheitsdaten aufgezeichnet – und vielfältig verarbeitet. Wo liegen die Probleme bei diesem sogenannten Self-Logging- bzw. Self-Tracking-Trend?

Die technischen Möglichkeiten des Self-Trackings sind sehr verführerisch. Daher ist es absolut verständlich, dass man sie einsetzen will. Damit uns dieser Service jedoch überhaupt zur Verfügung gestellt wird, werden unsere Gesundheitsdaten auf irgendeinem Firmenserver gespeichert und analysiert.

Generell stellt sich hier folgende Frage: inwieweit ist es überhaupt notwendig, dass ich diese Daten hergebe und dass sie geteilt werden? Wäre es nicht besser, wenn sensible Daten nur bei mir auf meinem Gerät bzw. in meiner App behalten und nicht auf Firmenserver geschickt werden? Natürlich darf man nicht vergessen, dass viele Firmen genau davon leben, diese Daten zu nutzen und weiterzugeben bzw. zu verkaufen. Und da sind Gesundheitsdaten für andere natürlich besonders interessant, um Profit damit zu machen. Im Gegenzug sind diese Tools dann häufig kostenlos oder sehr günstig. Wichtig ist hier allem voran, eine bewusste Entscheidung zu treffen, denn wir wissen viel zu wenig darüber, inwieweit die Firmen für ausreichende Sicherheitsmaßnahmen sorgen, um unsere Daten zu schützen.

Eine weitere Frage betrifft den Aspekt, wie diese Daten in Zukunft genutzt werden könnten, um zum Beispiel Entscheidungen über mich zu treffen. Habe ich aufgrund meiner Daten noch Anrecht auf eine Rentenversicherung? Auf welche Daten hat ein Arbeitgeber Zugriff, falls ich mich auf einen neuen Job bewerben möchte? Man sollte vor der willkürlichen Nutzung solcher Self-Tracking-Anwendungen schon kritisch hinterfragen, welchen Anbieter man wählt, welches Sicherheitsniveau gilt und wie viele Daten man preisgibt. Muss man wirklich alles tracken, alles sofort smart machen oder wartet man mit gewissen Dingen vielleicht noch?

Das klingt plausibel. Allerdings haben viele Menschen das Gefühl, es sei ohnehin schon zu spät, da sie in den vergangenen Jahren schon sehr viel von sich preisgegeben haben. Die Firmen wüssten eh schon alles über sie, sodass ein Umschwenken zu einer bewussteren und verantwortungsvolleren Nutzung keinen Unterschied mehr machen würde. Ist dem so?

Das ist etwas zu schnell aufgegeben und zu weit gedacht. Zu sagen, es ist eh schon alles verloren, verkennt eigentlich die gute Situation, in der wir leben, denn: dieser Kampf ist noch nicht entschieden – und er ist auf keinen Fall vorbei. Wir sind jetzt genau in der Zeit, in der die Gesetze geschrieben werden, die die Grundlage dafür

bilden, wie wir diese Technologien nutzen werden. Die EU-Datenschutzgrundverordnung gibt es ja auch erst seit wenigen Jahren. Vorher waren Strafen bei Datenschutzverletzungen extrem niedrig, in Österreich waren es, glaube ich, ein paar 10.000 Euro. Für einen amerikanischen Großkonzern hätte es sich nicht einmal gelohnt, einen Anwalt zu nehmen, der sich das Gesetz anschaut – der kostet nämlich mehr. Und jetzt haben wir seit Inkrafttreten der EU-DSGVO (Mai 2017) Strafen, die in die Milliarden gehen, und deutlich schärfere Gesetze. Das Internet, wie wir es heute kennen, wurde in seinen Anfängen bewusst so gebaut, dass es den demokratischen Austausch von Wissen und Software ermöglicht, indem es keinen Unterschied bei der Übertragung von Daten macht. Das hat die Innovation, Vielfalt und die gesellschaftliche Teilhabe im Netz erst ermöglicht. Bestrebungen, das Prinzip der Netzneutralität anzugreifen, wurden durch die gesetzliche Absicherung in der EU erfolgreich verhindert.[3] Über diese Spielregeln entscheiden wir gerade alle gemeinsam.

Wie können Jugendliche überhaupt lernen, verantwortungsbewusst mit ihren Daten umzugehen?

Das Internet ist eine enorme Erfindung mit großen Auswirkungen auf die Gesellschaft – wahrscheinlich ist diese Erfindung nur mit dem Buchdruck zu vergleichen. Und da wir da alle noch mittendrin stecken, ist es für Jugendliche nicht einfach, dieses Thema zu verstehen.

Hier kommt natürlich den Bildungsinstitutionen eine sehr wichtige Aufgabe zu. Sie müssen vermitteln, welche ganz persönlichen Auswirkungen der verantwortungsbewusste Umgang mit Daten hat. Es ist schon möglich, bei den eigenen Daten zu differenzieren: Welche gebe ich preis und welche lieber nicht? Was ist ein sicheres Passwort? Welche Möglichkeiten habe ich, mit engen Bezugspersonen auf anderen Wegen zu kommunizieren und wie kann ich Softwareservices oder Apps für mich richtig einordnen?

> *„Wenn ich eine App gratis nutzen kann, dann ist ziemlich klar, dass hier ein anderes Geschäftsmodell dahintersteht, als wenn sie anderweitig finanziert wird."*

Ein wichtiges Indiz dafür ist natürlich die Frage, wer dahintersteckt und was deren Geschäftsmodell ist. Mir ist klar, dass die Datenschutzerklärungen nicht so geschrieben sind, dass man sie gerne liest und auch schnell versteht. Deswegen ist es darüber hinaus wichtig, Gesetze zu schaffen – ähnlich wie im Konsumentenschutz –, die ein gewisses Grundmaß an Sicherheit bieten.

Welche Möglichkeiten haben Jugendliche, die Apps und Plattformen, die sie nutzen, zu hinterfragen?

Um Apps und Plattformen zu hinterfragen, braucht man in einer Suchmaschine einfach nur mal die App in Verbindung mit dem Wort „Kritik" einzugeben, dann findet man schnell heraus, welche Kritik daran geäußert wird. Zu wissen, was hier überhaupt beanstandet wird und welche negativen Seiten es gibt, hilft einem, die App selbst für sich einzuordnen.

Oftmals lässt sich auch schon beim Anmeldeprozess schnell herausfinden, wie ein Portal gestrickt ist. Würde eine App von Anfang an kenntlich machen, nach welchen Kriterien hier die Reihenfolge der Inhalte festgelegt wird oder welche Möglichkeiten User haben, mitzuentscheiden, dann wäre es für den Nutzer nachvollziehbar. Viele Portale informieren den Nutzer aber nicht darüber, weil sie in der Regel andere Intentionen haben. Und darüber kann man sich schon ganz gut selbst informieren, welches Portal wie funktioniert.

Welchen Rat kann man Jugendlichen an die Hand geben und wie kann die Medienpädagogik sie darin unterstützen?

Jugendliche müssen vor allem verstehen, was die Intention von Gratis-Apps ist und warum der Service kostenlos zur Verfügung gestellt wird. Dass Jugendliche das Internet nutzen, ist ganz normal, und genau da kann man ansetzen.

Es macht zum Beispiel einen großen Unterschied, ob ich nur WhatsApp oder sonstige Messenger von Firmen nutze, die viele Daten sammeln, um ihr Geschäftsmodell zu betreiben, oder ob ich zum Beispiel auf Alternativen setze, wie Signal. Dort kann ich sicher kommunizieren und weiß, dass meine Daten nicht abgefangen, meine Kommunikation nicht gelesen werden kann.

Auch hinsichtlich des genutzten Internetbrowsers kann man eine bewusste Entscheidung treffen, denn nicht jeder Browser ist gleichermaßen datenschutzfreundlich. Es macht einen Unterschied, ob man den Google Chrome Browser nutzt, der eine enorme Marktbreite in Europa hat, oder aber den open-source-entwickelten Browser Mozilla Firefox. Dazu muss man natürlich wissen, welchen Unterschied es macht, wenn ein Programm open-source-programmiert ist, der Quellcode also offenliegt. Ein offenliegender Quellcode ist nämlich für jeden einsehbar. So können Programmierer konkret erkennen, was genau das Programm macht.

Darüber hinaus kann ich meine Browser auch noch zusätzlich aufwerten, indem ich bestimmte Add-ons installiere, die meine Privatsphäre erhöhen. Das sind Add-ons wie zum Beispiel Privacy Badger, die Cookies automatisch blockieren und mein Verhalten im Internet somit nicht mehr für sämtliche Firmen nachvollziehbar macht.

Auch Werbung, die oft ein Sicherheitsrisiko darstellt, lässt sich blockieren – zum Beispiel mit uBlock Origin. Darüber hinaus gibt es noch weitere praktische Add-ons.[4]

Dieses Wissen über den selbstbestimmten Umgang muss für junge Menschen zielgruppengerecht aufbereitet und ihnen ohne erhobenen Zeigefinger nahegebracht und zur Verfügung gestellt werden. Das müssen wir als eine der wichtigsten Bildungsaufgaben der Gesellschaft begreifen und vielfältig vorantreiben. Als zivilgesellschaftliche Organisation mit Expertenwissen sehen wir das auch als unsere Aufgabe. Deshalb sind wir gerade am Aufbau einer Bildungsinitiative für Jugendliche in der Berufsausbildung, um das Bewusstsein für Datenschutz, das Wissen um rechtliche Rahmenbedingungen sowie technische Hilfestellungen zu vermitteln. Dafür arbeiten wir an einem offenen E-Learning, das wir online zugänglich machen, der Schulung von Trainer:innen und einem Workshopangebot für Schulen. Unterstützt wird das Vorhaben von Arbeiterkammer Niederösterreich, der gesetzlichen Vertretung der Arbeiter und Angestellten, durch eine Förderung im Rahmen des Projektfonds Arbeit 4.0.

Bleibt zum Schluss die Frage, wie gehen Sie ganz persönlich mit Ihren Daten um?

Ich nutze viele dieser gerade genannten Tools und weitere, um meine Privatsphäre zu erhöhen. Für die private Kommunikation, das heißt mit meinen engen Bezugspersonen und meiner Familie, nutze ich ausschließlich sichere Messenger. Die sind Open Source und sie sind so gebaut, dass sie möglichst wenig Daten speichern (Privacy-by-Design). Mir ist auch wichtig, welchen Browser ich nutze und dass nicht alles, was ich mir im Internet anschaue, nachverfolgt und gespeichert wird.

Quellen

1. Vgl. Epicenter.works: *Vorratsdatenspeicherung. Alle Menschen unter Generalverdacht*, https://epicenter.works/thema/vorratsdatenspeicherung (abgerufen am 14.04.2022).

2. Vgl. Demuth, Kerstin: *Wissenschaftliche Materialsammlung: Wirkt Videoüberwachung?*, in: digitalcourage vom 06.05.2017, https://digitalcourage.de/videoueberwachung/materialsammlung (abgerufen am 14.04.2022).

3. Vgl. Epicenter.works: *Netzneutralität. Gleichbehandlung aller Daten*, https://epicenter.works/thema/netzneutralitaet (abgerufen am 14.04.2022).

4. Epicenter.works: Digitale Selbstverteidigung, https://epicenter.works/crypto (abgerufen am 14.04.2022).