DIGITAL CHECK NRW

Digital weiterwissen.

#digitalweiterwissen

Das Magazin Ausgabe 04 (2025)

Schwerpunkt Datenschutz

Ratgeber Demokratie online | Gesundheitsdaten | Künstliche Intelligenz |

INHALT

#digitalweiterwissen
Das Magazin 04

VORWORT

Liebe Leserinnen und Leser,

wir alle leben in einer digitalen Welt. Wir kommunizieren weltweit, teilen Fotos, finden schnell Informationen und erledigen Einkäufe oder Bankgeschäfte bequem von zu Hause. Die Digitalisierung bietet uns enorm viele Vorteile und Chancen, aber die rasanten Entwicklungen haben auch Veränderungen mit sich gebracht. So können manche alltägliche Dinge nur noch online oder per App erledigt werden, z. B. Ticketkäufe, Paketabholungen an Packstationen oder die Vereinbarung von Terminen in Praxen oder Ämtern. Sofern du über entsprechende digitale Geräte verfügst und damit zurechtkommst (oder Hilfe bekommst), sind diese Prozesse einigermaßen zu bewältigen. Was aber – quasi unsichtbar – noch dazu kommt, sind die Datenspuren, die du bei all diesen Vorgängen hinterlässt: je nach Dienst/App, z. B. Standort-, Bewegungs- oder Sensor-Daten, auf dem Gerät gespeicherte Kontaktdaten und Fotos sowie Informationen, wie und wann du eine App genutzt hast.

Vielleicht denkst du: „Ich habe doch nichts zu verbergen.“ Doch Datenschutz bedeutet viel mehr, als nur Geheimnisse zu bewahren. Es geht darum, deine Persönlichkeitsrechte zu schützen – also das, was dich als Mensch ausmacht: Deine privaten Informationen, deine Gewohnheiten, deine Bilder und deine Entscheidungen. Wie sensibel diese Daten sind, bewertest oftmals gar nicht du selbst, denn es kommt darauf an, wofür sie von anderen verwendet werden. So kann es z. B. gewinnbringend für dich sein, deine Schlafgewohnheiten über das Smartphone, eine Smartwatch oder ein digitales Fitnessarmband überwachen zu lassen, aber wenn die Daten über deinen ungesunden Schlaf an Versicherungen weitergegeben werden und dir damit höhere Beiträge drohen, dann wirkt sich dies direkt auf deine Lebensrealität aus – und solche Zusammenhänge machen Firmen nur selten transparent.

Datenschutz ist kein Thema nur für Expert*innen – es betrifft jede und jeden von uns. Und mit ein wenig Wissen kannst auch du bereits selbstbestimmt und sicher mit deinen Daten umgehen. In diesem Magazin geben wir dir viele wertvolle Tipps an die Hand.

Viel Freude beim Lesen
wünscht der #DigitalCheckNRW!

INTERVIEW: „DATENSCHUTZ IST EIN GRUNDRECHT!“

Friedemann Ebelt

Herr Ebelt, Sie setzen sich für eine Digitalisierung ein, bei der die Grundrechte der Bürger*innen gewahrt werden, und appellieren für den Schutz personenbezogener Daten auf ethischer, gesellschaftlicher und politischer Ebene. Was bewegt Sie dazu?

Ich denke, dass wir bei der Gestaltung der Digitalisierung sehr intensiv darauf achten müssen, dass wir uns als Gesellschaft eine nachhaltige und gemeinwohlorientierte digitale Zukunft bauen. Wichtig dabei ist die Machtfrage. Wer entscheidet darüber, welche Daten eine App über mich sammelt? Welche Interessen verfolgen die großen Kommunikationsplattformen? Wer macht die Regeln? Wer hat die Kontrolle über meine Daten? Wenn die Antwort auf diese Fragen lautet: ein großer Tech-Konzern, dann ist das ein Problem. Denn dann reden wir mehr darüber, was eine Handvoll großer Tech-Konzerne und deren Eigentümer wollen, als darüber, was wir als Gesellschaft mit Digitalisierung erreichen wollen. Ich finde es faszinierend, wie wir mit digitaler Technik Wissen offen und frei zugänglich machen können, wie Menschen über Kontinente hinweg miteinander kommunizieren können und wie sich datenbasiert Prozesse verbessern lassen. Gleichzeitig ist es ernüchternd zu sehen, wie Desinformation und Hass im Internet verbreitet werden, wie anlasslose staatliche und kommerzielle digitale Überwachung hochgefahren wird und wie schwer es anspruchsvolle digitale Projekte haben. Ich denke, dieses Spannungsfeld motiviert mich.

„Datenschutz ist ein Grundrecht, das Menschen verschiedene Möglichkeiten gibt, sich gegen Übergriffe auf persönliche Daten zu wehren.“

Wo sehen Sie Entwicklungen, die Bürger*innen den Schutz ihrer Daten erschweren?

Datenschutz ist ein Grundrecht, das Menschen verschiedene Möglichkeiten gibt, sich gegen Übergriffe auf persönliche Daten zu wehren. Im Wesentlichen sind es der Staat und private Unternehmen, die auf persönliche Daten zugreifen. Hier will ich nicht pauschal sein.

Es gibt staatliche Stellen, wie die Datenschutzbeauftragten von Bund und Ländern, die das Grundrecht auf Datenschutz durchsetzen sollen. Es gibt auch Unternehmen, die absolut verantwortungsbewusst mit den Daten ihrer Kundschaft umgehen. Beide sind aktuell allerdings in der Defensive gegenüber Tech-Konzernen und gegenüber der Überwachungspolitik, die flächendeckende, dauerhafte und tiefgehende Übergriffe auf die Daten von Menschen voranbringt.

Auf staatlicher Seite sind es Großprojekte wie die anlasslose Vorratsdatenspeicherung von Internetverbindungs- und Telefon-Daten, Videoüberwachung, die Schwächung und Umgehung von Verschlüsselung sowie die sogenannte Chatkontrolle, bei der pauschal die Inhalte von privaten Chats automatisch gescannt werden sollen. In der Wirtschaft sind es Datenhandelsplattformen und die sogenannte Werbetrackingindustrie, die fortwährend technische und psychologische Methoden entwickeln, um Menschen noch präziser, noch umfassender und noch eindringlicher digital zu verfolgen, zu analysieren und zu beeinflussen. In vielen Bereichen arbeiten Unternehmen und Staaten zusammen, wie etwa die US-Überwachungsfirma Palantir mit einzelnen deutschen Landespolizeien.

Tech-Konzerne verfügen über sehr hohe Budgets und staatliche Überwachungsprogramme können flächendeckend ausgerollt werden. Demgegenüber sind Datenschutzbehörden ungleich schwächer ausgestattet und können oft nur punktuell wirken. Datenschutzfreundliche Unternehmen sind kleiner und werden zu wenig gefördert. Im Ergebnis ist es einfacher und bequemer, sich von Unbekannten digital durchleuchten zu lassen, als sich davor zu schützen.

Jede*r sollte beim Schutz von Daten bei sich selbst anfangen und an dem bestmöglichen Umgang mit den eigenen Daten arbeiten. Aber was können Bürger*innen tun, damit ihnen die Last der Eigenverantwortung etwas genommen wird?

Das ist tatsächlich eine Kernfrage in der Datenschutzdebatte.

Wer sich technisch und rechtlich für Datenschutz interessiert und sich dafür etwas Zeit nimmt, hat viele interessante Möglichkeiten, die eigenen Daten vor Übergriffen zu schützen. Es muss aber möglich sein, in ein Geschäft zu gehen, ein Smartphone zu kaufen, eine App zu installieren und diese

INTERVIEW: „DATENSCHUTZ IST EIN GRUNDRECHT!“

Friedemann Ebelt

zu nutzen, ohne dass im Verborgenen eine digitale Akte angelegt wird. Aktuell ist das nicht möglich. Ich muss davon ausgehen, dass mein Standort, meine Nutzungsdaten und mein Nutzungsverhalten in der einen oder anderen Form erhoben, gespeichert und an eine große Anzahl mir Unbekannter weitergegeben werden.

Hier müsste Regulierung ansetzen. Das heißt, der Gesetzgeber müsste klare Regeln erlassen und durchsetzen, am besten EU-weit. Mit der Datenschutz-Grundverordnung gibt es bereits eine solide Rechtsgrundlage. Allerdings betreiben datenhungrige Tech-Konzerne trickreiche und intensive Lobbyarbeit mit dem Ziel, diese Regeln zu umgehen und aufzuweichen. Dazu kommt: Politiker*innen, die großflächig an Daten von Bürger*innen interessiert sind, machen Druck in Parlamenten, Ministerien und Ausschüssen. Datenschutz wird dabei gern belächelt, als innovationsfeindliches Hindernis dargestellt und teilweise sogar als Täterschutz diffamiert – die Diskussionskultur ist hier teilweise sehr weit entfernt von Fakten und Fairness.

„… die Diskussionskultur ist teilweise sehr weit entfernt von Fakten und Fairness“

Jetzt zurück zur Frage: Zunächst ist es wichtig, die Situation immer wieder klar zu kommunizieren. Milliardenschwere Konzerne, die keine bis kaum Steuern zahlen, durchleuchten Bürger*innen weltweit rund um die Uhr, wortwörtlich bis auf die Unterhose. Hier muss bei jeder Gelegenheit politischer Druck gemacht werden.

Mal ein ganz anderer Aspekt: Wir tragen alle eine große Verantwortung für uns selbst, unsere Mitmenschen und unsere Umwelt. Der Betrieb von Software (Programmen) und Hardware (Geräten) verbraucht viel Energie. Dazu wird der Nutzung von Künstlicher Intelligenz ein besonders hoher Energieverbrauch nachgesagt. Wie würden Sie den Zusammenhang von Datenschutz und Klimaschutz beschreiben?

Smarte Geräte, Künstliche Intelligenz und Cloud-Anwendungen sind, ökonomisch gesprochen, riesige globale Märkte. Je mehr Smartphones gekauft und weggeworfen werden, je mehr Künstliche Intelligenz für alle eingesetzt wird und je mehr Daten gesammelt und verarbeitet werden, desto höher ist das Potenzial für Gewinne. Mit dem Konsum steigen natürlich die benötigten Ressourcen: seltene Rohstoffe, die oft aus Krisengebieten stammen, das Lebensmittel Wasser und natürlich Energie. Dazu kommt, dass sogenannte soziale Medien, Apps, Onlineshops immer weiter konsumverstärkend optimiert werden.

Ein Beispiel dafür ist, was ich als Müllfluencing bezeichne: Menschen mit sehr großer Reichweite in sozialen Medien verleiten ihr Publikum dazu, möglichst viele Dinge zu kaufen, die in vielen Fällen bereits nach kurzer Zeit auf dem Müll landen. Um diesen digitalen Konsum optimal anregen zu können, wollen Werbeunternehmen ihre Zielgruppen bestmöglich erreichen und beeinflussen. Dafür benötigen sie Daten über die Einkommensverhältnisse, die Vorlieben, den Wohnort, den Freundes- und Bekanntenkreis, den Beruf, die Lieblingsurlaubsziele und so weiter. Die Autorin Shoshana Zuboff nennt das Überwachungskapitalismus und hat darüber ein sehr lesenswertes Buch geschrieben.

„Studien bestätigen: Mit Digitalisierung produzieren wir mehr und nicht weniger Müll.“

Im Allgemeinen müssen Unternehmen dieses Vorgehen nicht rechtfertigen, weil Konsum unserem Wirtschaftssystem entspricht und das liefert, was die meisten Menschen am meisten wollen: Bequemlichkeit und Selbstwert. Bei den seltenen Gelegenheiten, bei denen Umweltauswirkungen von smarten Geräten und Künstlicher Intelligenz kritisch diskutiert werden, beobachte ich einen interessanten Effekt: Verantwortliche verweisen auf ökologische Chancen- und Risiken der Digitalisierung und betonen dabei die Wichtigkeit von Digitalisierung für die Energiewende. Das ist korrekt, doch die Umweltschäden der Digitalisierung haben wir trotzdem, auch wenn wir weniger Kohle verbrennen. Studien bestätigen: Mit Digitalisierung produzieren wir mehr und nicht weniger Müll.

Ich denke, wir sollten über Digitalisierung als Katalysator sprechen. In der Chemie sind Katalysatoren Stoffe, die die Geschwindigkeit einer Reaktion erhöhen. Genau das macht Digitalisierung mit Konsum und Umweltverbrauch in den

INTERVIEW: „DATENSCHUTZ IST EIN GRUNDRECHT!“

Friedemann Ebelt

meisten Bereichen. Konsumieren wird schneller, einfacher und flexibler. Das ist das Gegenteil von nachhaltigem, datenschutzfreundlichem und umweltverträglichem Wirtschaften. Böden und Wälder leiden unter Trockenheit und Giftstoffen, die Meere sind verdreckt von Plastik, das Artensterben und die Klimakrise spitzen sich immer weiter zu. Zu glauben, Digitalisierung hätte aus sich heraus darauf einen positiven Einfluss, ist falsch, naiv und gefährlich.

Wie würde ein Zukunftsszenario für Sie aussehen, in dem der Schutz von Daten von allen Beteiligten ganz selbstverständlich gelebt und umgesetzt würde?

Diese Frage wird leider viel zu selten gestellt! Wir brauchen dringend Szenarien, Utopien und Fahrpläne für eine gemeinwohlorientierte digitale Zukunft. Beim Verkehr ist klar, dass es eine Verkehrswende braucht, damit umweltverträgliche, bezahlbare und sichere Mobilität möglich wird. Wir wissen auch, dass es eine Energiewende braucht, damit die Folgen der globalen Erwärmung möglichst gering ausfallen. Aber noch haben wir als Gesellschaft nicht verstanden, dass wir auch dringend eine Digitalwende beginnen müssen. Denn nüchtern und langfristig betrachtet, schaden wir uns mit einer Digitalisierung, die für Werbung, Datenhandel, Bequemlichkeit und Konsumsteigerung optimiert ist. Aktuell kommen die spannendsten Ansätze dafür aus der Permacomputing-Bewegung. Hier übertragen Menschen die Idee einer dauerhaften Landwirtschaft auf die Digitalisierung. Das könnte so aussehen:

„Szenarien, Utopien und Fahrpläne für eine gemeinwohlorientierte digitale Zukunft“

Milliardenschwere Online-Handelsplätze, Social-Media-Plattformen und Big-Tech-Unternehmen zahlen angemessene Steuern wie jeder Handwerksbetrieb. Mit den Mehreinnahmen aus geschlossenen Steuerschlupflöchern werden bessere digitale Strukturen aufgebaut, die gemeinwohlorientiert, dezentral, offen und daten- sowie ressourcensparsam arbeiten. IT-Profis entwickeln nicht mehr Geräte und Anwendungen, die möglichst viele Gewinne abwerfen, möglichst viele Menschen möglichst lange vor einem Bildschirm fesseln und dabei möglichst viele Daten abgreifen, sondern sie entwickeln eine Digitalisierung, die messbar hilft, die 17 UN-Nachhaltigkeitsziele zu erreichen, wie hochwertige Bildung, Gesundheit und Wohlergehen, Geschlechtergleichheit und weniger Ungleichheiten. Geräte werden lange genutzt, repariert und recycelt. Software verarbeitet nur Daten, die notwendig sind. Was online funktioniert, funktioniert auch offline.

Plattformen gehören nicht wenigen Milliardären, sondern sind dezentral. Klimaschutz- und IT-Expert*innen arbeiten eng zusammen. Regierungen investieren in Soziales, gezielte Ermittlungsarbeit und Prävention statt in anlasslose Überwachung. Menschen werden mit Werbung und Tracking in Ruhe gelassen und bekommen stattdessen wirklich nützliche Produktinformationen. Komplizierte Datenschutzregeln sind nicht mehr nötig. Der Energieverbrauch sinkt und wir produzieren keinen Elektroschrott mehr. Keine Cookie-Banner – mehr Zeit für Pausen!

ÜBER DEN AUTOR

Friedemann Ebelt ist Medienwissenschaftler und Ethnologe sowie Autor. Er berät als Kommunikationsexperte öffentliche Einrichtungen und Unternehmen zu nachhaltiger Social-Media-Kommunikation im Fediverse.

DATENSCHUTZ SCHÜTZT NICHT DEINE DATEN, SONDERN DICH

Klaudia Zotzmann-Koch

„Datenschutz" klingt unglaublich staubig. Bei manchen löst das Wort regelrechten Widerwillen aus. Das ist verständlich, ist doch in unserer komplexen Welt alles schwieriger geworden. Allerdings fallen wir häufig auf die Erzählungen großer Datenkonzerne rein, die den Datenschutz als den großen Schuldigen hinstellen, der allen Fortschritt verhindert. Datenschutz, der alles komplizierter macht. Datenschutz, der daran schuld ist, dass … ja, was eigentlich? Bemerkenswert ist, dass es beim Datenschutz nur nebenbei um den Schutz von Daten geht, aber immer um den Schutz von Menschen. Insbesondere den Schutz von Menschen, die nicht zur breiten Masse gehören.

In der breiten Masse unterzutauchen, war lange Zeit mehr oder weniger einfach: sich angepasst kleiden, sich angepasst in der Öffentlichkeit verhalten und im Zweifelsfall mal nichts sagen. Zu Hause konnte man ja immer noch so sein, sagen und denken, was man wollte. Zu Hause konnte man sich mit Menschen treffen und bei einem gemeinsamen Essen über Gott und die Welt sprechen und niemand konnte einem das verbieten. Doch dank der Milliarden kleinen und großen Geräte überall, ist unser Rückzugsraum verschwindend klein geworden. Überall sind Kameras und Mikrofone, die potenziell mitschneiden, was wir sagen, wie und wo wir uns bewegen, uns aufhalten, mit wem wir kommunizieren. Auch in unserem Zuhause und unseren Hosentaschen. Und alles, was irgendwie über das Internet läuft, von der Apothekenbestellung über die Suche nach einer* einem Notar*in oder dem Stichwort „Prostatakrebs" bis zu Messenger-Nachrichten, was wir uns anschauen, wie viele Millisekunden lang wir das tun, wohin wir scrollen, mit wem wir kommunizieren, von wo aus, wann und wann nicht (wann wir schlafen) … wird von den Datenfirmen mit großem Eifer mitgeschnitten, ausgewertet und durch Werbeverkauf zu Geld gemacht. Und an genau dieser Stelle kommt der Datenschutz ins Spiel. Datenschutz schützt nämlich nicht deine Daten, sondern dich vor der Auswertung von allem, was du willentlich oder unwillentlich an digitalen Spuren im Netz hinterlässt. Kein Wunder also, dass Datenfirmen im Datenschutz ein enormes Übel sehen. Von denen gibt es übrigens sehr viele, nicht nur Alphabet und Meta, den Konzernen hinter Google und Facebook. Über 14.000 Unternehmen machen nichts anderes als unsere Datenspuren zu ernten, aufzubereiten und gegen uns zu verwenden. Es ist bedenklich, dass sich Politik und Medien oft genug davon mitreißen lassen und gegen den „bösen Datenschutz" wettern.

WIE FÜR DICH GEMACHT

Das große Schlagwort, mit dem die Datenbranche arbeitet, ist dabei „Personalisierung". Alles soll so persönlich wie möglich auf uns Einzelne zugeschnitten sein. Jetzt mag man denken, dass es in all der Datenflut ja ganz praktisch ist, wenn man Werbung angezeigt bekommt, die zu einem passt. Allerdings hat das einen ziemlichen Haken. Dass wir bunte Bildchen angezeigt bekommen, die uns interessieren könnten, ist ja nur der letzte Dominostein in einer langen Kette und das Einzige, was wir von der riesigen Maschinerie dahinter zu sehen bekommen. Was wir nicht sehen ist, wie perfide die Massendatenverarbeitung (Stichwort ›Big Data‹ und ›KI‹) die über uns vorhandenen Informationen auswertet und ausspielt. Und das sind mehr Informationen, als den meisten bewusst ist: Deine Suchanfragen, deine Internethistorie, was du dir angesehen hast, mit welchen Geräten du das tust, was auf diesen Geräten

DIE TOP-5 DINGE, DIE DU IN UNTER 5 MINUTEN TUN KANNST, UM DEN DATENFIRMEN EIN SCHNIPPCHEN ZU SCHLAGEN

1. Einen **Browser** verwenden, der dir erlaubt, einen guten Werbeblocker einzurichten. Mozilla Firefox ist der letzte freie Browser auf dem Markt und in Richtung Datenschutz sehr anpassbar. Firefox herunterladen und als Standard-Browser festlegen. → www.firefox.com/de/browsers/desktop/
2. Den Standard-Browser kannst du auch auf dem Mobiltelefon wechseln. Einfach den Firefox aus dem App-Store laden und als Standard-Browser-App festlegen. Du kannst bei der Neueinrichtung auch deine Lesezeichen aus dem alten Browser übernehmen. Es geht also nichts verloren.
3. **Werbeblocker installieren:** Einstellungen → Add-ons → z. B. nach uBlock Origin suchen und im Firefox installieren. Falls du ein Android-Mobiltelefon hast, kannst du auch dort im Firefox uBlock Origin als Werbeblocker installieren.
4. **Cookies im Browser löschen:** Einstellungen → Datenschutz & Sicherheit → Cookies & Websitedaten löschen; dann Häkchen setzen bei „Cookies & Websitedaten automatisch beim Beenden löschen".
5. **Standardsuchmaschine wechseln:** Einstellungen → Suchen → Standardsuchmaschine auf DuckDuckGo, Quant oder Ecosia stellen. Die Standard-Suchmaschine kannst du auch auf dem Mobiltelefon einstellen.
6. **Einen sicheren Messenger verwenden:** Signal oder Threema aus dem App-Store laden und Account einrichten. Du wirst vielleicht feststellen, dass ein großer Teil deiner Kontakte bereits dort ist.

DATENSCHUTZ SCHÜTZT NICHT DEINE DATEN, SONDERN DICH

Klaudia Zotzmann-Koch

noch alles installiert ist, mit wem du kommunizierst, wo und wann, wann nicht (also wann du schläfst), was für Apps auf deinem Telefon installiert sind, was du wann und wo mit denen machst, alle Inhalte deiner ganzen Kommunikationen, insbesondere deiner E-Mails, von wem du Rechnungen bekommst … Übergreifende Kundenkarten wie Payback oder Deutschlandcard sind natürlich mittendrin dabei. Die Informationsmassen sind riesig und reichen weit in unsere höchstpersönlichen Lebensbereiche rein. Ganz schön viel Gegenleistung für ein buntes Werbebildchen.

Das klingt erst einmal überwältigend. Aber: David hat auch gegen Goliath gewonnen und genauso haben auch wir eine Chance. Mehr als eine sogar. Der Datenschutz ist unser Freund und treuer Verbündeter, wenn wir uns – zu Recht – auf die Hinterbeine stellen und sagen, dass uns die Geschäftspraktiken der Datenfirmen zu weit gehen.

DIE TOP-3 DINGE, DIE ETWAS LÄNGER BRAUCHEN

1. **Updates machen:** Lass deinen Rechner und auch dein Mobiltelefon und Tablet alle Updates machen. Auch die Programme und Apps. Es sind immer wichtige Sicherheitsupdates dabei.
2. **Ein Backup machen**: Also eine Datensicherung erstellen. Dazu nimmst du im einfachsten Fall einen USB-Stick und gibst diesem ein Passwort; das geht beim Löschen und Neuformatieren des Sticks. Das Passwort musst du dir gut merken oder es an einem sicheren Ort aufschreiben. Noch besser wäre ein Passwortmanager (siehe Infokasten S. 11). Alle wichtigen Daten auf den USB-Stick kopieren und diesen an einem sicheren Ort verwahren. Wichtige Daten sind z. B. dein Adressbuch, ein Export deines Kalenders, deine wichtigen Dokumente wie Abschlusszeugnisse, Verträge (z. B. Autokauf), Heiratsurkunde, Testament, Patientenverfügung etc., deine 100 wichtigsten Fotos, deine Steuerunterlagen, Gewerbeanmeldung usw. und was immer du sonst auf jeden Fall wiederhaben willst, sollte der Rechner oder auch das Mobilgerät kaputtgehen.
3. **Sichere Passwörter & Passwortmanager:** Ein riesiger Gewinn für deine Onlinesicherheit und Schutz vor Kontoklau ist es, für jeden Account und jeden Service ein eigenes, langes Passwort zu verwenden. Lang heißt: Länger als 16 Zeichen. Die musst du dir nicht alle merken, dafür gibt es Passwortmanager. Wenn du Apple-Geräte verwendest, hast du den Apple-eigenen Passtwortmanager „Passwörter" bereits vorinstalliert. Du kannst auch ein freies Programm wie KeepassXC herunterladen → www.keepassxc.org. Mit einem Passwortmanager musst du dir nur noch das Passwort für den Passwortmanager merken. Alle anderen liegen in einem verschlüsselten Safe und das Programm füllt sie automatisch im Browser für dich aus, wenn du das freigibst. Das Programm erkennt auch gefälschte Seiten, wie z. B. Phishing-Seiten, und hält dich davon ab, deine Login-Daten dort einzugeben.

VOM MAMMUT ZU MEHR INTERNETSICHERHEIT

Manche finden es schwierig, wenn irgendetwas auf dem Computer oder Smartphone plötzlich anders aussieht als zuvor und schieben daher die nötigen Sicherheitsaktualisierungen auf. Aber: Es ist nicht grundsätzlich schlecht, wenn etwas anders aussieht. Es ist nur ungewohnt. Wir haben auch alle mal anders ausgesehen, hatten andere Haarschnitte, vielleicht andere Haarfarben. Und die Bäume sehen im Jahresverlauf ständig anders aus und sind trotzdem – oder gerade deswegen – unsere Freunde. Wenn der Button zum Herunterfahren des Geräts plötzlich nicht mehr blau, sondern grün ist, ist das zuerst ungewohnt, aber es muss uns keine Angst machen. Das gilt für alle Umstellungen im Leben.

Früher war es mal überlebenswichtig, mit allen anderen mitzuschwimmen, gemeinsam zu jagen und zusammen am Feuer gegrilltes Mammut zu essen. Deswegen haben wir im Kopf eine Hürde, wenn wir etwas anders machen wollen, als alle anderen. Es ist aber wirklich nicht überlebenswichtig, denselben Browser zu verwenden wie „alle anderen". Und auf der anderen Seite ist man auch nicht allein. Die Menge an datenschutzbewussten Menschen wächst und wächst. Du kommst also schon zu einer bestehenden Gruppe an Menschen dazu, wenn du etwas an deinen digitalen Gewohnheiten änderst.

Datenschutz ist wie die eine Person aus der Clique, die bei der launigen Party als Spießer*in galt, als sie die Partygäste davon abgehalten hat, betrunken Auto zu fahren. Im Internet ist Datenschutz dein Freund, um nicht unter die Räder der Datenkonzerne zu kommen. Im wahren Leben kann es sein, dass ein Algorithmus – zu Recht oder wegen einer Fehlzuordnung – dich in eine Risikogruppe einsortiert und du deswegen fortan das Doppelte für deine Versicherung zahlen musst. Um so etwas zu verhindern, dafür haben wir den Datenschutz. Zusammen mit den Maßnahmen, die wir selbst treffen können (lange Passwörter für jeden Service, Backups, Updates …), hilft er uns auch, uns souverän im Digitalen zu bewegen.

ÜBER DIE AUTORIN

Klaudia Zotzmann-Koch ist Autorin, Datenschutzexpertin und spezialisiert auf IT-Security-Awareness. Sie schreibt neben Sachbüchern zu digitaler Souveränität auch Science Fiction, Krimis und Historisches und hat gerade ein Studium in Creative Nonfictional Writing an der Universität Cambridge abgeschlossen.

www.zotzmann-koch.com

SCHWERPUNKT

SO FUNKTIONIERT SMARTPHONE-TRACKING UND SO KANNST DU DICH SCHÜTZEN

Jan Schötteldreier

Was das Smartphone so spannend für Behörden, Werbeunternehmen und Datenhändler*innen macht: Keinem Gerät vertrauen wir mehr über uns an als unserem Smartphone: Shopping, Kontaktpflege, Reisen, Recherchen, Zahlungen an der Kasse. Es gibt kaum noch Situationen, in denen wir es nicht mitnehmen. Die Daten auf dem Gerät sind dabei nur so sicher wie das Betriebssystem, dass die Daten und die vielen Apps, die wir heute nutzen, verwaltet.

Problematisch ist, dass sich Apple und Google den Markt für Smartphones de facto als Duopol teilen und beide die Programmierungen im Hintergrund als Firmengeheimnis weitgehend für sich behalten. Von außen kann also kaum jemand nachvollziehen, was mit den Daten der Nutzer*innen passiert. Alternativen zu Produkten von Google und Apple gibt es zwar, spielen aber nur eine vergleichsweise winzige Rolle auf dem Markt. Aber was unterscheidet Apples Betriebssystem iOS und Googles Android voneinander?

Apple inszeniert sein iPhone gern als besonders privates Gerät: „What happens on your iPhone, stays on your iPhone", prangte mal groß an einem Gebäude während einer großen Elektronikmesse 2019. Aber ist da wirklich was dran? Die meisten Sicherheitsmaßnahmen von Apple lassen sich nur bedingt überprüfen. Apple verkauft die strikten Vorgaben und Richtlinien für Apps auf dem eigenen Gerät als Sicherheitsgarant. Die Kehrseite ist aber auch, dass viele Möglichkeiten, die für mehr Privatsphäre und Sicherheit sorgen würden, auf iOS nicht möglich sind.

Android wird als quelloffene Basis zur Verfügung gestellt. Klingt eigentlich gut. In der Praxis starten Android-Geräte aber auch mit schlechten Grundbedingungen: Nicht immer lassen sich vorinstallierte Apps entfernen oder deaktivieren. Immerhin lassen sich aber alternative App-Stores (z. B. F-Droid) installieren. Außerdem unterliegen Apps unter Android weniger Hürden, so dass das Angebot an Apps, die Privatsphäre auf dem Gerät schützen, deutlich größer ist. Leider zeichnet sich ab, dass Google das Betriebssystem in Zukunft zunehmend abschotten wird und damit die Möglichkeit für Nutzer*innen, selbst für die Privatsphäre bei Nutzung des Smartphones zu sorgen, beschränkt wird.[1]

„Nicht selten stellen die Gerätehersteller für Alternativangebote zusätzliche Hürden auf."

INTRANSPARENZ & TRACKING BY DESIGN

Was Smartphones grundsätzlich von den üblichen PCs und Laptops und vorigen Mobiltelefonen unterscheidet, ist ihr grundlegendes Design als „Konsumgeräte". Betriebssystem, App-Angebot und Hardware sind vor allem darauf ausgerichtet, dass die Nutzenden digitale Inhalte ohne besondere Kenntnisse auf dem Gerät konsumieren können. Werbung ist bei vielen Diensten ein steter Begleiter, während im Hintergrund Nutzungsdaten gesammelt und übertragen werden und zu Profilen zusammengeführt werden, damit personalisierte Werbung ausgespielt werden kann. Durch das zentrale Hersteller-Konto (eine Apple-ID oder einen Googleaccount) binden die Konzerne die Nutzer*innen auch langfristig an die eigenen Geräte und Dienste: Man gewöhnt sich an den gebotenen Komfort. Eine Nutzung ohne Konto ist unattraktiv und anstrengend – falls überhaupt möglich. Denn ohne die vielen Bequemlichkeiten gehen viele grundlegende Funktionalitäten verloren. Sich Alternativen aufzubauen, ist mühsam und nicht selten stellen die Gerätehersteller für Alternativangebote zusätzliche Hürden auf. Die Installation von alternativen Betriebssystemen ist auch bei Android-Geräten nicht immer möglich. Gerade Google achtet darauf, dass Maßnahmen der Nutzer*innen gegen Werbung und Tracking nicht zu einfach anzuwenden sind. Der Grund: Über 200 Mrd. US-Dollar Umsatz macht Googles Mutterkonzern Alphabet mit Werbung[2]. Und auch Apple verdient bei sämtlichen Verkäufen im App-Store und auch innerhalb der Apps von Drittanbietern durch eine Umsatzbeteiligung von bis zu 30 Prozent kräftig mit[3].

WELCHE ART TRACKING DARF ES DENN SEIN?

Google und Apple unterstützen den Wunsch von App-Entwickler*innen, Werbung anzubieten und die Aktivitäten der Nutzer*innen zu tracken: Mit einer einzigartigen Zeichenfolge, der sogenannten **Werbe-ID**, können Werbetreibende über Apps Geräte und damit die Nutzenden über verschiedene Dienste auf einen längeren Zeitraum wiedererkennen.

Wie mächtig diese zentrale und eindeutige Kennung ist, hat im Juli 2024 die umfassende Recherche „**Databroker Files**"

SO FUNKTIONIERT SMARTPHONE-TRACKING UND SO KANNST DU DICH SCHÜTZEN

Jan Schötteldreier

von netzpolitik.org und dem Bayerischen Rundfunk gezeigt[4]. Die Daten fließen bei Datenhändlern zusammen, die wiederum an Werbetreibende und andere verkauft und zu umfassenden Datensätzen zusammengefügt werden. Dadurch konnten die Journalist*innen dieser Recherche Bewegungsprofile einzelner Personen nachvollziehen und diese klar identifizieren. Brisant ist die Herkunft dieser Daten: Beliebte und vermeintlich harmlose Apps, die laufend Standortdaten sammelten und diese mit der Werbe-ID verknüpften. Eine davon war die millionenfach und gerade in Deutschland beliebte App Wetter Online.

Mit einer Standortzuordnung und einer Werbe-ID lässt sich Werbung deutlich besser personalisieren. Eine genaue Standortbestimmung erfolgt üblicherweise über Satellitenortung, für die oft vereinfacht das US-amerikanische GPS als Sammelbegriff genutzt wird. In anderen Kontexten können Geräte auch allein anhand von WLAN- oder Bluetooth-Signalen lokalisiert werden. Und auch die IP-Adresse oder genutzte Mobilfunkzelle lassen Rückschlüsse auf den Gerätestandort zu. Weitere Merkmale, mit denen sich Geräte verfolgen lassen, sind diverse Geräteinformationen und Eigenschaften sowie Browser-Cookies.

Während Apps in Googles Play Store zwingend die Werbe-ID zur Aktivitätenverfolgung nutzen müssen, können durch den Hersteller vorinstallierte Apps diese Einschränkung umgehen und weit mehr Daten erheben. Das ist besonders ärgerlich, da vorinstallierte Apps oft nicht einfach so entfernt oder deaktiviert werden können.

WERBE-ID DEAKTIVIEREN UND STANDORT-ZUGRIFF EINSCHRÄNKEN

Glücklicherweise ist das **Deaktivieren des Zugriffs von Apps auf die Werbe-ID** auf nahezu allen aktuellen Geräten möglich. Dadurch können Apps die ID nicht mehr einsehen und Unternehmen nicht mehr so einfach eindeutig zuortbare Daten sammeln.

Achtung: Bei Android können der Weg und die Namen der jeweiligen Menüs je nach Gerät, Hersteller und Android-Version unterschiedlich sein. Suche nach der jeweiligen Einstellung und deinem Gerätenamen im Internet oder nutze die Suchfunktion in den Einstellungen deines Geräts.

Android: Einstellungen → Google → „Alle Dienste" auswählen → Nach unten zu „Werbung" scrollen → „Werbe-ID löschen" antippen und bestätigen

iOS: Einstellungen → zu „Datenschutz & Sicherheit" scrollen → Tracking antippen → den Schalter bei „Apps erlauben, Tracking anzufordern" deaktivieren

Ähnlich einfach ist es, den **Standortzugriff von Apps zu beschränken:**

Android: Einstellungen Datenschutz & Sicherheit → ggf. Privatsphäredashboard → Standort

Hier werden alle Apps angezeigt, die zuletzt auf den Standort zugegriffen haben. Per Antippen des Buttons „Berechtigung verwalten" kann der Standortzugriff für alle Apps einzeln eingestellt werden. Alternativ kann man auch die Eigenschaften einer App aufrufen (langes Drücken des App-Symbols auf dem Startbildschirm) und dort die Berechtigungen prüfen.

Unter Einstellungen → Standort werden Apps angezeigt, die zuletzt auf den Standort zugegriffen haben. Unter „Alle ansehen" können sämtliche Apps chronologisch sortiert angezeigt werden, die Zugriffe angefragt haben.

iOS: Einstellungen → Datenschutz & Sicherheit→ „Ortungsdienste"

Falls die Ortungsdienste aktiv sind, werden hier alle Apps angezeigt, die auf den Standort zugegriffen haben. Apps, die das kürzlich getan haben, werden mit einem Pfeil markiert.

Auf beiden Systemen kann für jede App einzeln eingestellt werden, wann der Standort genutzt werden darf und ob die Bestimmung genau oder grob erfolgen soll. Für eine Wetter-App reicht z. B. eine reine Angabe des Ortes oder der ungefähre Standort, während für Navigationsdienste eher der genaue Standort sinnvoll ist.

Ebenfalls ist es empfehlenswert, unter Android die permanenten WLAN- und Bluetooth-Scans zu deaktivieren, die auch zum Sammeln von Daten eingesetzt werden:

Einstellungen → Standort → Standortdienste → „WLAN-Suche" und „Bluetooth-Suche" deaktivieren.

Grundsätzlich sollten WLAN und Bluetooth bei Nichtgebrauch deaktiviert werden.

APP-MINIMALISMUS PFLEGEN

Weißt du, wie viele Apps derzeit auf deinem Telefon installiert sind und welche Berechtigungen sie haben? Nein? Dann ist es mal an der Zeit, dem eigenen App-Bestand auf den Zahn zu fühlen. Die Stores sind voll mit Apps, denen es nicht an eigentlich unnötigen Berechtigungen und Datensammelei mangelt. Taschenlampen-Apps mit Internetzugriff und Auslesen des Telefonstatus? Leider keine Seltenheit.

Nimm dir an einem Abend in Ruhe Zeit und gehe deine installierten Apps durch (in beiden Systemen unter Einstellungen → Apps):

SO FUNKTIONIERT SMARTPHONE-TRACKING UND SO KANNST DU DICH SCHÜTZEN

Jan Schötteldreier

SCHWERPUNKT

? **Brauche ich diese oder jene App wirklich?** Deinstalliere sie, wenn du sie nicht mehr brauchst.

? **Sind die erteilten Berechtigungen wirklich notwendig?** Auch dort, wo angefragte Berechtigungen naheliegend erscheinen, kann man das überraschend oft ablehnen: Apps von Lieferdiensten funktionieren z. B. auch oft ohne Zugriff auf den Standort. Messenger wie Signal und WhatsApp laufen auch ohne Zugriff auf die Kontakte – die muss man dann selbst eintragen.

? **Kann man anstatt der App vielleicht einfach eine Website des entsprechenden Anbieters nutzen?** Websites speichern meist etwas weniger Daten als Apps.

? **Arbeitet die App datensparsam und gibt es evtl. freie Alternativen?** Dazu später mehr.

Praktisch: Android und Apple entziehen in aktuellen Versionen ihrer Betriebssysteme automatisch Berechtigungen, sofern sie lang nicht mehr gestartet worden sind.

DAS EIGENE GERÄT UND INSTALLIERTE APPS DURCHLEUCHTEN

So kannst du Apps selbst auf ihre Tracking-Aktivitäten prüfen: Für Android-Apps gibt es das Projekt **Exodus Privacy** (www.reports.exodus-privacy.eu.org/de/) und für iOS das Projekt **Tracker Control** (www.ios.trackercontrol.org/, wird nicht mehr aktualisiert): Die Dienste scannen Apps aus dem entsprechenden Store und prüfen, ob dort bekannte Tracking- und Werbemodule enthalten sind. Das kann man als Indikator nutzen, ob eine bestimmte App eher datenschutzfreundlich ist oder eine Veranlagung zum Datensammeln hat. Ein kurzer Blick auf die Datenschutzerklärungen der App und die Suche nach Stichwörtern wie „Dritte" oder „Drittanbieter" kann auch aufschlussreich sein.

PRIVATSPHÄRENFREUNDLICHE UND FREIE ALTERNATIVEN WÄHLEN

Android: Da Android ein grundlegend offeneres System als Apple hat, gibt es dort eine deutlich größere Auswahl an quelloffenen und datenschutzfreundlichen Apps. Hauptanlaufstelle ist hier der freie Alternativ-App-Store **F-Droid:** Dort sind ausschließlich freie Apps zu finden, die im Schnitt wesentlich besser mit den privaten Daten der Nutzenden umgehen. Das hängt auch damit zusammen, dass die meisten Apps aus F-Droid keine kommerziellen Interessen verfolgen, während im App Store und Play Store empfehlenswerte Apps im Wust an werbe- und trackingverseuchten Apps geradezu untergehen.

iOS: Hier ist das Angebot an freien Apps deutlich übersichtlicher. In der EU und inzwischen auch in anderen Ländern wird Apple immer häufiger gezwungen, sich für alternative App-Stores zu öffnen und auch alternativen Browsern mehr Spielraum zu gewähren. Eine dieser Alternativen ist der AltStore: www.altstore.io

Übersichten und Empfehlungen zu besonders privatsphärenfreundlichen Diensten und Alternativen sind auf folgenden Seiten zu finden, z. B.:

www.kuketz-blog.de/empfehlungsecke

www.smartphone-dont-spy.de

www.switching.software

www.privacyguides.org

ÜBER DEN AUTOR

Jan Schötteldreier arbeitet als Systemadministrator und engagiert sich seit über zehn Jahren als Experte für Digitale Selbstverteidigung. In diesem Rahmen hat er zahlreiche Workshops und Veranstaltungen an Universitäten, Volkshochschulen und Verbraucherzentralen durchgeführt. Nach vielen Jahren Mitarbeit beim Verein Digitalcourage hat er in Bielefeld den neuen Verein Datenpunks (www.datenpunks.de) mitgegründet, der sich dem Schutz von Grundrechten sowie digitalen Bürgerrechten widmet."

1 www.heise.de/news/Android-Google-verbietet-anonyme-Apps-10617479.html
2 www.diemedien.at/articles/google-youtube-alphabet-wohin-die-grossten-werbeeinnahmen-der-welt-gehen
3 www.iphone-ticker.de/entwicklerfreundliche-statistiken-apple-verteidigt-app-store-modell-257457/
4 www.netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland/

RATGEBER

In Zeiten, in denen es auf der ganzen Welt politische und gesellschaftliche Krisen zu überwinden gibt, ist es wichtiger denn je, sich politisch zu engagieren und es gibt unzählige Möglichkeiten, aktiv zu werden. Besonders beliebt ist die Teilnahme an Online-Petitionen. Diese bieten einen einfachen und schnellen Weg, mit dem du ohne großen Aufwand Einfluss nehmen kannst. Du kannst sie z. B. nutzen, um gegen Tierversuche vorzugehen, den Klimaschutz zu fördern, faire Löhne einzufordern, den Abriss von Gebäuden zu verhindern oder mehr Kitaplätze zu schaffen. Außerdem können Petitionen dazu beitragen, Gesetze zu stoppen, die unsere Demokratie gefährden könnten.

IST ONLINE-BETEILIGUNG GUT ODER SCHLECHT?

Das Mitmachen bei Aktionen wie Online-Petitionen stärkt das Gemeinschaftsgefühl und gibt das Gefühl, durch die direkte Beteiligung, wirklich etwas bewegen zu können: Man fühlt sich mächtiger, hoffnungsvoller und auch ein kleines bisschen glücklicher.[1] Da sich diese Teilhabe digital gestalten lässt, findet sie viel Zuspruch. Die Reichweite solcher Petitionen kann, wenn sie von bekannten oder prominenten Personen geteilt werden, enorm groß werden und sich sogar global verbreiten, während die Hürden zur Teilnahme gering sind (manchmal das Anlegen eines Accounts).

QUALITÄT UND QUANTITÄT ABWÄGEN

Es kommt natürlich darauf an, wofür genau du dich einsetzt. Setzen sich Menschen beispielsweise für Gesetze und Verbote ein, die freiheitlich-demokratische Grundrechte einschränken, dann ist das zwar, solange das Grundgesetz beachtet wird, ihr Recht, aber im Sinne der Demokratie keine gute Entwicklung. Viele Menschen klicken im Internet außerdem oft zu schnell und lassen sich von Emotionen leiten, ohne sich richtig mit den Themen oder dem Hintergrund zu beschäftigen. Sobald eine Petition unterschrieben ist, wird gedanklich ein Haken dahinter gemacht, da man seinen Beitrag als geleistet ansieht. Wenn man sich nicht ausreichend Zeit dafür nimmt, kann es auch passieren, dass man

WAS GENAU BEDEUTET DEMOKRATIE?

Demokratie bedeutet, dass das Volk die Macht hat, über politische Entscheidungen mitzubestimmen, entweder direkt oder durch gewählte Vertreter*innen. Die wichtigsten Faktoren einer Demokratie sind freie Wahlen, Meinungsfreiheit, Gleichheit vor dem Gesetz und die Achtung der Menschenwürde. Ausführliche Informationen: www.bpb.de/kurz-knapp/lexika/politiklexikon/17321/demokratie/

1 www.lpb-bw.de/beteiligung

Petitionen unterstützt, hinter denen Personen, Gruppen oder Parteien stehen, die man eigentlich nicht unterstützen würde. Oftmals muss eine Petition schnell gehen, z. B. um eine Entscheidung zu stoppen oder ein Eilverfahren zu bewirken. Es ist nicht immer möglich, alle Hintergründe einer Petition zu kennen, aber es gibt Unterschiede zwischen Petitionen – manche sind realistischer und haben bessere Chancen auf Erfolg, während andere im Sande verlaufen und für Politiker*innen und Gesetzgeber nicht relevant genug sind, um beachtet zu werden.

SERIOSITÄT EINSCHÄTZEN

Petitionen verbreiten sich schnell und ziehen viel Aufmerksamkeit auf ein Thema. Das ist auch eine Art Marketing, um Menschen zu begeistern. Das ist bis zu einem gewissen Punkt okay, weil es das Ziel ist, viele zu erreichen. Aber es ist nicht in Ordnung, politische Teilhabe nur als Marketinginstrument zu nutzen, wenn die Chance auf Erfolg gering ist oder die Forderungen in der Petition an der Lösung der Probleme vorbeigehen (solche werden auch als „Nebelkerzen" bezeichnet, die viel Rauch machen und damit den Kern eines Problems verschleiern).

ECHOKAMMERN BEACHTEN

Es besteht außerdem die Gefahr, dass Menschen sich durch extreme Meinungen im Internet radikalisieren und dementsprechend sehr radikale Forderungen stellen, die sie über das Einreichen von Petitionen umsetzen möchten. Wenn man nur noch eine bestimmte Perspektive einnimmt und kaum noch mit anderen Meinungen konfrontiert wird – dieses Phänomen wird auch als „Echokammer" bezeichnet – kann das dazu führen, dass man immer radikaler in den eigenen Ansichten wird. Deshalb ist es wichtig, bei politischem Engagement offen für unterschiedliche Ansichten zu bleiben und respektvoll mit anderen umzugehen.

RATGEBER

AUF EINEN BLICK:
Darauf solltest du bei Online-Petitionen achten

☑ **Wer hat die Petition gestartet?**
Wer steckt hinter dem Aufruf zu unterschreiben? Sind die Texte selbst geschrieben oder versucht jemand, sich mit fremden Inhalten zu präsentieren? Achtung: Wenn die Petition nur reißerisch klingt und kaum Infos bietet, ist Vorsicht geboten.

☑ **Werden die Verantwortlichen erreicht?**
Wird das Anliegen an die richtigen Personen geschickt oder werden Befugnisse falsch eingeschätzt, z. B. Bürgermeister*innen bei EU-Themen? Du solltest die Hintergründe kurz prüfen.

☑ **Wie ist das Verhältnis von Sachlichkeit und Empörung?**
Hat die Petition ein klares, umsetzbares Ziel oder nur Kritik ohne Lösung? Auch ohne Fachwissen sollten Forderungen geprüft werden. Vorsicht: Manche Petitionen dienen nur dazu, Ärger zu schüren.

☑ **Ist das noch Politik oder schon Marketing?**
Wie viel Werbung für Produkte oder Spenden gibt es bei der Petition? Wird man beim Unterzeichnen nach Newslettern oder Spenden gefragt? Organisationen dürfen sich vorstellen und um Unterstützung bitten, echte politische Arbeit sollte aber keine Geschenke oder Vorteile anbieten. Das Ziel der Petition sollte klar sein und Anreize bieten. Vorsicht also bei Lockangeboten mit Geschenken oder Vorteilen.

☑ **Viele Unterschriften = großer Erfolg?**
Natürlich geht es genau darum, viele Unterschriften zu sammeln: je mehr, desto größer ist die Wahrscheinlichkeit, etwas zu bewirken. Angaben zur Anzahl der bereits eingereichten Unterschriften können bei der Einschätzung helfen, ob es sich lohnt dran zu bleiben, können aber auch irreführend sein, denn du kannst nicht immer sicher sein, dass diese Zahl stimmt. Eine Orientierungsgröße bildet auch der Zeitrahmen, wie lange die Petition noch läuft: Wenn kurz vor der Deadline noch Tausende Unterschriften fehlen, solltest du zumindest kurz innehalten und überlegen, woran das liegen könnte.

☑ **Geht es nur um meine Daten?**
Auf welcher Plattform wird die Petition beworben? Werden nur meine Adresse und politische Meinung gespeichert? Welche Daten werden abgefragt und wann gelöscht? Werden unnötige Daten gesammelt, die nichts mit der Petition zu tun haben? Gibt es versteckte Tracker, die meine Infos an Dritte weitergeben könnten? Um das zu prüfen, kann man Tools wie Webbkoll nutzen, die Serverstandorte und Cookies anzeigen. Achtung: Wenn keine Infos zum Datenschutz vorhanden sind oder die Server außerhalb der EU (z. B. in den USA) stehen, ist Vorsicht geboten – gerade, wenn die Politik in diesen anderen Ländern sehr restriktiv ist. Petitionen, die aus der EU kommen, müssen sich zumindest an die europäischen Datenschutzgesetze halten, die strenger sind als außerhalb der EU.

☑ **Wie geht es nach der Unterzeichnung weiter?**
Was passiert nach dem Unterschreiben? Wann und wie wird die Petition an die Verantwortlichen übergeben? Kann ich sicher sein, dass meine Stimme gehört wird? Gibt es später eine Möglichkeit zu sehen, was aus der Petition geworden ist? Wenn nach kurzer Zeit nichts mehr passiert und keine Infos kommen, ist das verdächtig. Achtung: Wenn nicht erklärt wird, was nach dem Unterschreiben passiert, ist Vorsicht geboten.

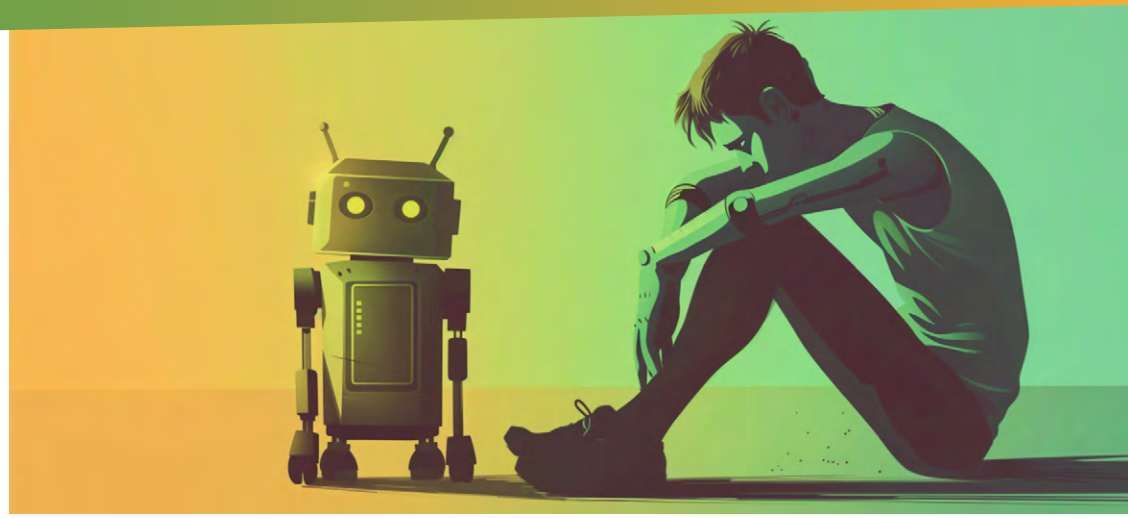
HILF MIT UND VERTEIDIGE DEINE RECHTE!

Es sollten viel mehr Menschen für unsere Demokratie aktiv werden! Das kann durch Demonstrationen geschehen, durch das Unterstützen von Petitionen oder auf andere Weise. Online-Aktivismus – manchmal auch Klick-Aktivismus genannt – ist eine einfache Möglichkeit, viel zu bewirken. Schon ein kleiner Klick kann große Wirkung zeigen.

Weitere Möglichkeiten, um sich an der Gesellschaft und damit an unserer Demokratie zu beteiligen:

- Wählen gehen
- Teilnahme an demokratiefördernden Demonstrationen
- Medienkompetenz stärken
- Gegen Hass im Netz einsetzen
- Informationskompetenz aufbauen und Desinformation aufdecken
- Augen aufhalten in sozialen Medien, um demokratiefeindliche Strukturen zu bemerken

KÜNSTLICHE INTELLIGENZ – Wie wir im Alter davon profitieren



Was genau ist eigentlich Künstliche Intelligenz? KI-Systeme basieren auf mathematischen Modellen und Algorithmen und versuchen menschliche Fähigkeiten, wie Denken, Lernen und Problemlösen, nachzuahmen. Dafür verarbeitet KI eine große Menge an Daten und erkennt Muster, um darauf basierend Entscheidungen zu treffen.

Stellen wir uns vor, KI ist wie ein*e Bäcker*in, die*der lernt, Brot zu backen. Die Daten sind in diesem Fall die vielen Rezepte, die gesammelt und genau studiert werden. Der Algorithmus ist die Methode, mit der die*der Bäcker*in Schritt für Schritt herausfindet, welche Zutaten und Backzeiten am besten zusammenpassen. Nach vielen Versuchen entwickelt sie*er ein gutes Gespür dafür, welche Kombinationen das beste Ergebnis liefern. Das Produkt oder Ergebnis ist schließlich das fertig gebackene Brot. Natürlich sind KI-Systeme viel komplexer und oft auch nicht transparent. Wichtig ist zu wissen, dass eine KI meistens nur für bestimmte Aufgaben trainiert wird, ihre Qualität von den Trainingsdaten abhängt und sie trotzdem Fehler machen kann.

KI IM ALLTAG

Künstliche Intelligenz steckt schon in unserem Smartphone, etwa bei der Gesichtserkennung, in Waschmaschinenprogrammen, Sprachassistenten, Übersetzungsprogrammen, beim Online-Shopping sowie in Navigationssystemen, die uns die beste Route berechnen. KI kann u. a. bei Problemen mit Apps und Programmen helfen, Anleitungen leicht verständlicher formulieren und für Recherchezwecke eingesetzt werden. Chatbots können beispielsweise beim Erlernen einer neuen Sprache unterstützen, tragbare Geräte wie Smartwatches tragen hingegen zur Gesundheitsförderung bei. Besonders KI-Sprachassistenten sind leicht zu bedienen und können Menschen eine Unterstützung bieten. Um Telefonanrufe zu starten, Musik oder Nachrichten abspielen zu lassen oder einfach nach dem Wetter zu fragen. Anstatt auf einem kleineren Gerät, wie dem Smartphone, zu tippen, kann ein Sprachbefehl praktisch und einfacher sein. KI kann auch als Erinnerungsstütze eingesetzt werden, etwa bei Fragen wie „Habe ich die Tür abgeschlossen?“ oder „Habe ich meine Tabletten genommen?“. Darüber hinaus kann auch mit Chatbots gespielt werden: Eine Runde Bingo, Sudoku oder ein Kreuzworträtsel können ganz einfach durch eine kurze Anfrage erstellt werden.

KI UND EINSAMKEIT

Spätestens seit der Coronapandemie zeigt sich deutlich, dass Einsamkeit immer mehr Menschen betrifft. Vielen fällt es im Alltag schwer, Kontakte zu knüpfen oder Beziehungen aufzubauen. Die digitale Welt bietet zunehmend neue Möglichkeiten, um mit anderen in Kontakt zu treten. So ermöglichen Social-Media-Plattformen wie Instagram oder Facebook nicht nur den Austausch mit Familie und Freund*innen, sondern auch das Knüpfen neuer Kontakte. Durch den Einsatz Künstlicher Intelligenz eröffnen sich dabei noch ganz neue Möglichkeiten der Kommunikation. Chatbots wie ChatGPT oder auch Sprachassistenzen wie Alexa integrieren sich immer mehr in den Haushalten und übernehmen dabei zunehmend soziale oder kommunikative Rollen. So wird die KI immer häufiger als Fitnessberater*in, Lernpartner*in oder Freund*in genutzt. In diesem Zusammenhang bietet die KI eine niederschwellige und flexible Möglichkeit, Gespräche zu führen. Sie kann sich sprachlich anpassen, Rückfragen stellen und ist rund um die Uhr verfügbar.

Doch kann eine Maschine eine zwischenmenschliche Beziehung ersetzen? Nein, denn ein Chatbot wie ChatGPT versucht, Muster aus einer Vielzahl von Daten zu erkennen und berechnet darauf basierend die bestmögliche Antwort. Diese ist jedoch nicht immer passend für die Nutzer*innen und es bleibt fraglich, wie gut eine solche Technologie uns tatsächlich verstehen kann. Zwar kann Empathie simuliert werden, doch stößt sie dabei an ihre Grenzen, denn echtes Einfühlungsvermögen bleibt eine unverzichtbare menschliche Fähigkeit. Zudem besteht das Risiko, einen Realitätsverlust zu erleiden, wenn man nur mit einem Bot o. ä. kommuniziert.

„Kann eine Maschine eine zwischenmenschliche Beziehung ersetzen?“

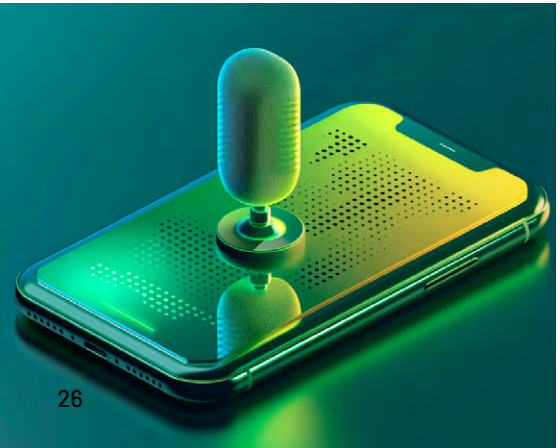
DEEPFAKES

Mit der rasanten Entwicklung der Technologie entstehen auch neue Herausforderungen. Sogenannte Deepfakes werden generiert und verbreiten sich online. Dabei handelt es sich um verschiedene Formen der Manipulation von Medieninhalten, wie Bild-, Video- und Tonaufnahmen, die mithilfe von KI erstellt wurden. Inhalte wirken oft realistisch und es wird zunehmend schwieriger zu erkennen, was wirklich echt ist. Das führt dazu, dass die Gefahr von Desinformation steigt und gezielte Propaganda stattfinden kann. Daher ist es wichtig, Quellen und Inhalte, die einem im

KÜNSTLICHE INTELLIGENZ – Wie wir im Alter davon profitieren

Netz begegnen, zu prüfen. Bei Unsicherheiten kann es helfen, mit jemanden darüber zu sprechen und Inhalte, auch solche, die z. B. in die Familiengruppe auf WhatsApp geschickt werden, nicht unmittelbar weiterzuleiten.

Auch bei Telefonbetrugsmaschen stellt KI eine zusätzliche Gefahr dar. Bei der Enkel-Trick-Masche setzen Betrüger*innen KI ein, um Stimmen zu klonen, sodass es am Telefon so klingt, als würde tatsächlich eine vertraute Stimme mit einem sprechen. Inhaltlich geht es dabei immer um einen Notfall, bei dem Geld erforderlich wird. Betrüger*innen brauchen nur wenig Audiomaterial, es reichen meist einige Sekunden, um mithilfe von KI die Stimme nachzubilden. Und auch in Bezug auf Emotionen hat die KI Fortschritte gemacht, sodass Stimmen nicht nur authentischer wirken, sondern auch Emotionen wie Weinen nachgestellt werden können. Ein weinendes Familienmitglied wirkt in solch einer Situation sehr überzeugend. Auch wenn die Stimme vertraut klingt, sollten Betroffene zunächst auflegen und die Person über eine bekannte Nummer zurückrufen. Ansonsten kann man sich zur Absicherung ein Codewort überlegen, was innerhalb der Familie festgelegt wird.



KI ENTDECKEN

Wie alle digitalen Entwicklungen bringt Künstliche Intelligenz sowohl Chancen als auch Risiken mit sich. Man muss sich davon also nicht abschrecken lassen. Stattdessen lohnt es sich, KI-Anwendungen einfach mal auszuprobieren.

Starte doch damit, folgende Aufgaben in den Alltag zu integrieren:

- Achte eine Woche lang auf deine Umgebung und beobachte, wo dir Künstliche Intelligenz begegnet. So bekommst du ein besseres Bewusstsein dafür, wie KI deinen Alltag beeinflusst.
- Diskutiere mit Freund*innen oder der Familie über KI: Nutzen sie schon KI? Wenn ja, wofür? Nutzt das Thema als Gelegenheit, gemeinsam Tools auszuprobieren und voneinander zu lernen.

Eigene Prompts ausprobieren

Wie bekomme ich jetzt aber das bestmöglichste Ergebnis bei einer KI? Dafür braucht es einen guten Prompt. Ein Prompt, das heißt eine präzise Anweisung, in der man der KI möglichst viele Hintergrundinformationen mitteilt, sich klar ausdrückt und lange Sätze vermeidet. Oft muss ein Prompt mehrfach eingegeben und dabei immer wieder angepasst werden, um das gewünschte Ergebnis zu liefern. Antworten sollten stets hinterfragt und geprüft werden, denn die KI ist nicht unfehlbar und nur so gut wie ihre Trainingsdaten.

Probiere doch folgenden Prompt einmal bei einem Chatbot aus: „Erstelle ein Kreuzworträtsel mit 10 Begriffen zum Thema Sommerurlaub, mit Hinweisen für jede Antwort. Die Begriffe sollten aus verschiedenen Schwierigkeitsgraden bestehen."

Viel Spaß beim Rätseln!

QuickDraw

QuickDraw von Google funktioniert wie das Spiel „Montagsmaler" allerdings online im Browser. In 19 Sekunden müssen sechs Begriffe gezeichnet werden, während die KI versucht, sie zu erkennen.

Which Face is Real

Auch wenn es zunehmend schwieriger wird, KI-generierte Bilder von echten zu unterscheiden, gibt es dennoch bestimmte Merkmale, auf die man achten kann, sowie Fehler, die nach wie vor auftreten können. Auf der Website *WhichFaceIsReal* geht es darum, zwischen zwei Personen zu entscheiden, welche echt ist und welche von einem KI-System erstellt wurde.

Sendung mit der Maus

Auch die „Sendung mit der Maus" hat sich mit dem Thema KI beschäftigt und nimmt die Zuschauer*innen mit vielen Infos, Videos und Spielen in diese Welt mit. Hier können Groß und Klein viel Neues lernen und sich selbst ausprobieren.

KI für ein gutes Altern

Das Projekt der Bundesarbeitsgemeinschaft der Seniorenorganisationen e.V. (BAGSO) setzt sich dafür ein, älteren Menschen KI-Kompetenz zu vermitteln. Auf der Webseite finden sich spannende Artikel, Tipps und Veranstaltungen zum Thema KI.

Digital mobil im Alter

Ein Projekt von O_2 Telefónica und der Stiftung Digitale Chancen mit dem Ziel, älteren Menschen die Teilhabe an der digitalen Gesellschaft zu ermöglichen. Hier gibt es unter anderen einen Wissensbereich zum Thema Künstliche Intelligenz und ein Glossar zu Begriffen aus der digitalen Welt.

Quellen zum Thema:
Einsamkeit: www.bmbfsfj.bund.de/bmbfsfj/themen/engagement-und-gesellschaft/strategie-gegen-einsamkeit/wissen-zu-einsamkeit-vertiefen-228600
Einsamkeit & KI: www.wir-mit-ki.de/kuenstliche-intelligenz-und-einsamkeit/
Enkeltrick: www.tagesschau.de/wirtschaft/verbraucher/enkeltrick-ki-betrug-100.html

RATGEBER

Gesundheitsdaten gehören zu den persönlichsten Informationen, die wir haben, denn sie verraten viel über unseren körperlichen und geistigen Zustand. Deshalb solltest du auf diese Daten ganz besonders achten und sie nicht leichtsinnig anderen anvertrauen, wenn es nicht unbedingt sein muss.

Dazu gehören beispielsweise

- medizinische Diagnosen, Laborwerte, MRT-Bilder, Impfstatus und Allergien,
- behandlungsbezogene Daten, wie Arztberichte,Therapie-, Pflege-, und Medikationspläne,
- Daten aus digitalen Geräten und Gesundheitsapps, z. B. Schritte, Puls, Herzfrequenz, Schlafdauer oder Blutzuckermessungen und
- persönliche Angaben mit Gesundheitsbezug, wie Alter, Geschlecht, Schwangerschaft und Angaben zu Behinderungen.

WAS KANN PASSIEREN, WENN GESUNDHEITSDATEN IN DIE FALSCHEN HÄNDE GERATEN?

Wenn Gesundheitsdaten innerhalb des Gesundheitssystems, z. B. zwischen Ärzt*innen, an der falschen Stelle landen, ist das meist kein großes Problem. Kritisch wird es jedoch, wenn Unternehmen, Versicherungen oder Unbefugte Zugriff bekommen. Dann können folgende Risiken entstehen:

- **Diskriminierung:** Arbeitgeber*innen oder Versicherungen könnten dich benachteiligen, wenn sie von Krankheiten, einer Schwangerschaft oder bestimmten Risiken erfahren. Auch scheinbar harmlose Infos – wie Motorradfahren – können im Gesamtbild zu Nachteilen führen.
- **Identitätsdiebstahl und Betrug:** Kriminelle könnten mit deinen Daten Rezepte fälschen, Behandlungen abrechnen oder deine Versichertennummer missbrauchen.

- **Erpressung und Rufschädigung:** Unbefugte könnten mit der Veröffentlichung sensibler Diagnosen drohen, etwa zu psychischen Erkrankungen, Suchtproblemen oder anderen persönlichen Themen.
- **Ungewollte Werbung und Profilbildung:** Unternehmen können Gesundheitsprofile erstellen und dich mit passender Werbung beeinflussen. Das kann zu Fehlentscheidungen führen – vor allem, wenn medizinischer Rat fehlt.

WANN IST DIE HERAUSGABE VON GESUNDHEITSDATEN IN ORDNUNG?

Bei Ärzt*innen, im Krankenhaus, in der Apotheke, bei der Krankenkasse, bei medizinischen Notfällen und bei Pflege- oder Betreuungsdiensten ist natürlich klar, dass Gesundheitsdaten benötigt werden, um dich bestmöglich versorgen und beraten zu können. Das Wichtigste ist, dass

- du weißt, wer die Daten bekommt,
- verstehst, warum sie gebraucht werden und
- darauf achtest, dass deine Daten sicher behandelt werden.

Letzteres ist nicht immer leicht zu erkennen und auch wenn soweit alles vertrauenswürdig klingt, besteht keine Garantie,

RATGEBER

dass deine Angaben in sicheren Händen bleiben – insbesondere bei zunehmender Digitalisierung von Daten.

DIGITALISIERUNG UND GESUNDHEITSDATEN

Viele Gesundheitsdaten werden heute über Patientenportale, die elektronische Patientenakte oder über Apps und smarte Geräte erfasst. Wenn du unsicher bist, ob du sie nutzen solltest, helfen dir im Zweifel folgende Schritte:

- **Angebot kritisch prüfen:** Sind Anbieter*innen vertrauenswürdig? Offizielle Apps von Krankenkassen oder Arztpraxen sind meist sicherer. Bewertungen, Siegel und Empfehlungen bieten hier eine erste Orientierung.

- **Datenerhebung prüfen:** Achte darauf, wie deine Daten geschützt werden und welche Informationen du teilst. EU-Angebote unterliegen meist strengeren Datenschutzregeln, deshalb solltest du vor allem diese nutzen. Nutze außerdem sichere Passwörter, die du sonst nirgendwo anders verwendest.
- **Auf das eigene Gefühl hören:** Wenn dir eine App nicht geheuer ist, suche Alternativen. Vieles geht weiterhin auch ohne digitale Angebote – z. B. Termine per E-Mail oder Telefon. Auch die Nutzung der elektronischen Patientenakte ist keine Pflicht.
- **Selbstbestimmt bleiben:** Du entscheidest, wer deine Daten bekommt. Du hast das Recht, Auskunft über gespeicherte Informationen zu erhalten und sie korrigieren oder löschen zu lassen.

MEHR SELBSTBESTIMMUNG = WENIGER SORGEN

Je besser du verstehst, wie digitale Angebote funktionieren, desto leichter kannst du entscheiden, wem du deine Gesundheitsdaten anvertraust – und wem lieber nicht. Sensible Informationen verdienen einen besonders sorgfältigen Umgang. Mit etwas Medienkompetenz und gesunder Vorsicht kannst du dich sicher im digitalen Gesundheitsbereich bewegen. Mach unsere Online-Selbsttest auf www.digitalcheck.nrw, um deine digitalen Kompetenzen zu verbessern!

Quellenangaben zu diesem Text findest du auf unserer Website:
www.digitalcheck.nrw/digital-weiterwissen/uebersicht/artikel/so-schuetzt-du-deine-gesundheitsdaten-am-besten

Der Computer hat immer Recht – oder?

Klaudia Zotzmann-Koch

Es ist schon normal geworden, Chatbots wie ChatGPT, Google Gemini, Deepseek, Mistral oder Claude nach allem Möglichen zu fragen. Deren Chat-Format gaukelt uns vor, mit einem denkenden Gegenüber zu sprechen, das auf unsere Fragen und Äußerungen antwortet – von trivialen Fragen, über Kochrezepte bis hin zu intimsten Fragen zu Krankheitssymptomen und Problemen im Privaten.

Einigen mag es vorkommen, als wäre der Chatbot emphatischer als die*der beste Freund*in oder der*die Ärzt*in. Leider trügt der Schein, denn die Maschine ist von der Herstellerfirma schlicht darauf programmiert, uns so lange wie möglich zu beschäftigen.

Das andere Problem an diesen Chatbots ist, dass sie leider häufig Mumpitz von sich geben. Das gilt ebenso für KI-gestützte Suchen wie die neue Google-Suche. Diese Maschinen errechnen bloß durch reine Statistik, was eine wahrscheinlich passende Antwort ist. Den Chatbots oder auch Googles KI-Suche ungeprüft zu vertrauen, kann schwere Probleme bereiten. Was bei völlig frei zusammengerechneten Informationen wie einer vorgeschlagenen Eisdiele, die man vor Ort vergeblich sucht, ärgerlich ist, kann bei Gesundheits-, zwischenmenschlichen oder psychischen Themen tragisch enden. Auch sind oft genug gesundheitsgefährdende Kochrezepte in den »Empfehlungen«, genauso wie juristische Fehlinformationen. Besser also immer die Fakten checken und Fragen zu Gesundheit und Zwischenmenschlichem mit anderen Menschen besprechen.

IMPRESSUM #digitalweiterwissen Das Magazin | Ausgabe 4 (2025)

HERAUSGEBERIN

Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK) e.V.
Obernstar. 24a | 33602 Bielefeld
www.gmk-net.de
Geschäftsführung:
Dr. Friederike von Gross,
André Weßel

GMK Gesellschaft für Medienpädagogik und Kommunikationskultur

REDAKTION

#DigitalCheckNRW
Telefon: 0521/677 88
www.digitalcheck.nrw
E-Mail: digitalcheck@medienpaed.de

DIGITAL CHECK NRW
Digital weiterwissen.

GESTALTUNG

Isabel Wienold, Bielefeld, iwi-design.de
E-Mail: iwi@iwi-design.de

Alle verwendeten Bilder wurden mit KI erstellt.

GEFÖRDERT DURCH

Minister für Bundes- und Europaangelegenheiten, Internationales sowie Medien des Landes Nordrhein-Westfalen und Chef der Staatskanzlei

„Ich schütze meine Daten, weil ich es mir wert bin! Schützt du auch deine?

Lerne die digitale Welt besser kennen und verstehen: www.digitalcheck.nrw

ÜBER DEN #DIGITALCHECKNRW

Der #DigitalCheckNRW ist ein kostenfreier Selbsttest im Internet. Mit seiner Hilfe können Nutzer*innen herausfinden, wie kompetent sie im Umgang mit digitalen Medien sind und z. B. ihr Wissen zu Themen wie Künstliche Intelligenz, Cybersicherheit und Desinformation verorten. Neben dem Ergebnis liefert der Test passende Weiterbildungsangebote aus einer umfangreichen Datenbank – vor Ort oder auch online. Zudem finden sich auf der Website im Bereich #digitalweiterwissen weitere Informationsangebote rund um digitale Mediennutzung und die durch sie geprägten Lebenswelten. Der #DigitalCheckNRW ist ein Projekt der Gesellschaft für Medienpädagogik und Kommunikationskultur e.V. (GMK) und wird gefördert durch die Landesregierung Nordrhein-Westfalens. Der Test basiert auf dem bewährten Medienkompetenzrahmen NRW, der erst für Schulen entwickelt und nun für Erwachsene nutzbar gemacht wurde, um die Förderung von Medienkompetenz und Medienbildung in jeder Lebensphase zu ermöglichen.

FEEDBACK UND ANREGUNGEN? NACHBESTELLUNGEN?

Du hast Ideen und Wünsche für unsere nächsten Ausgaben oder möchtest weitere Exemplare bestellen? Dann schreib uns eine E-Mail an digitalcheck@medienpaed.de. Wir freuen uns auf deine Rückmeldung!

DIGITAL CHECK NRW