„Update verfügbar – ein Podcast des BSI“

Transkription für Folge 66

Titel: Vom Like zum Leak – wie soziale Medien Daten weiterverkaufen

Moderation: Schlien Gollmitzer und Hardy Röde

Gast: Rainer Rehak vom Weizenbaum-Institut

Hardy: Schlien?

Schlien: Hardy?

Hardy: Wirst du eigentlich verfolgt?

Schlien: Kurzer Blick über die Schulter? Nervös, etwas? Nein, nicht, soweit ich weiß. Im Moment nicht. Wieso?

Hardy: Ich meine auch nicht Menschen, die hinter dir stehen können, sondern Dinge, die dir nachlaufen.

Schlien: Ah, okay. Dinge, die mir nachlaufen. Eigentlich habe ich eher so ein bisschen den Eindruck, dass Dinge mir weglaufen. Zum Beispiel, wenn ich das Haus verlassen möchte und meinen Autoschlüssel nicht finde oder sowas. Dann habe ich den Eindruck, dass der sich irgendwo verkrochen hat. Oder Sonnenbrillen ist auch so ein Thema. Ich habe ungefähr fünfmal die gleiche Sonnenbrille an strategisch wichtigen Plätzen verteilt, sodass ich immer eine mindestens finden kann.

Hardy: Aber nie ist sie da, wenn man sie sucht.

Schlien::Nie, ist sie da, wo ich sie vermute.

Hardy: Also mir geht es eher um Dinge, die dir online nachlaufen. Zum Beispiel: Stell dir mal vor: Die fünfte Sonnenbrille ist weg, du googelst nach neuem Sonnenbrillen-Sale und komischerweise rennt dir dann diese Sonnenbrille über dein ganzes digitales Leben wochenlang hinterher.

Schlien: Ja, doch, das kenne ich definitiv. Da werde ich gefühlt von zwei kompletten Kleiderschränken, vier verschiedenen Hausständen, mehreren Handtaschen und natürlich dem Sonnenbrillen-Sale und sehr, sehr wunderschönen Urlauben beispielsweise gestalkt.

Hardy: Alles klar, du kennst das Phänomen. Dann können wir heute in dieser Folge darüber reden: Warum verfolgt uns Werbung für so viele Dinge im Netz und eben auch in Socials, in Apps und so weiter? Und warum ist es wirklich ein Problem, dass da irgendjemand draußen anscheinend viel zu viel genau weiß, wer wir sind und was Schlien und Hardy gerade brauchen.

Das ist Update verfügbar – ein Podcast des BSI für Sicherheit im digitalen Alltag. Mit Schlien Gollmitzer und Hardy Röde.

Schlien: Um jetzt gleich mal mit diesem Gefühl von Paranoia zu starten – ich rede zum Beispiel mit Freunden über einen Urlaub, den ich ganz gerne machen würde. Vielleicht auch so ein bisschen darüber – also nicht einen Urlaub, den ich tatsächlich buchen kann. Und beim nächsten Griff nach dem Handy sehe ich auf einmal Urlaubswerbung oder Airbnb oder Booking oder wie sie alle heißen, der Tour und so weiter und sofort. Und dann frage ich mich schon manchmal so ein bisschen, hört da eigentlich jemand mit? Ist das so, wenn ich mein Handy neben mir liegen habe? Weil, ich will ja gar keinen Urlaub machen im Moment. Ist jetzt gar nicht so die Frage, ich mache eher so Urlaub auf dem Balkon sehr häufig.

Hardy: Es könnte sogar jetzt sein, dass gleich nach dieser Aufnahme, wenn wir auf Stopp gedrückt haben, du das nächste Mal auf dein Handy guckst und ausgerechnet dann Werbung für Urlaube auf deinem Handy erhältst.

Schlien: Stimmt! Wo ist mein Handy überhaupt?

Hardy: Dass unsere Handys uns abhören, um das schon mal zu spoilern, und dass irgendjemand quasi live mithört und uns dann mit Werbung vollballern kann, das wurde schon von vielen Experten und Expertinnen ziemlich genau untersucht und nach allem, was man so mitlesen kann, also an Datenverkehr oder dem Verhalten von Smartphones, hört normalerweise keiner einfach so uns zu. Also wenn man jetzt mal ausnimmt, dass bestimmte Leute, PolitikerInnen oder Menschen, die in Unternehmen zentrale Positionen haben, dass die gezielt attackiert werden – von Geheimdiensten oder sehr spezialisierten Kriminellen, die es auf eine Person gezielt abgesehen haben und Schwachstellen im Handy ausnutzen.

Schlien: Okay, also auf mich hat es jetzt keiner abgesehen. Das heißt, dass mir plötzlich Gartenschlauch-Werbung angezeigt wird, ist dann doch eher Zufall und liegt nicht daran, dass mir zugehört wurde. Und dann natürlich auch irgendwie so dieser immense Aufwand, den man da betreiben würde. Nur wegen meines Gartenschlauchs, das macht ja keinen Sinn.

Hardy: Genau, also das ist der Wissensstand da draußen, dem vertraue ich auch. Aber zweite Erkenntnis aus diesem allem, warum du tatsächlich oft das Gefühl hast, ich denke doch nur an Urlaub oder ich rede mit irgendjemandem drüber und zack kriege ich Werbung dafür: Das liegt unter anderem wirklich und im Ernst daran, dass dich so viele Tracking-Dienste oder die Social-Plattformen, auf denen du unterwegs bist. Oder im Hintergrund auch Datenaggregatoren und Datenbroker, die also Daten zusammenführen und weiterverkaufen von verschiedenen Stellen, dass die dich einfach viel genauer kennen, als du glaubst.

Schlien: Das ist schon krass creepy ehrlich gesagt, weil dann merkt dieses Datensammelsurium: Ah die Schlien war schon lang nicht mehr im Urlaub, es wäre dann mal wieder so weit. Ich weiß aber nicht, was ich jetzt creepier finden soll, dass mich mein Handy abhört oder dass all diese Daten von mir existieren, auf die einfach nur zugegriffen werden muss.

Hardy: Beides ist keine sehr schöne Vorstellung natürlich. Und diese tiefgehende Datensammlung und Zusammenführung über uns, dich und mich und euch Hörerinnen da draußen, sehr wahrscheinlich auch, die zum Beispiel in diesen Plattformen anfängt, die wir alle irgendwie nutzen, die ist also wirklich ganz real. Nehmen wir jetzt nur als Beispiele die ganz Großen: Google, Meta mit Facebook, WhatsApp, Instagram und so weiter. Oder TikTok, Twitter alias X oder, oder, oder. Die wissen alle eine ganze Menge von uns. Darüber sollten wir dringend reden.

Schlien: Ich würde aber ganz gerne vorher noch über diesen Begriff Tracking reden, den wir gerade schon verwendet haben. Den kennen viele von euch garantiert. Aber auch hinter dem steckt schon deutlich mehr, als man vielleicht so denkt.

Hardy: Dann erklären wir das doch gerne.

Schlien: Was ist eigentlich Tracking? Tracking bedeutet, dein Verhalten im Netz, am Computer, am Smartphone und so weiter – das wird erfasst und ausgewertet. Also zum Beispiel, wenn du Websites besuchst, auf Inhalte klickst oder etwas suchst oder eine App nutzt, die Daten über dich sammelt. Dabei entstehen viele kleine Stückchen an Informationen, welche Seiten du anschaust, wie lange du bleibst oder auch wie du dich bei der Nutzung einer App genau verhältst. Tracking ist also kein einzelnes Werkzeug, sondern ein Zusammenspiel verschiedener Techniken. Cookies sind ein Teil davon. Die kennen viele, es gibt sie schon lange und wir klicken wahrscheinlich jeden Tag zig Banner auf Websites weg, die uns über Cookies informieren. Aber es gibt zum Beispiel auch Gerätekennungen, die wie ein Fingerabdruck dein Smartphone oder deinen Computer sehr genau identifizierbar machen. Oder unsichtbare Skripte, die zum Beispiel bei manchen Apps im Hintergrund laufen. Aus vielen, vielen solcher Daten entstehen Profile und die können ziemlich genau sein: Wofür du dich interessierst, was du in eine Suchmaschine halb eingetippt hast, aber dann doch nicht gesucht hast. Oder aus vielen einzelnen Puzzlestücken zusammengesetzt eine Information darüber, in welcher Lebenssituation du anscheinend gerade bist. Dieses Bild von dir wird – natürlich – für Online-Werbung genutzt, die dir möglichst genau passende Artikel anbieten soll. Aber zum Missbrauch solcher Daten ist es leider kein weiter Weg, sodass ein Profil von dir zum Beispiel auch für gezielte politische Manipulation benutzt werden kann.

Hardy: Wir müssen uns also ganz viel Technisches anschauen und ganz viel mögliche Folgen davon, welche Daten über uns gesammelt werden in ganz verschiedenen Bereichen, wenn wir wissen wollen, wie aus unserem harmlosen Like ein Leak wird. Also wie solche einzelnen, harmlose Daten zusammengefügt werden und dann am Ende viel zu viel über uns erzählen, ob legal oder illegal. Ich habe dazu ein Interview geführt mit jemandem, der seit Jahren sehr genau in viele dieser Bereiche schaut und der uns ein klares Bild davon zeigen kann, was technisch im Hintergrund passiert, wenn im Netz und im analogen Leben auch Daten über uns gesammelt werden. Und er weiß auch, an welcher Stelle das problematisch wird für uns als Menschen und für unsere ganze Gesellschaft.

Rainer Rehak arbeitet beim Weizenbaum-Institut in Berlin. Er forscht dort zu den gesellschaftlichen Auswirkungen digitaler Technologien. Besonders beschäftigt er sich mit der Frage, wie Daten, Plattformen und Algorithmen unseren Alltag prägen. Das macht er gleich in mehreren Arbeitsgruppen. Zu einer habe ich ihn gleich gefragt, weil der Name schon eine ziemliche Ansage ist, finde ich: Die Forschungsgruppe heißt Technik, Macht und Herrschaft. Rainer, hallo und vielen Dank schon mal, dass du bei uns bist. Du bist ziemlich gefragt, oft in öffentlichen Debatten, Anhörungen, Workshops für Ministerien, Behörden und andere Organisationen. Du arbeitest auch immer wieder mit dem BSI eng zusammen. Jetzt Technik, Macht und Herrschaft. Wie muss ich mir das vorstellen? Wie forscht ihr da an eurem Institut zu diesen Themen?

Rainer: Ja, sehr gerne. Danke für die Einladung. Na ja, Technik, Macht und Herrschaft, das ist quasi die Analyse der technischen Systeme. Dann auch die Frage, wer eben Macht darüber ausübt, im Sinne von: Wer formt sie? Wer gestaltet sie? Wer wird gehört, wer wird nicht gehört? Wozu wird sie verwendet? Welche Rahmenbedingungen gibt es, um sie zu verwenden? Und Herrschaft ist die Frage danach: Welche Macht, die da ausgeübt wird, ist eigentlich legitim oder nicht legitim. Wir haben auch eine Rechtswissenschaftlerin, die die Gruppe leitet. Aber auch Soziologin, ich bin Informatiker, alles interdisziplinär, um – wie das Weizenbaum-Institut ja aufgestellt ist – die Digitalisierung zum Wohle der Gesellschaft zu

erforschen. Und da ist es natürlich eben zentral, genau diese Gestaltungs- und Machtfragen auch zu stellen.

Hardy: Wenn wir jetzt das hochkomplexe Themenfeld, womit du dich mit Kolleginnen und Kollegen in eurer Forschungsgruppe beschäftigst, wenn wir das auf was ganz Konkretes runterbrechen, was jeder und jede von uns schon mal erlebt hat: Ich google irgendetwas, ein Produkt, ich like irgendetwas auf einer Social-Media-Plattform. Ich überlege mir, ob ich einen Urlaub irgendwo buche und plötzlich verfolgt mich thematisch etwas, teilweise über Wochen, auf jeden Fall über mehrere Plattformen. Was passiert da im Hintergrund? Können wir erklären, wie so etwas zustande kommt?

Rainer: Ja, das ist eine sehr gute Frage. Das hat was damit zu tun, dass viele der Werbeanbieter oder auch der Social Networks und der Nachrichtenportale und Blogs und so weiter, selbst auch, um sich zu finanzieren, teilweise sozusagen Werbung anzeigen. Und die einzelnen Dienste, die sammeln nicht jeweils einzeln Daten, sondern die werden von Werbevermarktern im Hintergrund zusammengeführt. Das ist teilweise Facebook oder Meta, teilweise sind es aber auch andere Werbenetzwerke, bei denen kann man Werbeplatz kaufen. Oder man kann selbst diese bei sich einbinden. Da gibt es auch große Player mit Google Ads und so weiter Es gibt aber auch kleinere. Diese Werbenetzwerke funktionieren deswegen, weil sie die Werbung und die User-Eingaben und das User-Verhalten und die Likes und diese ganzen Daten über Plattformen und über Netze und Webseiten hinweg zusammenführen.

Hardy: Um kurz einzuhaken: Das Gefühl, ich werde verfolgt, ist dann schon eigentlich ganz richtig. Also, dass man da vielleicht ein bisschen Paranoia kriegt, dass etwas, was sich anfühlt wie: Ich hatte doch gerade nur einen Gedanken oder einen Wunsch im Kopf und plötzlich weiß das Internet das alles. Das ist gar nicht so weit hergeholt.

Rainer: Ne, das ist gar nicht so weit hergeholt. Und es geht sogar auch so weit: Mal angenommen ich bin in meinem Browser in drei Tabs auf drei verschiedenen Plattformen angemeldet und dann in meinem Mobiltelefon in fünf anderen, dann ist natürlich klar, wenn ich auf beiden bei Google angemeldet bin oder bei anderen Diensten, dass ich darüber eine Verbindung kriege, auch über Geräte hinweg. Und das ist in dem Moment natürlich dann eine Sache, die wir Menschen, wenn wir jetzt gerade auf irgendeine Aufgabe fokussiert sind oder auch in sozialer Interaktion stecken, selten im Kopf haben, in wie vielen Verbindungen wir gerade aktiv drinstecken. Und die Systeme sind dann natürlich gnadenlos, sozusagen, und verbinden diese Sachen. Es gibt allerdings noch einen zweiten Effekt, der ist klein, aber den will ich trotzdem nennen. Das ist das Prinzip der selektiven Wahrnehmung, das kennen wir sicherlich auch alle. Wenn ich mir eine rote Handyhülle kaufe, fällt mir danach auf, wie viele Leute in der Bahn rote Handyhüllen haben. Und es ist ja nicht so, dass plötzlich sich alle rote Handyhüllen gekauft haben, um mir einen Streich zu spielen, sondern es fällt mir einfach auf. Diesen Teil muss man schon auch noch sehen, um diese Paranoia vielleicht auch so ein bisschen abzumildern.

Hardy: Jetzt können wir das einfach mal creepy finden und da eine Haltung dazu haben und sagen, geht nicht. Jetzt könnten wir aber auch die Meinung vertreten, die Plattformen müssen Geld verdienen. Und das passiert mit Werbung. Es ist sehr viel, was wir benutzen, jeden Tag in unserem Alltagsleben im Netz, kostenlos. Und irgendwo muss Erlös ja herkommen, zum Beispiel mit Werbungen. Wie legitim ist das?

Rainer: Man kann jetzt erst mal sagen, in einem marktorientierten kapitalistischen Wirtschaftssystem ist jetzt erst Mal Werbung zu machen, es gehört halt einfach mit dazu. Also: Warum soll man es online nicht machen, wenn man es offline auch macht? So könnte man die Frage stellen. Also wenn man das ablehnt, dann ist es auch okay, dann müsste man das in gleichem Maße online wie offline angehen. Der Unterschied ist nur, dass es

gerade im Online-Bereich sehr, sehr detailliert wird. Also diese Daten, die über Menschen entstehen, das sind nicht nur Vorlieben wie, mag gerne Kaffee, sondern es gibt da wunderbare Forschungen. Die haben über investigative Recherchen Datensätze bekommen, wo die Klassifizierungen mal aufgelistet worden sind. Und es sind dann eben Leute, die Autos mögen und so weiter Aber das sind auch Leute, die gerade vulnerabel sind, weil sie in einer Trennung sind. Oder Kategorie Teenager mit Identitätsfragen. Oder die Kategorie Frauen in der Schwangerschaft. Oder abhängig von Drogen und so weiter. Also das sind hochsensible Sachen, die teilweise, wenn es um psychische Fragen geht, vielleicht die Menschen selber nicht mal wissen. Das heißt, wir haben da so eine systematische psychologische Auswertung ganzer Gesellschaften. Wobei diese Werbenetzwerke im Endeffekt Psychogramme haben, die weder irgendein politischer Akteur noch irgendein anderer Akteur hat. Und die sind dann international tätig und können Gesellschaften quasi bewerten und danach beeinflussen. Und aus dieser politischen Theorie würde man dann fragen, wo kommt da eigentlich bei dieser Macht die Legitimität her? Niemand hat die gewählt. Die Aktivitäten sind teilweise fragwürdig. Bis jetzt ist es so, dass sich Max Zuckerberg seit 15 Jahren jedes Jahr tief entschuldigt für all diese Probleme, die immer verursacht werden. Spätestens, wenn Parteien diese Manipulationswerkzeuge, ich sage es mal explizit, dafür verwenden, Menschen in eine Richtung zu drängen, nicht nur Sachen zu kaufen, sondern für Parteien zu wählen oder bestimmte Glaubenssätze zu erheben. Oder auch ihre politische Meinung zu radikalisieren, finde ich, reden wir auf einmal nicht mehr nur über Werbung.

Hardy: Du hast ein paar Player schon erwähnt, die da tätig sind. Du hast unter anderem von Meta, dem Mutterkonzern von Facebook, WhatsApp und diversen anderen Plattformen, Instagram natürlich gesprochen. Kannst du uns so ein kleines Panoptikum aufmalen, wer da aktiv ist. Ich sehe nur manchmal auf Websites, wenn das Cookie-Banner kommt, dass ich dem Teilen meiner Daten mit unseren 976 Partnern oder über 1000 sogenannten Partnern zustimmen soll. Und da denke ich mir, ach, das sind ja viele. Gibt es da eine Struktur, die du uns aufmalen kannst, um das zumindest durchschaubar zu machen für uns?

Rainer: Das ist eine sehr gute Beobachtung, wie komplex das eigentlich ist. Man kann erst mal sagen, es gibt viele kleine Tools, die einem auch visualisieren, wie hängen die zum Beispiel zusammen? Welche Akteure sind das? Wo sitzen die und so weiter? Aber grob kann man eigentlich unterscheiden zwischen denen, die quasi so groß sichtbar sind, also Google, Meta und so weiter, die direkt auch diese Daten sammeln, um selber noch Werbung auszuspielen. Und die anderen anbieten, Werbung auf Basis dieser Daten auszuspiele. Das heißt, die machen das ganze Tracking und bieten dann als Produkt den Zugang zu den Nutzerinnen und Nutzern an. Und die geben die Daten auch nicht raus. Also, das ist ihr eigenes Asset, das ist ihr größter Schatz. Dieser Punkt sorgt dann auch manchmal für irritierende Szenen, wenn dann zum Beispiel im US-Senat Mark Zuckerberg von so Senatoren oder Parlamentariern gefragt wird, ob sie denn wirklich keine Daten verkaufen. Und er eben ganz ehrlich und wahrhaftig sagt, nein, wir verkaufen keine Daten. Als wäre das eine Verteidigung. Aber der Punkt ist natürlich, natürlich verkaufen sie keine Daten. Das ist eben nicht ihr Geschäftsmodell. Ihr Geschäftsmodell ist: Ich gehe da hin und sage, ich würde gerne Teenager in einer Identitätskrise, denen würde ich gerne ein Produkt verkaufen. Oder Leute, die mit dem demokratischen System sehr unzufrieden sind, denen möchte ich gerne eine politische Werbung anzeigen. Dann gebe ich den Playern das Geld und die Werbung und dann sorgen diese dafür, dass das zum richtigen Moment bei der richtigen Person ankommt. Das ist so die eine Kategorie. Dann gibt es die zweite Kategorie von denen, die mit Daten handeln. Die Daten erheben und diese Daten dann zusammenführen, rekombinieren, Kategorien daraus bauen, Pakete bauen und die dann anderen zum Verkauf anbieten. Das sind dann sozusagen so Werbenetzwerke, die zum Beispiel in Apps oder in Webseiten oder in Produkten sozusagen ihre Dienste anbieten, die werden dann da integriert. Bei Apps heißt das dann, da werden so Tracker eingebaut. Das steht dann meistens auch in den Bedingungen, wie du schon gesagt hast, irgendwo ganz

unten. Und diese Daten fließen dann irgendwo hin. Das sind dann so Firmen wie Axiom oder Cobweb oder so, das sind so verschiedene Namen, die man üblicherweise noch nie gehört hat. Weil die eben nicht, sozusagen im Jargon würde man sagen, wie Consumer Facing sind. Die haben selber mit den Nutzerinnen und Nutzern nichts zu tun. Die kriegen dann ein bisschen Geld von den Werbetreibenden oder von den Trackingfirmen, dafür, dass sie die mit einbauen. Genau, dafür kriegen die dann die Daten. Und dann gibt es diese Daten, diese Datenpakete, die dann sozusagen angeboten werden. Und die kann man dann kaufen, um wiederum andere Werbung irgendwo auszuspielen. Die kann man kaufen, um zum Beispiel die eigenen Produkte zu verbessern, weil man Erkenntnisse kriegen kann. Die werden allerdings auch gekauft von politischen Parteien, um ihre Wahlregister aufzufrischen. Ich sag jetzt mal nett aufzufrischen. Da gibt's auch verschiedene Regeln in Deutschland, zum Beispiel in der EU ist es schwieriger als in den USA. Und wir sehen aber auch zunehmend, und das ist ein Problem, dass diese Daten gekauft werden von Polizeien, von Militärs, von Geheimdiensten und zum Beispiel von der ICE, von der Behörde in den USA, die diese Deportationen durchführen, um Leute zu tracken. Der Weg ist: Leute in den US haben irgendeine Shopping-App, dadurch ist klar, wo die sind. Dann liken sie Sachen oder surfen auf irgendwelchen Seiten. Dadurch wird klar, wer sie sind, was sie machen, wo sie sind und so weiter Und wann sie das machen.

Hardy: Ab hier klingt es so wie etwas, was nicht mit diesen Daten passieren sollte, also etwas, womit ich auch nicht rechne als Nutzerin oder Nutzer in meinem ganz normalen Umgang mit Plattformen im Web, mit Apps, die ich auf meinem Handy habe und dem digitalen Leben, was ich einfach lebe.
Die Frage, was mit diesen Daten schiefgehen könnte, da sind wir jetzt schon mittendrin. Ich würde gern von dir wissen: Was ist denn der Worst Case? Ist der Worst Case dieser ganz normale Gebrauch, diese ganz normale Nutzung der Daten für bestimmte Zwecke?

Rainer: Einerseits sehen wir, da sind natürlich riesengroße Daten, die entstehen. Es gibt regelmäßig Leaks. Und diese Leaks sorgen regelmäßig auch für Wellen von – man sagt das immer so – Identitätsdiebstahl. Also, wenn ich Passwörter und Zugänge habe – teilweise ist es E-Mail oder Facebook oder so – und wenn man die gleichen Passwörter in verschiedenen Services verwendet, insbesondere bei E-Mail, da sind ja dann andere Services mit dran verbunden, ist es relativ einfach, aus so einer großen Datenbasis da quasi die Identität von vielen Menschen zu übernehmen und dann Sachen einzukaufen oder Sachen zu posten oder so. Und da gibt's quasi eine ganze Bandbreite von allein finanziellen Schäden über einfach zeitlichen Aufwand, das alles wieder zurückzudrehen, bis hin zu dem Verlust zum Zugang zum halben Leben, wenn man sich da sozusagen in der Cloud das gemütlich gemacht hat. Und das ist hochproblematisch an der Stelle und individuell einfach sehr ärgerlich. Jetzt haben wir natürlich aber auch die Situation, dass da sehr viel Wissen über ganze Gesellschaften drinsteckt. Das heißt, diese Illusion, dass ich das persönlich entscheiden könnte, die müssen wir uns in der vernetzten Gesellschaft leider abschminken. Das heißt, wir müssen damit auch kollektiv umgehen. Wir müssen darüber nachdenken, es ist kein individuelles Problem mehr. Jetzt zu dem Gefahrenpotenzial. Jetzt kann man ein bisschen schwächer auch sagen, wenn mir da jemand in meinen schwachen Momenten genau das Richtige anbietet, ist es auch sehr ärgerlich, wenn ich zu Käufen gebracht werde, die ich dann später bereue. Und jetzt kann man sagen, mal angenommen, diese Daten werden veröffentlicht oder kommen in falsche Hände. Dann ist das auf jeden Fall hochproblematisch. Ich würde gerne ein anderes Szenario mehr in den Vordergrund schieben, denn wir sehen jetzt gerade, also die meisten dieser Firmen sitzen in den USA, gerade die großen, also Big Tech könnte man auch so zusammenfassen, gerade in Bezug auf Werbung und da ist die politische Situation ja auch gerade nicht besonders einfach. Das heißt, es ist so ein bisschen so eine Frage, die wir uns stellen müssen, Machtzentren entstehen zu lassen. Dann wird da ein, zwei Mal in eine Richtung gewählt. Und dann findet ein Staatsumbau in Richtung Autoritative bis – je nachdem, wo man dazu hört – Faschistoide statt. Und dann sind die Firmen, die wir als Dienstleister wahrgenommen

haben – als Teil der Wirtschaft – auf einmal komplett Gegenstand eines politischen Diskurses. Und da merkt man so ein bisschen, dass diese Frage, wenn das in falsche Hände gerät, dass man die auch anders stellen kann und fragen kann. Diese Daten sind da, was passiert, wenn der Akteur, der die hat, auf einmal seine Meinung ändert. Oder sie schon immer so hatte, aber es immer anders dargestellt hat. Das ist eine große Legitimitätsfrage, dass Firmen in anderen Ländern Einfluss haben auf deutsche Geschicke oder auch europäische Geschicke. Wo kommt die Legitimität her? Wie kann man die herstellen und wie kann man die einhegen? Das ist dann eine politische Frage. Aber das Gefahrenpotenzial ist dann enorm, politisch Einfluss zu nehmen oder auch Menschen einfach, das Leben schwer zu machen. Und ich würde sagen, aus demokratietheoretischer Sicht ist das Problem nicht erst da, wenn man konkret von Identitätsdiebstahl betroffen ist oder wenn man jetzt konkret Sachen falsch gekauft hat. Sondern der Aufbau dieser Macht, die dahintersteht. Die allein würde ich schon als problematisch ansehen.

Hardy: Was du schilderst, ist ja so umfassend, passiert auf so vielen Ebenen, mit so vielen teilweise wirklich sehr mächtigen Akteuren – seien sie politisch, seien sie im Bereich Unternehmen. Es ist international, es ist sehr bis völlig intransparent. Wer hilft uns denn da als Nutzerinnen und Nutzern? Wer schützt uns denn? Kann es eine Instanz geben, die uns vor etwas schützt, was mit unseren Daten passiert.

Rainer: Man muss glaube ich trotzdem sagen: Die Zukunft ist offen und wir haben das Glück im – ich würde mal sagen –demokratischsten Teil der Welt zu leben. Es gibt auf jeden Fall Möglichkeiten sich zu schützen, aber auch den Schutz oder diese Art von Problemen irgendwie politisch anzugehen. Ich würde auch gar nicht so eine Hilflosigkeit hinstellen. Wir haben diverse Situationen gehabt, zum Beispiel als Facebook damals WhatsApp gekauft hat und alle Daten zusammenführen wollte, da haben dann die deutschen Datenschutzbehörden gesagt, die führt ihr nicht zusammen, und dann wurden sie nicht zusammengeführt. Wo man das wollte, dann ist es tatsächlich auch passiert. Oder Twitter zum Beispiel damals, oder X wollte bestimmte Regelungen vom brasilianischen Staat nicht umsetzen in Bezug auf Datenverarbeitung. Und dann hat der Staat ihm angedroht, Twitter komplett zu sperren. Und dann plötzlich ging es. Dann hat sich X gefügt. Also viel an der Stelle ist auch eine Frage des Wollens. Und da darf man, glaube ich, nicht vor den eigenen Möglichkeiten zurückschrecken.

Hardy: Du meinst also, was wir machen können, ist in erster Linie ein politisches Verständnis, ein politisches Agieren und sich zum Beispiel als Europäische Union sehr klar zu positionieren und sehr klar hinzustellen. Das ist, wenn ich dir zuhöre, ein mächtigerer Hebel, als ich es dachte.

Rainer: Genau. Der große Hebel ist auf alle Fälle der politische Hebel und aus demokratischer Sicht ist das eine Frage, welche Parteien wählen wir, schreiben wir unsere Abgeordneten mal an, aber auch ganz simpel zum Beispiel: Es gibt auch wirklich beeindruckend auswirkungsreiche NGOs und auch journalistische Stellennetzpolitik oder es gibt auch Non-On-View-Business, also das ist so eine NGO in Österreich, die so Datenschutzklagen macht – strategisch auf europäischer Ebene gegründet, damals von Max Schrems, der auch schon sozusagen dieses EU-US-Privacy-Shield und Safe Harbor weggeklagt hat.

Hardy: Damals ein Jurastudent aus Österreich, dessen Name jetzt zum geflügelten Wort in den Datenschutzkreisen geworden ist.

Rainer: Absolut, genau. Und der einfach weggeklagt hat, dass die Datenschutzregelungen von den USA mal eingehalten werden. Und die Gerichte, das Europäische Gericht, hat dann auch festgestellt, dass diese Geheimdienstregeln in den USA und so weiter nicht mit europäischem Datenschutzrecht kompatibel sind. Oder Netzpolitik.org, die gute Recherchen

machen, das gut aufbereiten, dass auch normale Menschen das nachvollziehen können, was gerade passiert und was man da tun kann und so weiter. Und das ist natürlich auch eine Möglichkeit, die einfach zu unterstützen. Es gibt auch andere Projekte, zum Beispiel das BSI hat auch den Dialog mit der Zivilgesellschaft, wo ich selber auch im Dialogkomitee bin. Wo Menschen in der Zivilgesellschaft, also technikinteressierte, aber auch digitalpolitikinteressierte, Projekte vorschlagen können und die werden dann finanziert und unterstützt. Also da gibt es auf vielen Ebenen Möglichkeiten: Ohne dass man das jetzt selber machen müsste, kann man einfach die Organisationen unterstützen, die das machen.

Hardy: Jetzt geben wir hier in „Update verfügbar“ den Hörerinnen und Hörern gerne Tipps, wie sie konkret handeln können. Angesichts der 976 Tracker, denen ich beim Aufruf einer ganz normalen Website ab und zu zustimmen soll, fühle ich mich bei dem Thema aber so ein bisschen überfordert. Und Frage an dich Rainer: Macht das überhaupt Sinn? Diese 976-Tracker einzeln wegzuklicken, an welcher Stelle soll ich ansetzen bei meiner Online-Nutzung, wenn ich das nicht möchte, was du uns schilderst?

Rainer: Also wir haben ja zum Beispiel das Glück in Europa, dass ganz viele Webseiten zwar diese nervige Cookie-Banner und so weiter anzeigen müssen, aber an ganz vielen Stellen gibt es genau auch den Knopf, nee, ich möchte alle ablehnen. Das gibt es in anderen Ländern oder in anderen Bereichen der Welt nicht. Das kann man sich ein bisschen angewöhnen, da einfach immer auf `Ablehnen´ zu klicken. Also manchmal geht das nicht, aber sehr, sehr oft geht das und das ist so ein erster kleiner Schritt. Das auch einfach zu praktizieren, es dauert ja genauso lange auf `Zustimmen´ zu klicken wie auf `Ablehnen´. Und dann kann man auch auf `Ablehnen´ klicken. Es gibt auch für Web-Browser so was wie Adblocker. Da gibt es auch sehr einfache, die automatisiert die Standard-Werbung wegziehen. Und gerade dieses Anzeigen von Werbung sorgt auch für sehr viel neues Datenaufkommen. Diese Adblocker sind sowohl aus Datenschutzsicht, aber auch aus IT-Sicherheitssicht – manche von diesen Werbungen enthalten auch Schadsoftware – eine super Idee.

Hardy: Als Plug-in im Browser?

Rainer: Genau, Plug-In im Broser, genau. Bei Telefonen oder bei Smartphones oder Tablets oder so, kann man sagen, viele von diesen kleinen, kostenlosen Apps, diese Spiele oder Wetter-Apps sind auch so eine Sache, das ist wirklich sehr schwierig. Viele von diesen kleinen Sachen, da kommen die Apps mit sehr viel Tracking und die Webseiten aber nicht. Vielleicht kann man da ein bisschen reduzieren – einfach weniger Apps. Dieses kleine kostenlose Zeug – das ist leider immer noch so – wenn es kostenlos ist, dann muss man sich fragen, was da das Geschäftsmodell ist. Das hilft auf alle Fälle. Man kann auch den Browser zum Beispiel wechseln. Und wenn ich mich ein bisschen mehr damit beschäftige, kann ich auch Datenschutzeinstellungen durchgucken in Social-Media-Netzwerken. Da gibt es teilweise Einstellungen, mit wem Daten geteilt werden und ob personalisierte Videoempfehlungen oder so weiter angezeigt werden. Das ist immer auch mit einer Einwilligung verbunden, diese Daten auch zu verwenden. Das ist eine Sache. Und wenn ich noch tiefer einsteigen will, kann ich natürlich auch mal schauen, möchte ich vielleicht in alternative soziale Netzwerke gehen, wie zum Beispiel Mastodon oder so, die sind komplett werbe- und manipulationsfrei. Das ist ein bisschen was anderes, aber der Aufwand ist da ein bisschen höher. Ich glaube, das ist ganz gut so Schritt für Schritt. Da gibt es auch gerade dieses Projekt des D-Days, also des Digital Independence Days. Da kann man, glaube ich, auch noch mal nachsuchen und gucken, sich Hilfe holen. Das ist eine gute Idee, sich von diesen Machtzentren generell zu entfernen. Und das hilft auf alle Fälle. Also zusätzlich zu diesen strukturellen Sachen, die wir vorher besprochen haben. Und diesen Podcast hören natürlich.

Hardy: Danke fürs Endorsement. Mit dem Blick auf das, was sich im Großen, im Strukturellen, im Politischen bewegen kann – wie du sagst – und den Schritten, die ich als Nutzerin oder Nutzer selber gehen kann, lässt du uns jetzt hier nicht ganz hoffnungslos zurück nach diesem Interview. Rainer, es war ein spannender Blick hinter die Kulissen dessen, was mit unseren Daten passiert. Ich danke dir ganz, ganz herzlich, dass du dir die Zeit genommen hast.

Rainer: Vielen Dank für die Einladung. Und ja, wir sind nicht machtlos. Das ist in der Tat der Fall. Danke dir.

Schlien: Krass, Hardy, dieses Interview, das ihr da geführt habt. Ich muss immer wieder dran denken, so vor zehn Jahren ungefähr fand ich das eigentlich praktisch, dass das Internet vor mir schon wusste, wo ich den günstigsten Gartenschlauch herbekomme oder die nächste Sonnenbrille für meine große Sammlung oder sowas. Aber mittlerweile ist es ja wirklich nur noch creepy und gruselig. Und weil wir es vorhin schon von diesen Cookies hatten. Das Interview hat mir jetzt ein bisschen wieder zurück in Erinnerung gerufen oder auch aufgezeigt, dass es eben schon auch in meiner Hand liegt, mich darum zu kümmern, aber nicht nur.

Hardy: Ja, tatsächlich. Also dass es kein rein individuelles Thema ist, wo man sagt, ja, passt besser auf eure Daten auf.

Schlien: Selbstverantwortung.

Hardy: Richtig, sondern dass wir uns da als Teil einer Gesellschaft verstehen, die selber Gesetze und den gesamten Rahmen für das, was technisch passiert, in die Hand nehmen kann und damit auch was verändert. Also dass wir nicht ausgeliefert sind, sondern, dass wir politisch, gesellschaftlich auch im Kleinen Möglichkeiten haben, was zu ändern.

Schlien: Und trotzdem, das haben wir ja jetzt vom Rainer gerade gehört, bringt es etwas, auf alles ablehnen zu drücken. Also man muss jetzt nicht gleich Facebook verklagen, wie ein österreichischer Jurastudent, aber man hat es trotzdem selber auch in der Hand. Und auch wenn es manchmal nervt, bitte erst mal alles ablehnen und nicht jeden Cookie akzeptieren, der einem da geboten wird.

Hardy: Damit ist ein Anfang auf alle Fälle gemacht. Rainer hat im Interview ziemlich viele handfeste und einfache Tipps gegeben, wenn ihr euch noch weiter mit dem Thema beschäftigen wollt. Beim Bundesamt für Sicherheit in der Informationstechnik, dem BSI, da findet ihr viele Infos und konkrete Tipps.

Schlien: Die Links stellen wir euch wie immer in die Show-Notes zu dieser Folge. Und wenn sie euch gefallen hat, diese Folge, dann abonniert uns doch gerne und empfehlt uns auch weiter an eure Freunde. Dann verpasst zum einen ihr nicht die nächste Folge und zum anderen könnt ihr euch mit euren Freunden dann endlich mal über was Vernünftiges unterhalten mit Inhalt und nicht nur über das Wetter.

Hardy: Das war es jedenfalls für heute mit „Update verfügbar“. Wir sagen herzlichen Dank fürs Zuhören.

Schlien: Bis zum nächsten Update!

Hardy: Bis zum nächsten Update.