Novo Argumente für den Fortschritt

05.03.2018

„Die Freiheit bleibt vollkommen auf der Strecke“

Interview mit Volker Tripp

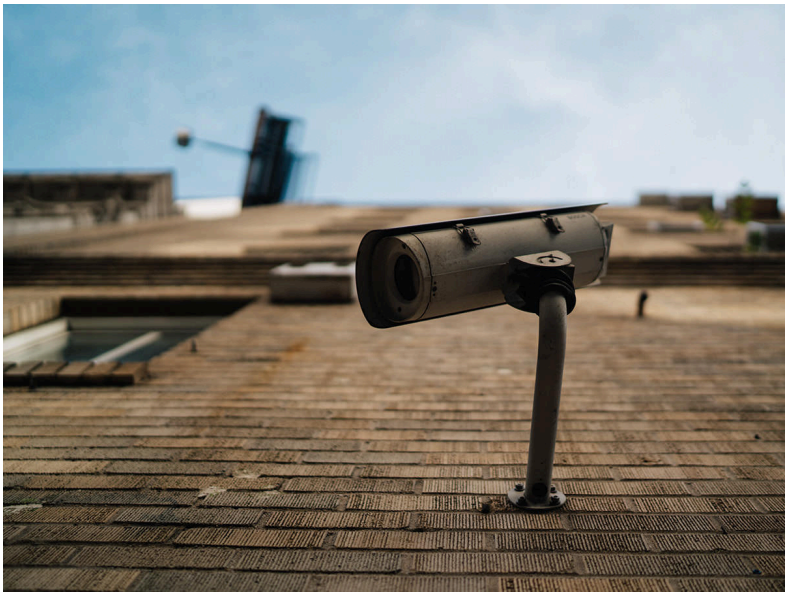

Foto: Rishabh Varshney via Unsplash.com / CC0

Im Netz werden Grundrechte zunehmend dem Sicherheitsdenken geopfert. Volker Tripp vom Verein Digitale G trojaner & Co. widersetzen sollten.

Novo: Herr Tripp Digitalen Gesellschaft, einem Verein, der 2010 als Interess braucherrechte gegründet wurde. Warum brauchen

Volker Tripp: Es ist er digitale Wandel alle Bereiche der Gesellschaft durc , ist Netzpolitik heute Gesellschaftspolitik. Die bestimmende herheitsbehörden und Wirtschaftsunterr Gestaltung dieses sehr wichtigen Politikfeldes zu üb g auch eine netzpolitische Vertretung der digitalen Zivilgese s. Unser Ziel ist dabei, der Wahrnehmung entgegenzutreten Wirtschaftsfaktor oder Sicherheitsrisiko sind. Wir wollen ei itale Raum auch ein Entfaltungsraum für die Grundrechte is

Eine Entwicklung e Sorgen bereitet, ist das kürzlich vom Bundestag verab at es damit auf sich?

Die Kritik an dem , schon mit der Art und Weise seines

Themen
Artikel
Printausgabe
Rezensionen
Über Novo
Unterstützen
Printausgabe kaufen

Zustandekommen n der Strafprozessordnung. Durch eine Formulierungshilf aatstrojaner in diesem Gesetz seinen Platz gefunden. Es gab wurde über die Gefahren und Risiken gesprochen. Dass lung des Bundesverfassungsgerichts, die sehr hart mit dies d extrem hohe Hürden für den Einsatz aufgestellt hat.

Jetzt kann man sic das Bundesverfassungsgericht formuliert hat, tatsächlich ge st. Es geht beim Staatstrojaner eigentlich um zwei Dinge: Er ner Hacker-Software, in fremde Computer eindringen, um di – das ist die sogenannte Quellen-TKÜ. Zweitens geht es uchung den Computer selbst zu durchsuchen. Bei dliche Grundrechte betroffen: In dem einen Fall ist es das Ferr ionsfreiheit; im anderen Fall sind es die informationelle Se ılichkeit und Integrität informationstechr gen sind in beiden Fällen höchst unterschiedlich. D ot in der Lage, trennscharf zwischen diesen unterschiedlichen prechend auch die unterschiedlichen Eingriffsvorausset schwer zu gewährleisten. Ich würde mich also weit aus dem erfassungskonformen Staatstrojaner. Es ist technisch nicht m ammieren.

Ein weiteres Probl ner auf den Computer des Betroffenen gelangt. Dazu gib ist, dass sich die Sicherheitsbehörden physikalisch des C spielen; oder aber sie erledigen das Ganze aus der Ferne, als ıdem sie Sicherheitslücken ausnutzen. Das bedeutet, dass de s, sie aber nicht schließen darf. Damit lässt er letztlich eine G diese Sicherheitslücken können nicht nur Sicherheitsbehörd e-Kriminelle. Wir müssen uns fragen: Wollen wir uns das als Ge t?

Ein weiteres Ther tsdatenspeicherung, also die anlasslose Speicherung von . Warum lehnen Sie diese ab?

Die Vorratsdatens und ist mittlerweile zu einer Art Symbolgefecht ge atenspeicherung abzulehnen, ist, dass sie ihren vorgesehen ekämpfung von schwerer Kriminalität und Terrorismus einse zigen konkreten Beleg dafür, dass die anlasslose Speicherung von Verkehrsdaten in irgendeiner Weise einen sinnvollen Beitrag dazu leistet.

Der zweite wesentliche Punkt ist die Anlasslosigkeit. Alle Menschen, die elektronische Kommunikationsmittel benutzen, müssen sich vom Staat wie Verdächtige behandeln lassen. Sie haben nichts weiter getan, als beispielsweise ein Telefonat zu führen, und doch werden die Verbindungsdaten, Standortsdaten usw. protokolliert.

Hinzu kommt die Missbrauchsgefahr. Egal, wie gut die Daten gesichert werden, wie dezentral sie gespeichert werden – es wird immer möglich sein, solche Sicherungen zu überwinden. Und das, was man mit diesen Daten machen kann, ist schon erschreckend: Wenn Sie Verbindungsdaten über einen längeren Zeitraum auswerten, können Sie mehr über einen Menschen wissen, als dieser Mensch über sich selbst weiß. Man kann ein extrem genaues Abbild seines Tagesablaufs, seiner Bewegungsmuster, seines gesamten sozialen Netzes schaffen. Man kann Aussagen über die sexuelle Orientierung treffen. Mit anderen Worten: Metadaten und Verkehrsdaten verraten unglaublich viel über Menschen. Deswegen ist die Speicherung dieser Daten kein oberflächlicher Eingriff. Er geht tief in die Privatsphäre und an die Grundfesten der Individualrechte.

Nun hat das Oberverwaltungsgericht Nordrhein-Westfalen kürzlich beschlossen, dass das 2015 von der Großen Koalition verabschiedete Gesetz zur Vorratsdatenspeicherung gegen EU-Recht verstößt. Die Speicherpflicht wurde ausgesetzt. Ist das Thema damit endgültig vom Tisch?

Leider nicht. Erstens: Es gibt noch andere Formen anlassloser Vorratsdatenspeicherung, etwa die Speicherung von Fluggastdaten. Pro Flug und Passagier werden bis zu 60 Einzeldaten über einen Zeitraum von fünf Jahren gespeichert und permanent einer elektronischen Rasterfahndung unterzogen. Mit der Maut haben wir eine 13-monatige Vorratsdatenspeicherung von Autokennzeichen. Zweitens ist die Speicherung von Telekommunikationsdaten keineswegs vom Tisch, denn das Gesetz gibt es ja immer noch. Die Bundesnetzagentur hat nur gesagt: Wenn Telekommunikationsunternehmen dieses Gesetz nicht umsetzen, werden wir nicht mit Sanktionen dagegen vorgehen. Aktuell steht noch die Entscheidung des Bundesverfassungsgerichts aus. Wenn das Gericht das Gesetz für verfassungskonform erklärt, könnte sich das ganze Spiel noch einmal ändern. Außerdem wird auf europäischer Ebene gerade über eine neue E-Privacy-Verordnung geredet. Dabei wird die Möglichkeit ausgelotet, einen Vorbehalt für die Vorratsdatenspeicherung explizit ins Gesetz einzubauen.

Nicht nur im Netz nimmt die Überwachung zu. Wer heute in der Öffentlichkeit unterwegs ist, kann damit rechnen, von unzähligen Überwachungskameras gefilmt zu werden. Als nächster Schritt sollen diese „intelligent“ werden, das Filmmaterial soll etwa mittels Gesichtserkennungssoftware ausgewertet werden. Was halten Sie von diesen Entwicklungen?

Wir lehnen auch diese Entwicklung ab, und zwar aus ganz grundsätzlichen Erwägungen. Gesichtserkennung bedeutet, dass die Computerprogramme hinter den Überwachungskameras mich eindeutig identifizieren und diese Information speichern können. Der Staat könnte so komplette Bewegungsprofile erstellen – von allen Personen, die sich auf seinem Territorium bewegen. Er könnte genauestens ausforschen, wer sich mit wem zusammen bewegt. Bei der intelligenten Videoüberwachung soll noch eine Verhaltensanalyse hinzukommen. Algorithmen sollen das Verhalten von Menschen bewerten: Ist das jetzt in irgendeiner Weise kritisch? Muss hier Polizeipersonal eingreifen?

In einer Situation, in der ich in der Öffentlichkeit nicht mehr anonym bin und in der mein Verhalten permanent von Algorithmen bewertet wird, wird zwangsläufig ein „Chilling-Effect“ einsetzen. Das heißt, Menschen werden sich überlegen, ob sie von bestimmten Grundrechten lieber keinen Gebrauch machen, weil es unter Umständen dazu führen könnte, dass man sie als verdächtig einstuft. Daher widerspricht speziell eine flächendeckende intelligente Videoüberwachung diametral dem Geist einer freiheitlichen Gesellschaft.

Wer sich heutzutage gegen die Ausweitung der Überwachung ausspricht, gilt schnell als nerviger Bedenkenträger, der das legitime Bedürfnis der Bevölkerung missachtet, vor Kriminalität und Terrorismus geschützt zu werden. Wer nichts zu verbergen habe, habe nichts zu befürchten. Was entgegnen Sie solchen Kritikern?

„Wer nichts zu verbergen hat, hat nichts zu befürchten“ – das können eigentlich nur Leute sagen, die unbekleidet im Glashaus wohnen, denen es also offenbar vollkommen egal ist, was andere Menschen von ihnen erfahren. Dieser Satz ist in vielerlei Hinsicht grundfalsch. Zunächst einmal verkehrt er das Rechtsstaatsprinzip in sein Gegenteil. In einem Rechtsstaat muss sich der Staat für jede Einschränkung der Freiheiten seiner Bürgerinnen und Bürger rechtfertigen und nicht umgekehrt. In dem Augenblick, in dem der Staat sagt: „Wer nichts zu verbergen hat, hat nichts zu befürchten“, muss ich mich als Bürger aber dafür rechtfertigen, dass der Staat nicht in meine Rechte eingreift.

Tatsächlich ist es natürlich so, dass jeder Mensch irgendetwas zu verbergen hat. Niemand wäre beispielsweise bereit, Ihnen einfach so den Schlüssel für seine Wohnung zu geben, die PIN seiner EC-Karte zu nennen oder Ihnen seine Steuererklärung zu zeigen. Insofern glaube ich, dass dieser Satz auch sehr häufig eine Art von geistiger Bequemlichkeit ist, eine Möglichkeit, sich nicht mit der Bedrohung, die von Überwachung ausgeht, auseinanderzusetzen. Vielleicht hat die Person, die das sagt, sogar subjektiv gefühlt nichts zu verbergen – dafür aber alle möglichen anderen Menschen, die ebenfalls in dieser Gesellschaft leben. Unter diesen sind auch Funktionsträger. In dem Augenblick, in dem irgendeine staatliche Stelle, etwa ein Geheimdienst, oder auch ein Wirtschaftsunternehmen, alles über eine Person weiß, wird diese Person erpressbar. Rechtsstaatliche Sicherungen können ohne Weiteres ausgeschaltet werden. Privatsphäre und persönliche Geheimnisse sind also für das Funktionieren eines Rechtsstaates elementar. Auch deshalb ist der eingangs genannte Satz grundfalsch.

Nutzt es denn überhaupt etwas? Schützt uns die Überwachung wirklich vor Terrorismus und Kriminalität? Sie haben ja bereits beim Thema Vorratsdatenspeicherung Zweifel geäußert…

Ich habe ganz erhebliche Zweifel daran, dass die überbordenden Überwachungsmaßnahmen, die wir haben, zu irgendeinem Schutz führen. In Frankreich, wo es seit 2006 die Vorratsdatenspeicherung gibt, konnten sich zahlreiche Attentate ereignen. Ich würde mir wünschen, dass wir zu einer evidenzbasierten Sicherheitspolitik zurückkehren. Eine, die zunächst fragt, was eine Maßnahme genau bringt, und die Maßnahmen regelmäßig evaluiert – mit der Bereitschaft, diese auch zurückzunehmen, wenn die Evaluierung negativ ausfällt.

Bietet die schiere Menge der gespeicherten Daten nicht auch einen gewissen Schutz, ganz einfach, weil die Sicherheitsbehörden personell überfordert sind? Warum sollte sich z.B. die NSA ausgerechnet dafür interessieren, welche Pizza oder welchen Billigflieger ich im Internet bestelle?

Ich glaube nicht, dass die großen Datenmengen selbst Sicherheit bieten. Wir dürfen nicht vergessen, dass Geheimdienste wie die NSA oder auch der GCHQ mit extrem starken Analysewerkzeugen arbeiten, die ohne Weiteres riesige Datenmengen bewältigen können. Wenn sich ein Geheimdienst für die Daten einer bestimmten Person interessiert, kann er diese ohne Weiteres aus dem Datenmeer herausfischen. Dass Missbrauchspotential ist enorm. NSA-Mitarbeiter nutzten etwa ihre Überwachungsmöglichkeiten, um privat ihre Partner auszuspähen oder um Menschen dahingehend zu manipulieren, mit ihnen eine Beziehung einzugehen. Man darf auch nicht vergessen, dass speziell in den USA sehr viel von der Überwachungstätigkeit an Privatunternehmen outgesourct wird. Edward Snowden selbst war ja Mitarbeiter eines sogenannten Private Contractors. Man kann davon ausgehen, dass die Kontrolle bei privaten Unternehmen wesentlich weniger scharf und engmaschig ist als bei rein staatlichen Institutionen. Gleiches gilt für die Grundrechtsbindung. Den besten Schutz vor Datenmissbrauch bietet immer noch das Prinzip der Datensparsamkeit. Daten, die gar nicht erst erzeugt und gespeichert werden, können auch nicht missbraucht werden.

Welche Rolle spielt die EU beim Ausbau des Überwachungsstaates? Schützt Sie eher die Bürgerrechte oder begünstigen ihre bürgerfernen Strukturen und das Fehlen einer europäischen Öffentlichkeit autoritäre Gesetze?

Teils, teils. Es ist sicherlich so, dass speziell im Bereich der Sicherheitsgesetze die Innenminister über den Ministerrat und auch die Sicherheitspolitiker über die entsprechenden Gremien im Europaparlament einen relativ starken Einfluss haben. Es gibt wenige Institutionen, die aus bürgerrechtlicher Sicht dagegenhalten. Wir haben zwar den europäischen Datenschutzbeauftragten und die Artikel-29-Gruppe, aber deren Stellungnahmen fallen im Verhältnis zu der Vielzahl an Stellungsnahmen, die von der anderen Seite kommen, kaum ins Gewicht. Insofern kann man sagen, dass die Innenminister im Ministerrat starke Treiber der europäischen Entwicklung zu mehr Überwachung sind.

Auf der anderen Seite haben wir mit dem Europäischen Gerichtshof (EuGH) eine Instanz, die im Vergleich zum Bundesverfassungsgericht noch deutlich stärker bürgerrechtlich orientiert urteilt. Ich erinnere an die bahnbrechenden Urteile des EuGH zur Vorratsdatenspeicherung und auch an das Gutachten zur „Passenger Name Record“-Vereinbarung mit Kanada. In beiden Fällen hat der EuGH ganz klar gesagt: Anlasslose massenhafte Datenspeicherungen sind unverhältnismäßig. Das Bundesverfassungsgericht hat sich bisher nicht getraut, in dieser Klarheit zu urteilen, gerade was anlasslose Speicherungen angeht. Insofern müssen die unterschiedlichen Institutionen auf europäischer Ebene unterschiedlich beurteilt werden. Die EU generell als Treiber des Überwachungsstaats zu definieren, ist schlicht falsch.

Eine bedeutende Errungenschaft freier, aufgeklärter Gesellschaften ist die Meinungsfreiheit. Viele betrachten das kürzlich verabschiedete Netzwerkdurchsetzungsgesetz (NetzDG), das sogenannte „Hate Speech“ im Internet bekämpfen soll, als ernste Bedrohung dieses vielleicht wichtigsten Bürgerrechts. Ihre Organisation war bei der Gründung eines zivilgesellschaftlichen Bündnisses gegen das NetzDG federführend. Was sind Ihre Kritikpunkte?

Mit dem NetzDG soll versucht werden, bestimmte strafbare Inhalte schneller von sozialen Netzwerken zu löschen. Das Gesetz definiert eine Frist, innerhalb derer diese Netzwerke eine juristische Prüfung durchführen müssen. Eine juristische Prüfung, die sehr komplex sein kann. Bei der Volksverhetzung zum Beispiel haben selbst Richter und Staatsanwälte sehr häufig ihre Probleme, den Tatbestand sauber zu subsumieren. Versierte Juristen kommen zu sehr unterschiedlichen Einschätzungen. Solche Prüfungen sollen jetzt von den sozialen Netzwerken innerhalb von 24 Stunden, maximal aber innerhalb von sieben Tagen, durchgeführt werden. Wenn sie das nicht tun, drohen ihnen Bußgelder bis zu 50 Millionen Euro.

In dieser Situation, in der man sozusagen die sozialen Netzwerke zum Ankläger, Richter und Vollstrecker in eigener Sache macht, wird ein Anreiz gesetzt, Inhalte im Zweifel zu löschen. Das ist der zentrale Kritikpunkt: Im Zweifel wird man gegen die Meinungsfreiheit entscheiden. Dabei bedeutet Meinungsfreiheit auch, dass unbequeme Meinungen, die an die Grenze des Sagbaren gehen, toleriert werden müssen. Genau das ist das Wesen einer offenen Gesellschaft. Ein weiterer Kritikpunkt ist, dass das NetzDG eine Privatisierung der Rechtsprechung vorantreibt. Man verlagert ein stückweit Aufgaben, die eigentlich originär Aufgaben der Justiz sind, auf Privatunternehmen, die dafür sachlich nicht qualifiziert sind und die dafür in der Regel auch nicht die notwendigen Kapazitäten haben. Für Nutzerinnen und Nutzer führt das zu spürbaren Verschlechterungen, etwa im Hinblick auf den Rechtsschutz.

Außerdem hilft diese Löschung von Inhalten nicht wirklich gegen das eigentliche Problem. Was man hier versucht zu bekämpfen, ist eigentlich ein soziales Phänomen. Bestimmte Menschen in Deutschland fühlen sich offenbar wieder berechtigt, verhetzende oder beleidigende Inhalte öffentlich zu äußern. Die Antwort darauf soll jetzt sein, die Symptome zuzudecken, und das war's. Wir sollten uns lieber fragen, wie wir die Ursachen sinnvoll bekämpfen können. Insbesondere stellt sich für mich hier die Frage nach einer effektiven Strafverfolgung. Denn beim NetzDG geht es nicht einfach um unschöne Kommentare oder Ähnliches. Es geht um strafbare Handlungen. Dann müssen die sozialen Netzwerke natürlich auch verpflichtet sein, diese strafbaren Handlungen der Staatsanwaltschaft zu melden, die dann sachlich und personell in der Lage sein muss, diese Anzeigen auch zu verfolgen. Nur dann, wenn auf eine strafbare Handlung in möglichst kurzer Zeit eine Sanktion folgt, wird das auch einen verhaltensändernden Effekt haben. Einfach nur irgendwelche Kommentare zu löschen, weil sie angeblich strafbare Inhalte sind, was nie ein Richter sondern nur ein Privatunternehmen beurteilt hat, wird dieses Problem nicht lösen.

Kann man nicht über viele sicherheits- und netzpolitische Maßnahmen, die aktuell diskutiert werden oder neu eingeführt wurden, sagen, dass sie technokratische Maßnahmen sind, die die tieferen Ursachen gesellschaftlicher Probleme ignorieren?

Das ist, glaube ich, tatsächlich sehr häufig so. Ich kann auch nur mutmaßen, was dahintersteht. Der Ansatz, zunächst einmal alles zu speichern und dann Algorithmen darüber laufen zu lassen, um zu schauen, ob sich irgendwelche Muster oder verdächtigen Anhaltspunkte finden, ist vielleicht auch deswegen für viele Politiker so charmant, weil er verhältnismäßig ressourcenschonend ist. Algorithmen sind praktisch unendlich skalierbar, ohne dass es einen großen Mehraufwand kostet. Echte Beamte muss ich hingegen bezahlen, ich muss für sie Altersvorsorgeaufwendungen machen usw. Das mag vielleicht ein Grund sein, warum viele Politiker technische Lösungen reizvoll finden.

Zum anderen mag dahinter auch der Glaube stehen, dass Computer im Grunde fehlerfrei und unbeeinflusst von Emotionen arbeiten. Auch das ist natürlich vollkommen falsch, denn es gibt keinen vorurteilsfreien Algorithmus. Jeder Algorithmus beinhaltet Wertentscheidungen und Überlegungen, die seine Programmierer ihm bewusst oder unbewusst eingepflanzt haben.

Ich würde aber noch weiter gehen und sagen, dass hinter vielen dieser Überwachungsmaßnahmen eine mehr oder minder kybernetische Sicht der Gesellschaft steht. Man begreift die Gesellschaft als eine Summe von Regelungskreisläufen, die man nur gut genug kennen muss, um vorausberechnen zu können, was als nächstes passieren wird. Das verspricht natürlich die ultimative Sicherheit, und vielleicht auch die ultimativen wirtschaftlichen Gewinnmöglichkeiten, die Freiheit bleibt dabei aber vollkommen auf der Strecke. Die Freiheit, jederzeit entscheiden zu können „jetzt verhalte ich mich anders“, ist jedoch der Kern menschlichen Seins. Daher halte ich eine kybernetische Betrachtungsweise der Gesellschaft für grundweg unvereinbar mit einer wirklich freiheitlichen Gesellschaft.

Initiativen wie „Freiheit statt Angst“ oder der anfängliche Erfolg der Piratenpartei zeigen, dass es in Deutschland durchaus Bewusstsein für die Themen Überwachung und digitale Bürgerrechte gibt. Andererseits regt sich kaum Widerstand gegen aktuelle Gesetzesvorhaben. Keine der größeren Parteien nimmt sich des Themas konsequent an. Wie können wir das bürgerliche Engagement stärken?

Ich weiß gar nicht, ob das bürgerrechtliche Engagement so wahnsinnig schwach ist. Protestbewegungen verliefen eigentlich immer schon in Wellen. Es gab immer wieder Hochzeiten und Zeiten, in denen der

Protest weniger laut war oder weniger gut wahrgenommen wurde. Das heißt aber keineswegs, dass momentan kein bürgerrechtliches oder zivilgesellschaftliches Engagement stattfindet. Auch unsere Organisation arbeitet sehr viel im Hintergrund. Wir versuchen, in Einzelgesprächen, öffentlichen Anhörungen oder Diskussionsrunden unsere Argumente anzubringen – Dinge, die vielleicht von der breiten Öffentlichkeit nicht so wahrgenommen werden. Das ist anders als bei Demonstrationen, über die groß berichtet wird.

Man muss auch immer damit rechnen, dass sich zivilgesellschaftliches Engagement sehr plötzlich und anlassbezogen aus dem Nichts entwickelt – denken wir beispielsweise an die ACTA-Proteste. Innerhalb kürzester Zeit ist eine europaweite Bewegung entstanden, wo Leute zu Hunderttausenden auf die Straße gegangen sind und gesagt haben: „Wir wollen das nicht.“ Letztlich ist ACTA genau daran gescheitert. Es ist wichtig, dass es Organisationen wie unsere gibt, die permanent an diesen Themenfeldern arbeiten und die Argumente für den Augenblick parat haben, in dem sich ein solcher Schub entwickelt. Gleichwohl würde ich mir natürlich auch wünschen, dass sich mehr Menschen aktiv für diese Themen interessieren und öffentlich mehr darüber gesprochen wird.

Was kann ich als Bürger konkret tun, um meine Privatsphäre im Netz zu schützen?

Es gibt eine ganze Menge Dinge, die man tun kann. Ich finde, eine der einfachsten Maßnahmen ist, nicht einfach mit seiner normalen IP-Adresse ins Netz zu gehen, sondern einen VPN-Dienst zu nutzen oder einen Tor-Browser. Es gibt eine ganze Reihe von Plug-Ins, die man beim Browsen benutzen kann, um seine Privatsphäre besser zu schützen. Beispielsweise gibt es Plug-Ins, die Java Script blocken oder das Tracking verhindern. Dann ist natürlich sehr wichtig, bei der Kommunikation – egal ob über Messenger oder E-Mail – darauf zu achten, dass man Verschlüsselungstechnologie benutzt. Je mehr Menschen ihre Mails verschlüsseln, desto aufwändiger wird es letztlich für staatliche Stellen, eine flächendeckende Überwachung zu organisieren. Das sind Maßnahmen, die für jedermann relativ einfach umsetzbar sind und die insgesamt schon einen großen Zugewinn an Sicherheit bedeuten.

Vielen Dank für das Gespräch, Herr Tripp.

Dieser Artikel ist zuerst in der Novo-Printausgabe Nr. 124 – 2/2017 erschienen. Kaufen Sie ein Einzelheft oder werden Sie Abonnent, um die Herausgabe eines wegweisenden Zeitschriftenprojekts zu sichern.

Das Interview führte Novo-Redakteur Kolja Zydatiss.