



Georg Markus Kainz ist Datenschützer. Manche würden auch sagen Nerd, einige nennen ihn Verschwörungstheoretiker. Er hat ein Programm, es geht um das Banalste der Welt: den Schutz der Privatsphäre und damit einhergehend, unsere Individualität und unsere Freiheit. Am ehesten ist er aber ein Robin Hood des digitalen Zeitalters, ein Verteidiger unserer digitalen Privatsphäre. Mit zwei Seiten voller Fragen sitzen wir vor ihm. Der Mann, der uns mit seiner runden, rotbraunen Brille gegenüber sitzt, braucht aber keine Fragen.

EIN MONOLOG VON GEORG MARKUS KAINZ, FREI ÜBERTRAGEN IN SCHRIFT UND MIT EIGENEN GEDANKEN ERGÄNZT DURCH MAX BRUSTBAUER UND DANIELA KRENN.

»Wir wissen gar nicht, welche Daten über uns gesammelt werden und wir spüren keine unmittelbaren Auswirkungen – also zumindest derzeit und wir wissen schon gar nicht, was mit den Daten passiert. Wir reden von Big Data, alles landet im Datenmülleimer. Jeder von uns ist eine Ameise, einer von acht Milliarden Menschen auf dieser Welt. Man denkt sich, wer soll schon Interesse an mir haben, außerdem bin ich ja nur einer von acht Milliarden, also unsichtbar. Die Sache ist nur, wenn jemand Interesse hat, wenn einer die Lupe anlegt und dich finden will, dann wird er es und er wird alles über dich finden, alles über dich wissen. In welches Netz habe ich mich eingeloggt? Wie lange telefoniere ich und mit wem? Was sind meine Vorlieben? Wie lebe ich? Wer sind meine Kontakte?

BMW baut Sensoren in die Autos. Nach einer EU-Richtlinie müssen in Zukunft alle Autos eCall haben – sollte man einen Unfall haben, würde automatisch die Rettung alarmiert werden. Ja, in Norwegen, wo stundenlang keine Hilfe weit und breit ist, macht das Sinn. Aber in Wien? In einer Großstadt? Da ist das kein Argument. Also, brauche ich das wirklich immer aktiv? Und will ich immer, dass BMW weiß, wo ich gerade hinfahre? All diese Daten sind mir ständig zuzuschreiben. Die Industrie sagt, dass diese Daten nicht personenbezogen sind. Klingt gut für uns, aber somit unterliegen sie nicht dem Datenschutzgesetz und sind frei verfügbar und frei veräußerbar. BMW kann sie verarbeiten, verkaufen und weitergeben. Das muss gar nicht die Polizei sein, die mich sucht. Jeder, der sich auskennt, kann mich finden.«

Dieser Gedanke fühlt sich gerade unwirklich an, während wir hier in dem kleinen Dachboden unter dem kulturbegegneten Dach des Museumsquartiers sitzen. Eine graue Treppe

hat uns hier herauf geführt, hinter eine Stahlgittertür mit magnetischem Sicherheitsschloss. Hier hat die Non-Profit-Organisation quintessenz ihr Hauptquartier. Die Stahlgittersicherheitstür, eigentlich überflüssig, weil die Wände reichen nicht bis an die Decke.

»Morgen lese ich dann mal die Facebook-Sicherheitsbestimmungen, ab morgen logge ich mich überall aus.«

»Es ist schon vorgekommen, dass bei uns im Büro eingebrochen wurde. Computer wurden geklaut. Die Polizei kam, DNA-Spuren von einem Kabel zu nehmen. Aber da ist dann nichts raus gekommen. Natürlich, denn die Daten liegen dann eben in einem Archiv. Weiter passiert nichts, aber sie sind generiert worden. Hauptsache, Daten sammeln. Speicherung kostet ja nichts mehr. Sollen sie machen, von mir aus, wie jetzt mit den Bodycams, die Polizisten tragen.¹ Nur sollen dann auch beide Seiten auf dieses Filmmaterial zugreifen können. Das ist aber nicht der Fall. Die Daten liegen bei der Polizei und sie werten sie aus und wir wissen nicht, nach welchen Kriterien sie diese auswerten. Beim WKR-Ball vor zwei Jahren hat die Polizei alle Videodaten der Nacht ausgewertet. Sie wollen wissen, wer da Aufstand betreibt. Wer war dabei, ist wichtiger, als wer hat etwas angestellt. Wer könnte das Potenzial haben für etwas, das passiert.«

Wir haben uns um den großen Tisch in der Mitte ausgebreitet, der fast den ganzen Raum füllt. Unsere MacBooks vor der Nase, die alle unsere Daten haben. Wie wir eigentlich schon wissen, wunderbar ignorieren, aber nicht sollten, aber tun, der ewige Kreislauf

des Prokrastinierens. »Morgen lese ich dann mal die Facebook-Sicherheitsbestimmungen, ab morgen logge ich mich überall aus.«

Diese Meinung: »Solange ich nichts mache, sollen Facebook, Google und Co. ruhig alles wissen dürfen«, haben wir zwar nicht, handeln aber so.

»Was mir viel mehr Angst macht, ist, was unsere Innenminister und Geheimdienste machen. Das Profiling.² Nach jedem Attentat – es muss ja nicht gleich ein Attentat sein, aber nach jedem Vorfall – wird nach Profilen derer gescannt, die verdächtig sind und da scheinen dann natürlich alle mit ähnlichem Profil auf. Und plötzlich ist man auf einmal verdächtig! Etwas banal und herunter gebrochen gesagt, der Attentäter hat zum Frühstück Nutella gegessen und eine Cola getrunken. Dann werden alle gesucht, die das auch so tun. Sehr vereinfacht gesagt. Breivik³ zum

Fußnoten

[1] Nach einer Testphase, die laut Polizeisprecher positiv verlief, wurde Mitte April vom Innenministerium entschieden, ab Ende 2017 bzw. spätestens Anfang 2018 alle Polizisten mit Bodycams auszustatten. Diese sollen im Notfall für eine bessere Nachverfolgung des Tätergangs sorgen. Die Kamera nimmt auch den Ton auf. Die Filme sind später vor Gericht als Beweismittel zulässig. Die Polizisten müssen im Vorhinein ankündigen, wenn sie die Kamera verwenden, sie ist also nicht durchgehend eingeschaltet. Datenschützer kritisieren das: Wenn die Kamera eigentlich polizeiliches Fehlverhalten genauso dokumentieren können sollte, dürften Polizisten sie nicht selbstständig und selbstbestimmt ein- und ausschalten können.

[2] Profiling: laut Definition heißt Profiling das Erstellen, Aktualisieren und Verwenden von Profildaten, die gesammelt und ausgewertet werden. Bei Kriminalfällen wird üblicherweise ein Täterprofil erstellt. Mit diesen Profilen wird versucht, potenzielle Täter ausfindig zu machen. Aber es muss nicht immer kriminell sein. Auch Google oder Amazon erstellen Käufer- und Suchprofile, um weitere Käufe vorzuschlagen bzw. die Suche einzuzugrenzen je nach Profil.

[3] Breivik: Anders Behring Breivik beging 2011 einen Autobombenanschlag in Oslo und Schusswechsel auf der Insel Utøya; zwei Anschläge, bei denen 77 Menschen ums Leben kamen. Er wurde gerichtlich für zurechnungsfähig erklärt und zu 21 Jahren Haft und anschließender Sicherheitsverwahrung verurteilt – die höchste Strafe in Norwegen. Nach der Tat wurde von einigen Politikern verlangt, mehr Kontrolle im Internet zu schaffen und eine Vorratsdatenspeicherung einzuführen.

Beispiel hat damals kurz vor dem Attentat aufgehört, Social-Media-Kanäle zu benutzen. Bin ich jetzt verdächtig, wenn ich das auch auf einmal mache? Der Batman-Attentäter von Aurora 2012 war zum Beispiel acht Stunden online pro Tag. Sind also alle heavy user auch verdächtig? Wieviele Stunden pro Tag sind also unverdächtig? Wir wissen nicht, was die Kriterien sind. Was die Kriterien heute sind und schon gar nicht, was sie morgen sind.«

Außerdem ist es ja nicht so, dass gescheite Täter sich nicht ebenfalls auskennen, Profiling kennen und dementsprechend ihr Handeln anpassen.

»Was man verstehen sollte: das Bewusstsein für Datenschutz in Österreich, in Deutschland und in vielen Ländern Europas entstand aufgrund unserer Geschichte. Nach der Machtübernahme, nach dem Anschluss oder nach der Invasion wurden die bereits vorhandenen Daten der Staaten missbraucht. Die hatten alle Daten der Volkszählung und damit Informationen zur Religion und zur Rasse. Dadurch wussten die alles. Oder in einigen Ländern wegen der Kirchensteuer, alle die Steuerprivilegien hatten, standen auf einer Liste. Die, die man gesucht hat, konnte man sich dann da rauspicken und finden. Damals schon.«

Die Novemberpogrome als Zeichen dafür, was Daten über dich verraten. Wofür sie verwendet, wie sie interpretiert werden können. Bei dem Gedanken fühlt man sich wie ein Verschwörungstheoretiker. Malt man gerade im Kopf zu schwarz?

»Weshalb bekomme ich diesen Kredit nicht, die Versicherung, die Wohnung? Wieso werde ich nicht zum Vorstellungsgespräch eingeladen?«

»Die Vorratsdatenspeicherung ist eigentlich anonym, wenn man das Telefonverzeichnis nicht hat. Das mag stimmen, es ist aber völlig egal. Unersere abstruse Vorstellung ist, dass wir glauben – weil wir es ununterbrochen hören – je mehr Daten gespeichert werden, desto mehr gehe ich in der anonymen Masse unter und bin nicht mehr zuordenbar. Das genaue Gegenteil ist jedoch der Fall, die Wahrscheinlichkeit erkennbar zu werden, steigt je mehr Daten vorhanden sind. Der großen, großen Mehrheit fehlt die Phantasie, wofür die Daten verwendet werden können, wie sie interpretiert werden können – und mit Mehrheit meine ich weit über 90 Prozent.

Wir sind Teil der Mehrheit, selbstverständlich. Wir wissen, dass wir ständig Daten eingeben, es ist so einfach. Wir haben Facebook. Wir loggen uns ins öffentliche WLAN ein. Wir verwenden die diversen Google-Dienste. Wir telefonieren. Wir verwenden die Facebook-Log-In-Möglichkeit bei neuen Applikationen. Es ist eben praktisch.

»Wir haben das Recht, unsere Privatsphäre zu schützen. Es geht nicht darum, bei etwas erwischt zu werden. Aber allen, die denken, ‚ich habe ja nichts zu verbergen‘, sei gesagt, dass es einfach darum geht, dass wir uns das Recht behalten müssen, unsere eigenen Gedanken und Geheimnisse zu haben. Ich denke da immer an die amerikanische Polizei, die bei einer Verhaftung sagt: ‚Alles kann und wird gegen Sie verwendet.‘ Mit unseren Daten ist es das selbe, irgendwann können und werden

sie gegen uns verwendet werden. Wir glauben dieser vorgespielten Anonymität leider zu sehr.«

Diese Anonymität scheint uns manchmal gut zu sein, aber schon jetzt wissen wir doch, jeder anonyme Hassposter kann gefunden werden. Was auch gut ist. Wo fängt Privatsphäre an, wo hört Anonymität auf?

»Ich kann mich noch an die Urzeiten des Internets erinnern. Da gab es die Netiquette, so etwas wie Tischmanieren. Wer in den Chaträumen einmal daneben gehaut hat, dem haben die anderen Teilnehmer auf die Finger geklopft. Aber heute? Heute nehmen wir den Leuten die Möglichkeit zu diskutieren. Zum Beispiel bei der Flüchtlingsdebatte, da gab es immer nur ganz eindeutige Meinungen online, die nicht diskutiert werden durften. Es fehlte die Diversität. Ich spreche aber nicht von den Hasstiraden, die man heute vorfindet. Dagegen muss man vorgehen, jeder einzelne von uns muss Diskussionskultur einfordern. Aber alles andere, das sollte ich frei sagen dürfen, ohne das alles auf ewig auf mich zurückfallen kann. Doch wir diskutieren nicht mehr, wir kriminalisieren. Wir bemerken durch diese geglaubte Anonymität zwei Dinge, einerseits, dass wir keine Netiquette mehr kennen. Wir sagen online Sätze mit einer Leichtigkeit, für die wir uns in der realen Welt in Grund und Boden schämen würden. Andererseits üben wir bereits Selbstzensur. Heute sagen Eltern ihren Kindern, ‚Pass ja auf, was du online tust, das könnte einmal später beruflich ein Nachteil sein.‘ Aber wenn ich mit 15, 16 Jahren keinen Blödsinn mehr machen darf? Da Beginnt die Zensur im eigenen Kopf.«

Haben wir uns das auch gedacht, mit 15 oder 16 Jahren? Eher nicht. Aber wir hatten damals auch kein Facebook.

Oder Smartphones. Nein, keine Gute-alte-Zeit-Nostalgie, sondern eine Feststellung. Wir durften Scheiß machen, von dem heute zum Glück keiner weiß. Wie schaffen das die heute 16-jährigen? Werden die jemals das Gefühl kennen, unbeschwert Scheiße bauen zu können?

»Wir brauchen wieder Zivilcourage. Wenn man in der Straßenbahn angemotzt wird, reagiert in der Regel irgendwer. Online gibt es das nicht – und wenn, dann nur im negativen Sinn, dass man sich gegenseitig aufhust. Menschen reagieren spontan. Wenn ich nicht laut schreie, dann falle ich nicht auf. Also am Besten gleich von Anfang an laut sein. Es gibt Politiker, die gehen mit Postings an den Rand der Legalität. Da setzen sie anstatt eines Punktes ein Fragezeichen und schon sind sie nicht mehr strafbar. Problematisch ist, dass wir mit dem Posting eines 14-jährigen Mädchens gleich umgehen, wie mit dem Posting eines Armin Wolf. Hinter dem steht im Falle einer Klage ein staatlicher Sender mit Rechtsanwälten und eine ganze Redaktion. Die 14-Jährige sitzt allein zu Hause.«

Wie sind nicht nur Teil der unwissenden Mehrheit, wir sind auch noch unmündig. Eigentlich können wir keine vernünftigen Entscheidungen in der digitalen Welt treffen. Wer soll das für uns machen?

»Jetzt wird verlangt, dass Facebook Aussagen seiner User selbstständig zensurieren soll. Aber eine amerikanische Privatfirma, die Zensur betreibt? Nein danke. Ja, wir müssen natürlich dafür gerade stehen, was wir geschrieben haben. Aber einiges sollte definitiv aus dem Strafrecht heraus genommen werden. Man sollte tadeln und sich gegenseitig wieder zu gutem Verhalten ermahnen. Eingriffe erwarte ich mir

bei Fake News, aber da reagiert Facebook überhaupt nicht. Als Betroffener sollte Facebook mich schützen. Machen sie aber nicht.«

Bei so vielen Möglichkeiten, einen digitalen Fußabdruck zu hinterlassen, wie kommuniziert Georg Markus Kainz?

»Ich verwende Telegram und Signal, Messenger, die end-to-end-verschlüsselt sind. Meine eigenen Spuren in der digitalen Welt habe ich mir schon öfter angeschaut. Manchmal kann man ja auch nicht beeinflussen, was alles ins Internet kommt. Das Interview zum Beispiel heute. Oder meine Email, meine Telefonnummer, natürlich gibt es das von mir. Ich benutze aber gern verschiedene Browser für unterschiedliche Aufgaben oder verwende bestimmte Programme, die das unkontrollierte Nachladen von Webseiten, was bei der meisten Werbung im Hintergrund geschieht, blocken. Mein Internetbrowser, und damit die Webseiten die ich sehe, sieht sicher ganz anders aus, als eurer. Das Problem ist ja, dass wir nicht mehr frei surfen können – früher oder später. Man lebt in der Google-Blase, wie es so schön heißt. Ich bekomme vorgefilterte Informationen. Google baut das System nach Gesichtspunkten der Gewinnmaximierung auf. Was völlig ok ist, denn Google ist ein Unternehmen, das Geld verdienen will. Aber ich als Person, ich muss die Entscheidung haben. Ich muss das Filtern auch abstellen können. Ich muss sagen dürfen, Filter heute ja, morgen nein. So einfach wäre das. Google glaubt heute zu wissen, was mich morgen interessiert. Das kann aber kein Logarithmus.«

Google entscheidet, welche Interessen wir aufbauen, Google als Mama und Papa. Zeig mir deine Wohnung und ich sage dir, wer du bist, dieser Spruch gilt bei einem Algorithmus leider nicht.

»Es gibt die Big Five, die alles von dir wissen. Microsoft mit Windows, Google mit Android und den Google-Diensten, Apple mit iOS, sowie Facebook und Amazon. Die Daten, die sie sammeln, sind natürlich alle nicht böse. Ich kann mich noch erinnern, früher an die alten Zugtickets. Die hat der Schaffner bei der Kontrolle mit einem Locher gestanzt. Einfach ein Loch, das die Karte entwertet, denkt man sich. Aber das war es nicht. Er hat das Loch einmal oben rechts, einmal mittig und so weiter gemacht. Je nachdem: junge Frauen wurden oben gestanzt, Männer mittig – so in der Richtung. Der Grund war ganz einfach: Damit man die Karten nicht untereinander weitergeben kann. Damit nicht ein Mann die Karte an eine Frau weitergeben kann. Den Kunden war das System dahinter aber gar nicht bewusst – und am Ende des Tages hatte man im Bahnhofsmistkübel die gesammelten Informationen über die Fahrgäste. Heute leben wir in einer Zeitwende. Wenn wir nicht aufpassen, verlieren wir ohne es zu bemerken alle Freiheiten. Weil wir zu 100 Prozent gläsern werden, weil wir dadurch manipulierbar werden, weil wir uns nicht mehr frei äußern können. Warum ist die Wahlkabine geschlossen? Weil ich etwas zu verbergen habe? Nein, weil wir das Recht dazu haben in einer Demokratie. Wenn Leute sich beobachtet fühlen, beeinflusst dieses Gefühl bereits ihr Verhalten. Wir sind wie die Zugkunden, aber bei uns geht es nicht mehr um ein Loch in einer Fahrkarte, bei uns geht es um alle unsere Gedanken und unsere Privatsphäre.«

Wenn jetzt alles eh schon online ist. Wenn man alles nachschauen kann. Müssen Schüler eigentlich noch lernen, was wir gelernt haben?

»Es ist völlig unverständlich, dass Schüler in Zukunft keine Handschrift mehr

lernen sollen. Tippen am Laptop ist etwas anderes, als Wörter zu schreiben. Dass Schülern heute gesagt wird, man muss nur mehr wissen, wo man etwas nachschaut. So ein Blödsinn. Man muss schon lernen. Man muss nicht mehr wissen, was ein Gulden wert war, aber man muss wissen, was ein Gulden war. Man muss verknüpfen können, man muss zuordnen können.«

Du musst es nicht wissen, du musst nur wissen, wo es steht. Was wird uns mit diesem Satz eingeredet?

»Wenn ich es nicht reflektieren kann, nicht mit eigenem Wissen vergleichen kann, dann kann ich nie skeptisch werden, weil ich alles glauben muss.«

»Wir müssen einfach darauf schauen, dass unsere Daten nicht das Geschäftsmodell des 21. Jahrhunderts werden. Von Daten, die meinen persönlichen Heimatbereich verlassen: eine Zahnbürste, die per App mittrackt, wie lange ich putze und wann; ein Auto, das aufzeichnet, wohin ich mich bewege; ein persönlicher Assistent der zuhause mitlauscht; ein Fernseher, der in den Wohnbereich hineinschaut. Man verliert einfach die Hoheit über persönliche und private Dinge. Und nicht nur das, auch die Hoheit über den privaten Besitz. Bei Kindle gab es da ein Ereignis, ironischerweise sogar mit George Orwells Buch 1984. Amazon verkaufte das E-book, aber bald kam heraus, dass es Diskussionen gab, ob sie überhaupt die Rechte dafür hatten. Also löschten sie das Buch von allen Kindles. Zack, weg war es. Obwohl ich es gekauft habe. Das muss man sich einmal vorstellen, das ging früher nicht. Was ich besessen habe, war meines. Dieses Recht verlieren wir immer mehr. Betriebssysteme, Programme und Bücher und Filme nur zum Verleih. Nicht mehr kaufen. Was jetzt nicht unbedingt schlimm ist, aber einfach eine Entwicklung, die man be-

wusst auch bedenken sollte, wo das hinführt.«

Wenn wir nichts mehr besitzen, entspricht das nicht auch irgendwie dem Geist der Sharing-Gesellschaft? Nur – selbst nichts zu besitzen bedeutet nicht, dass Dinge im Allgemeinbesitz sind. Sie sind im Besitz derer, die sie einem zur Verfügung stellen. Sie entscheiden, wann und wie lange man etwas zur Verfügung hat.

»Wir brauchen neue Spielregeln. Im Hintergrund passieren Entscheidungen, die nicht mehr begründet werden, nicht mehr begründet werden müssen. Profiling zum Beispiel. Weshalb bekomme ich diesen Kredit nicht, die Versicherung, die Wohnung? Wieso werde ich nicht zum Vorstellungsgespräch eingeladen? Wie die Entscheidungen dazu im Hintergrund laufen, das bekommen wir nicht mit. Das ist keine Zukunftsvision. Das gibt es alles schon. Leute, die sich fragen, warum sie keinen Job bekommen, aber hundert Bewerbungen ausgeschrieben haben. Leute, die keine Wohnung bekommen. Man merkt die gläserne Decke gar nicht, an die man stößt. Was wir dabei brauchen, ist Waffengleichheit. Wir müssen wissen, wann Profiling erfolgt. Warum ich bei der Bank keinen Kredit bekomme, den Job nicht bekomme. Das wäre Umgang mit der digitalen Welt auf Augenhöhe.«

Wir werden nervös. Wie oft wurden wir schon einem Profiling unterzogen? Was steht alles auf unseren Facebookprofilen? Sollten wir etwas löschen, ändern, und was können wir eigentlich wirklich für immer löschen? Tausend Gedanken.

»Wir werden gerade in die Kinderrolle zurück gedrängt, Papa Google kümmert sich um uns. Solange wir nicht auffällig werden, können wir rela-

tiv gut leben. Das stimmt aber nicht. Überwachung passiert heute unmerkelt. Wir sollten deshalb, ich kann es nicht oft genug betonen, über die Regeln bestimmen, wie die Interpretation dieser Daten passiert. Wir und nicht die Konzerne. Zum Beispiel bei der Wahl in den USA. Facebook wusste das Wahlergebnis bevor die Wahl stattfand. Sie mussten dazu nicht einmal direkt fragen, ‚Wen wählst du?‘, sie haben Daten ausgewertet über den Musikgeschmack der Facebookuser. Auf Österreich umgelegt wäre das in etwa so: Van der Bellen-Wähler hören eher Conchita Wurst. Hofer-Wähler hören eher Gabalier. Mit dieser These schaue ich mir die Likes der Österreicherinnen und Österreicher an. Das ist jetzt simpel formuliert, aber bei Big Data, wenn ich nur genug Daten zum vergleichen habe, hast du mit einer Wahrscheinlichkeit von 70–80 Prozent ein passendes Ergebnis. Ohne direkt fragen zu müssen. So werden Daten verglichen und interpretiert. Und damit sind wir wieder beim Problem von Big Data: das Individuum fällt weg. Helmut Schmidt hätte als starker Raucher statistisch gesehen nicht alt werden dürfen. Aber er ist es. Versichert mich also eine Versicherung irgendwann nicht mehr, weil ich nicht in die Statistik passe? Wir dürfen einfach nicht alles auf eine breite Masse auslegen und dabei das Individuum vergessen. Wo bleibt der Solidaritätsgedanke? Und diese Spielregeln müssen von der Gesellschaft aufgestellt werden. Denn eine Versicherung will natürlich Geld verdienen und das kann man ihnen auch nicht vorwerfen. Aber eine freie, offene Gesellschaft funktioniert nur mit Solidarität.«

Schaffen wir das als Gesellschaft? Einheitliche Spielregeln oder überhaupt Spielregeln für uns zu definieren? Haben wir das je geschafft? Wir stellen uns das schwierig vor und eigentlich

brummt uns irgendwie der Kopf bei all dem Nachdenken über Daten und den Umgang mit ihnen.

»Es gibt zwei Wege, wie das mit unserer Welt weitergehen könnte. Entweder wir als Gesellschaft tun nichts: Dann wird es eine kleine Gruppe geben, die sich aus möglichem Datenmissbrauch freikaufen können. Außerdem noch eine kleine technische Elite, die weiß, wie man Daten verhindert. Dann gibt es die nächstgrößere Gruppe an Europäern und Amerikanern, denen es gut geht, auch wenn sie nichts mitbekommen von der Überwachung. Und dann gibt es die restlichen sieben Milliarden auf der Welt, die sich überhaupt nicht mehr wehren können und auf deren Rücken wir leben. Dann gibt es noch die Möglichkeit zwei: Die Gesellschaft definiert Spielregeln und erhebt den Missbrauch nicht zur Regel. Ja, es werden dann weiter Daten entstehen, und nein, sie dürfen nicht missbraucht werden. Die Daten dürfen nur mit Zustimmung erhoben werden. Dann hat die Gesellschaft und jeder einzelne darin wieder die Hoheit über den Schatten, den er hinterlässt. Aber ganz ehrlich, ich denke, zur Zeit entwickelt sich unsere Gesellschaft zur Variante eins. Leider.«

Langsam verschwindet die Lust auf das Internet. Können wir nicht wieder Brieftauben schicken? Und Bücher lesen?

»Ich bemerke einen Trend, dass, egal ob digitale oder sonstige Firma, Unternehmen, gerade bei uns, wieder vermehrt auf ethische Werte und Glaubhaftigkeit setzen. Darauf sollten wir auch bestehen, dass Firmen datentechnisch ethisch handeln und Respekt vor ihren Kunden haben. Das Spiel ist also noch nicht verloren. Wir haben immer noch eine Chance auf Variante zwei.«

DATENSCHUTZGESETZ IN ÖSTERREICH

In Österreich ist der Datenschutz auf dreierlei Arten geregelt:

[1.] Das Grundrecht auf Datenschutz, der grundlegende menschenrechtliche Anspruch auf Datenschutz, der in Österreich im Verfassungsrang verankert ist: §1 Datenschutzgesetz 2000 (DSG). Er besagt, dass jeder das Recht auf Geheimhaltung seiner persönlichen Daten hat. Ausnahmen sind allerdings solche Daten, die nicht eindeutig auf die Person zurück zu führen sind (ZB ??????) oder allgemein verfügbare Daten (ZB ?????).

[2.] Die Charta der europäischen Grundrechte, Artikel 8. Der Artikel regelt in mehreren Unterpunkten, dass jede Person, erstens das Recht auf Privatsphäre hat, zweites das Recht hat, zu erfahren, welche Daten über ihn/sie erhoben werden, woher sie kommen und wofür sie verwendet werden. Generell dürfen Daten nur für festgelegte Zwecke und mit Zustimmung erhoben werden. (ZB ??????) Kontrolliert werden diese Vorschriften von einer unabhängigen Stelle, in Österreich von der Datenschutzkommission DSK.

[3.] Die Menschenrechte, Artikel 12: Jeder hat Anspruch auf rechtlichen Schutz gegen Eingriffe in sein Privatleben, seine Wohnung und Familie und seinen Schriftverkehr. (Der Datenschutz geht aber über die allgemeinen Menschenrechte hinaus, z.B. das Recht am eigenen Bild.)

Im Grunde ist der Datenschutz einfach zu fassen: Es geht um die Transparenz, wer welche Information für welche Zwecke sammelt. Die Polizei oder sonstige staatliche Organisationen dürfen nur unter ganz bestimmten lebenswichtigen Voraussetzungen den Datenschutz gewisser Personen missachten. Trotzdem gilt der Grundsatz der Transparenz.

Jeder hat auch Eigenverantwortung über seinen Umgang mit Daten, allerdings sollten Anbieter einen gewissen Mindeststandard gewährleisten und sie sollten transparent machen, wofür sie die Daten verwenden.

Das Datenschutzgesetz gibt es in Österreich seit 1978, ein Zeitpunkt, wo man weder in Österreich noch international große Erfahrungen in diesem Rechtsbereich hatte. Ähnliche Gesetze gab es nur in Schweden, den USA, der BRD, Frankreich, Kanada, Dänemark, Neuseeland und Norwegen. Aufgrund der neuen Erfahrungen mit dem Gesetz ist es im Laufe der Jahre ständig zu Anpassungen und Erweiterungen gekommen. Insgesamt gab es vier große Novellen zum Datenschutz seither. Der Datenschutzrat setzt sich zusammen aus Mitgliedern des Parlaments, Vertretern der Arbeiter- und Wirtschaftskammer, zwei Vertretern der Ländern, sowie Gemeindebundes und Städtebundes. Ein Vertreter des Bundes wird vom Bundeskanzler ernannt.