Festrede
anlässlich 50 Jahre Landesdatenschutzgesetz in Rheinland-Pfalz
von Adrian Lobe

Mainz, den 7. Februar 2024

Sehr geehrte Damen und Herren,
sehr geehrte Frau Vize-Landtagspräsidentin,
sehr geehrte Frau Ministerpräsidentin,
sehr geehrter Herr Prof. Dr. Kugelmann,

„was sind das für Menschen, die Datenschützer werden wollen?“, fragte der streitbare Kolumnist und Journalist Jan Fleischhauer unter der Überschrift „Plage unserer Zeit“ 2021 in einem Blogbeitrag. Der Autor hatte gerade, mitten in der Corona-Pandemie, die vielkritisierte Luca-App auf sein Smartphone geladen und damit, ganz unkompliziert, in einer Eisdiele eingecheckt.[1] Datenschützer, grantelte Fleischhauer, seien die, die anderen das Leben schwermachten. „Verstehen Sie die deutsche Obsession mit dem Datenschutz?“, fragte der Kolumnist weiter. „Ich nicht. Wir setzen uns ungerührt nackt mit einem Dutzend Fremder in die Hotelsauna. Aber wenn das Google-Auto um die Ecke biegt, um unseren leeren Vorgarten zu fotografieren, rufen wir panisch nach sofortiger Verpixelung.“

Man möchte dem kulturgeschichtlich ansonsten so beflissenen Kollegen an dieser Stelle zurufen, dass er hier womöglich einen Kategorienfehler zwischen Privatsphäre und Intimität begeht – letztere wird ja eher über die Scham reguliert – und bislang keine Fälle von Bäderbetrieben bekannt sind, in denen persönliche Daten von Saunagängern abgefragt wurden. Trotzdem spricht es Bände, wenn Datenschutz als – Zitat Fleischhauer – „biblische Plage“ desavouiert wird. Wie konnte es so weit kommen?

Erlauben Sie mir an dieser Stelle einen kurzen Rückblick: Als der rheinland-pfälzische Landtag 1974, vor genau 50 Jahren, nach Hessen und Schweden als weltweit drittes Land ein eigenes Datenschutzgesetz beschloss, leistete das Parlament Pionierarbeit. Das digitale Zeitalter schien damals noch in weiter Ferne: Die Bürger tuckerten in analogen Blechkisten über die Straßen, tippten Bewerbungsschreiben in Schreibmaschinen und bestellten Kleidung im Quelle-Katalog. Als Deutschland in diesem Jahr Fußball-Weltmeister wurde, kamen keine Videoassistenten oder sonstigen Überwachungssysteme zum Einsatz. Und doch gab es damals schon Formen elektronischer Datenverarbeitung: In Hessen, wo das gesamte Grundbuch auf EDV umgestellt worden war und IBM die Einheitswerte bebauter Grundstücke errechnete, wurden Daten von 5,5

[1] https://janfleischhauer.de/tag/datenschutz/, letzter Abruf: 1.2.2024.

Millionen Bürgern von Computern erfasst.[2] Schon damals gab es die Sorge vor einem Überwachungsstaat, der sensible Daten an Auskunfteien, Banken oder Geheimdienste weiterreichen könnte.

Heute sind die technologischen Voraussetzungen ganz andere: Milliarden Menschen laufen mit Taschenspionen namens Smartphone herum, High-Tech-Geräten, die mit Überwachungstechnologie vollgestopft sind: Kamera, Mikrofon, Bewegungssensor, Fingerabdrucksensor usw. Ein Tatortkoffer im Miniaturformat. Was vormals im Werkzeugkasten von Agenten war, gehört heute zur Grundausstattung des digitalen Bürgers. Das Smartphone ist Portemonnaie, Ausweisdokument und Postfach in einem. Ohne Handy kann man schon gar kein Ticket mehr im Zug buchen und immer seltener die Speisekarte in einem Restaurant erhalten. Der analoge Bürger muss draußen bleiben.

Mobile Endgeräte sind zu Ersatzbehausungen geworden, in denen man digitalisierte Gegenstände speichert, die man früher in analoger Form in Schränken oder Schubladen aufbewahrte: Bücher, Musik, Fotos, Tagebücher, Notizen, Kontoauszüge. Früher wusste niemand, was man in seinem Tagebuch notierte oder welche Bücher man las. Heute liest die intelligente „Auto-Korrektur" das Geschriebene mit und ergänzt automatisch Sätze. Amazon weiß, bis zu welcher Seite wir ein Buch lesen, Netflix, wann wir auf die Pausetaste drücken und ob wir bei Sexszenen zurückspulen, Spotify, ob wir Balladen hören und traurig sind. **Der Überwachungskapitalismus hat die Wände unserer Wohnungen eingerissen, und er schickt sich an, in unsere Köpfe einzudringen.** So ist es Elon Musk mit seinem Start-up Neuralink kürzlich gelungen, einen Chip in das Gehirn eines Menschen zu implantieren.[3] Damit soll es möglich sein, Handys zu bedienen und irgendwann vielleicht auch Gedanken zu lesen.[4] Was einst nur in den kühnsten Science-Fiction-Szenarien denkbar war, könnte bald Wirklichkeit werden: der Mensch als programmierbares Wesen.

Gleichwohl: Im Jahr 11 nach der NSA-Affäre begegnen die meisten Bürger der Massenüberwachung mit dem biedermeierlichen Reflex „Ich habe nichts zu verbergen" – und spinnen sich in den Kokon ihrer Filterblasen ein. Personalisierte Werbung? Egal. Hauptsache, Netflix läuft! Ich nenne das: die Gleichzeitigkeit der Gleichgültigkeit. Dass dieser Rückzug ins vermeintlich Private die Privatsphäre weiter erodiert, weil sich die Konsumgewohnheiten in den vier Wänden viel besser kontrollieren lassen, ist dabei eine bittere Ironie.

Es wird gerne übersehen, dass es sich beim Datenschutz um ein elementares Freiheitsrecht handelt. Dazu lohnt ein Blick in die USA: Dort haben Polizeibehörden über dubiose Datenbroker Nutzerdaten von Menstruations-Apps sowie Standortdaten von App-Nutzern verkauft, die eine Abtreibungsklinik besucht haben. Frauen in Bundesstaaten, in denen Abtreibung illegal ist, wurden damit kriminalisiert.[5] Die US-Geheimdienste kaufen sogar Daten von muslimischen Gebets-Apps auf, um potenzielle Terrorverdächtige aufzuspüren.[6] Und auch hierzulande hacken Bundespolizei und Nachrichtendienste beim Verdacht auf Straftaten IT-Geräte und spielen eine

[2] https://www.spiegel.de/politik/edv-im-odenwald-a-0746bb53-0002-0001-0000-000043176393, letzter Abruf: 1.2.2024.
[3] https://www.welt.de/wirtschaft/video249815360/Hirn-Computer-Schnittstelle-Musks-Neuralink-implantiert-ersten-Chip-in-menschliches-Gehirn.html, letzter Abruf: 1.2.2024.
[4] https://futurezone.at/science/neuralink-elon-musk-gehirn-chip-menschen-implantiert-eingesetzt-aktivitaet-patient-steuern-computer/402759823, letzter Abruf: 1.2.2024.
[5] https://www.wired.com/story/data-brokers-tracking-abortion-clinics-security-news/, letzter Abruf: 1.2.2024.
[6] https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x, letzter Abruf: 1.2.2024.

Schadsoftware (sogenannte „Staatstrojaner“) auf, die das Mitlesen von Messengernachrichten ermöglicht.

Infolge der Anschläge vom 11. September ergingen weltweit zahlreiche Anti-Terror- und Sicherheitsgesetze, die der Exekutive umfassende Befugnisse einräumten und der Massenüberwachung Tür und Tor öffneten. Strafverfolgungsbehörden erfassen automatisch Kennzeichen von Kraftfahrzeugen oder Fluggastdaten von Bürgern. Beim BKA gingen allein im Jahr 2022 Daten von 121 Millionen Fluggästen ein.[7] Die Datensätze enthalten neben Namen, Anschrift und Telefonnummer unter anderem Informationen über Reiseroute, gebuchten Sitzplatz, Zahlungsart sowie Essenwünsche.[8] Der Staat weiß also, ob der Passagier auf Sitzplatz 17 D seinen Flug über Booking.com gebucht hat und sein Veggie-Gericht mit Kreditkarte bezahlt.[9]

Das hätten sich die Aktivisten, die einst gegen die Volkszählung auf die Straße gingen, im Traum nicht vorstellen können. Genauso wenig die Tatsache, dass man beim Restaurantbesuch zu Beginn der Corona-Pandemie Name und Adresse auf einen Zettel kritzeln und der Wirt Kontaktlisten erstellen musste, die dann sogar die Polizei zur Aufklärung von Straftaten abtelefonierte. **Wir sind schlafwandlerisch in eine Überwachungsgesellschaft geschlittert.** Google weiß, wo sich seine zweieinhalb Milliarden Android-Nutzer auf der Welt aufhalten und die Nachfrage nach Immobilienkrediten steigt. Amazon sieht durch die Kameraaugen seines Staubsaugroboters Roomba, ob jemand noch Platz für eine Kommode in der Wohnung hat oder Spielzeuge auf dem Boden liegen. Und Apple fühlt am Puls von 100 Millionen Apple-Watch-Trägern auf der Welt.

Es nimmt wenig Wunder, dass dieser Datenschatz Begehrlichkeiten bei staatlichen Behörden weckt. So hat Amazon in den USA ohne Zustimmung der Nutzer Daten seiner Türklingel Ring sowie seines Netzwerklautsprechers Echo an die Polizei zur Aufklärung von Straftaten herausgegeben.[10] Auch die Google-Suchhistorie wird von der Polizei abgefragt. Bei aller Übergriffigkeit des Staates gab es unter Überwachungsgegnern immer eine leise Hoffnung: Dass Polizei und Geheimdienste das Material am Ende gar nicht sichten können. Interne Dokumente der NSA, die der Whistleblower Edward Snowden enthüllte, belegen: Die US-Geheimdienste ersticken in Daten.[11]

Die Fortschritte auf dem Gebiet der Künstlichen Intelligenz scheinen diese Hoffnung zu zerstören. Machine-Learning-Algorithmen, die mit riesigen Datenmengen trainiert werden, können in den Datensätzen verdächtige Muster und Verbindungen erkennen. Man gibt einfach den Suchbefehl „Weißer Lieferwagen“ ein, schon exekutiert der Objekterkennungsalgorithmus die computerisierte Rasterfahndung. Ein Konzern wie Amazon muss nicht mehr Vertragsarbeiter in Indien oder Costa Rica beschäftigen, um von Alexa aufgezeichnete Audioschnipsel von

[7] https://netzpolitik.org/2023/424-millionen-datensaetze-deutlicher-anstieg-bei-der-fluggastdatenspeicherung/, letzter Abruf: 1.2.2024.
[8] https://www.bfdi.bund.de/DE/Buerger/Inhalte/Polizei-Strafjustiz/National/PNR.html, letzter Abruf: 1.2.2024.
[9] https://fps-law.de/de/fps-blog/was-ist-eigentlich-das-flugdag-und-warum-weiss-das-bundeskriminalamt-bka-was-ich-auf, letzter Abruf: 1.2.2024.
[10] https://arstechnica.com/tech-policy/2022/07/amazon-finally-admits-giving-cops-ring-doorbell-data-without-user-consent/, letzter Abruf: 30.1.2024.
[11] https://www.washingtonpost.com/blogs/compost/wp/2013/10/15/nsa-complains-that-it-has-access-to-too-much-data-actually/, letzter Abruf: 1.2.2024.

Drogendeals oder Sex zu transkribieren – das erledigt einfach die Maschine. **KI könnte sich als ein Katalysator der Kontrollgesellschaft entpuppen.**

Den Treibstoff für diese Überwachungsmaschinerie liefern die Bürger selbst: Mit Dashcams, smarten Türkameras und Drohnen weben sie das immer engmaschigere Netz an Überwachung aktiv mit. Doch das, was heute an Überwachungstechnologie im Einsatz ist, könnte nur ein Kinderspiel gegenüber dem sein, was noch kommen wird. Augmented-Reality-Brillen, an denen Tech-Konzerne wie Apple, Alphabet, Meta und andere tüfteln, könnten Pupillenbewegungen wie Tastatureingaben und Mausbewegungen tracken: Bleibt man im Supermarkt am Süßigkeitenregal stehen und scannt die Schokoladentafeln? Nimmt man das Preisschild oder den Nutri-Score unter die Lupe? Ist man ein besonders preissensibler oder gesundheitsbewusster Kunde? Dann könnte einem der Händler Rabatte aufs Handy spielen. Irgendwann kann man mithilfe von Gesichtserkennung vielleicht auch Personen augmentieren und ihren Beziehungsstatus oder Kreditwürdigkeit im Brillenglas anzeigen lassen. Ist der Gegenüber in der U-Bahn eine gute Partie? Die KI weiß mehr. Im Metaversum, das Mark Zuckerberg und Co. zum 3D-Nachfolger des Internets ausbauen wollen, könnte die biometrische Überwachung auf eine neue Stufe gehoben werden: Augenbewegungen, Herzschlag, Gang – sensible biometrische Daten können mit Virtual-Reality-Hardware erfasst werden. Meta hat bereits Patente für passgenaue Anzeigen im Metaversum angemeldet.[12]

Den Datenschutz, der ja entgegen seines Wortlauts nicht Daten, sondern die dahinter stehenden Individuen schützen soll, stellen diese Entwicklungen vor große Herausforderungen. Wenn Daten das neue Öl sind, dann bedeutet ihr Schutz eine künstliche Verknappung eines wertvollen Rohstoffs. Datenschutz gilt vielen als Innovationsbremse. Diese Haltung zeigt sich jetzt in der KI-Debatte, aber sie trat auch schon in der Corona-Krise offen zutage. Da sprach Tübingens Oberbürgermeister Boris Palmer von einem „Datenschutz-Kult“ und forderte, die Corona-Warn-App „scharf zu schalten“. Mehr Smartphone-Daten gleich weniger Lockdowns und mehr Freiheit, so die Rechnung des studierten Mathematikers. Muss man den Datenschutz opfern, um Leben zu retten?

So mancher Politiker schaute in der Pandemie neidisch auf die Corona-Apps in Singapur oder Südkorea, wo der Staat ohne Rücksichtnahme auf den Datenschutz Infektionsketten nachverfolgen und Quarantäne anordnen konnte. Datenschutz darf keine Leben kosten, heißt es immer wieder aus Medizinerkreisen, wenn es um die Digitalisierung des Gesundheitswesens geht.[13] Sei es, weil Patientendaten unvollständig an den Arzt übermittelt werden. Oder Gesundheitsdaten für die Medizinforschung fehlen.[14] Die Ethikrat-Vorsitzende Alena Buyx forderte mehr „Datensolidarität“.[15] Wie aber könnte eine digitale Solidargemeinschaft aussehen? Wer muss hier einen Beitrag leisten? Ist man unsolidarisch, wenn man seine Daten nicht teilt? Wie kann das Spannungsverhältnis zwischen Daten- und Gesundheitsschutz austariert werden? Diese Fragen hängen ganz wesentlich davon ab, wo die Technik entwickelt wird. **Es geht längst nicht mehr darum, wer die schnellsten Computer oder leistungsfähigsten Chips baut, sondern darum, wer die Spielregeln für die digitale Gesellschaft schreibt.** Europa befindet in einem Systemwettbewerb mit den USA und China. Während der laissez-faire-Kapitalismus kalifornischer Spielart Tech-Giganten wie Google, Amazon oder Facebook hervorgebracht hat,

[12] https://www.protocol.com/bulletins/metas-tracking-you, letzter Abruf: 1.2.2024.
[13] https://www.aerztezeitung.de/Politik/Datenschutz-darf-keine-Leben-kosten-407161.html, letzter Abruf: 1.2.2024.
[14] https://www.faz.net/asv/digitale-medizin-2020/datenschutz-kann-leben-kosten-16949351.html, letzter Abruf: 1.2.2024.
[15] https://www.telepolis.de/features/Gesundheit-Krankenkassen-und-die-Ethik-Daten-oder-Leben-9193984.html, letzter Abruf: 1.2.2024.

sind im Staatskapitalismus Chinas Player wie Tencent emporgeschossen. Hierzulande kaum bekannte Super-Apps wie WeChat, die Bezahl-, Kommunikation- und Shopping-Funktionen bündeln, lassen selbst Mark Zuckerberg und Elon Musk vor Neid erblassen.

Das Reich der Mitte ist längst nicht mehr die verlängerte Werkbank des Westens, sondern beansprucht Technologieführerschaft auf vielen Gebieten. Der Autobauer BYD hat Tesla als größten Elektroautobauer abgelöst, und die beliebteste App der Welt kommt nicht aus den USA, sondern aus China: Tiktok. Eine Milliarde Nutzer auf der ganzen Welt wischen über ein digitales Daumenkino, dessen Programm der Black-Box-Algorithmus einer Pekinger Firma vorgibt. Was mit den Nutzerdaten passiert, bleibt ein Geheimnis.

Entgegen der Annahme, wonach Autokratien Innovationen tendenziell unterdrücken, finden sich in diesem Regimetyp besonders günstige Bedingungen für KI-Forschung vor[16]: Unternehmen können ohne die Fesseln eines strikten Datenschutzes massenhaft Daten sammeln, die für das Training der KI-Modelle benötigt werden. Überwachungstechnologie made in China, darunter Gesichtserkennung und Smart-City-Zubehör, kommt mittlerweile in über 80 Ländern auf der Welt zum Einsatz. Im kommenden Jahr wird China nach Schätzungen der International Data Corporation (IDC) erstmals mehr Daten als die USA produzieren. Entpuppt sich der Datenschutz also doch als Wettbewerbsnachteil?

Europa wird niemals so viele Daten wie die USA oder China produzieren können, doch es gibt vielversprechende Ansätze, wie sich dem Gebot der Datensparsamkeit folgend der informationelle Rohstoff substituieren lässt. Start-ups basteln an KI-Systemen, die mit synthetischen, sprich computergenerierten Daten trainiert werden. Der Vorteil: Man verletzt dabei keine Rechter Dritter, wenn man Personen oder Hintergründe am Computer designt. Beim Training von Fahrcomputern füllen synthetische Daten bereits die Lücke von selten auftretenden Verkehrsereignissen, für die es wenig Trainingsmaterial gibt. Synthetische Daten könnten also eine schonendere Alternative zum Raubbau des Data Minings sein. **Ich möchte gar die kühne These wagen, dass sich Datenschutz langfristig als Standortvorteil erweisen könnte. Denn: Er könnte die Innovation zu schlankeren und energiesparsameren KI-Modellen fördert. Daten- und Energiesparsamkeit sind zwei Seiten derselben Medaille.**

Angesichts des enormen Ressourcenverbrauchs von Rechenzentren und KI-Systemen – das Training des Sprachmodells GPT-3 benötigte allein 700.000 Liter Wasser[17] – müssen wir als Gesellschaft auch über so etwas wie eine **Ökologie der Information** diskutieren: einen verantwortungsvollen und maßvollen Medienkonsum, der a priori fragt, ob man jedes Essen von Spundekäs in Social Media teilen und das World Wide Web weiter mit Foodporn fluten muss. Vor allem, so scheint mir, braucht es ein Bewusstsein dafür, dass Datenschutz keine Gängelei ist, sondern eine freiheitseröffnende Funktion hat. Wenn das gelingt, werden wir den Datenschutz auch noch in 50 Jahren feiern.

[16] Vgl. Monika Schnitzer, „Chinas Vorteil in der KI-Entwicklung", FAZ vom 8.1.2024.

[17] https://www.heise.de/news/Wasserbilanz-von-KI-Modellen-Halber-Liter-Wasser-pro-Unterhaltung-mit-ChatGPT-8973680.html, letzter Abruf: 1.2.2024.