www.jusletter-it.eu

Sandra Husi-Stämpfli

Leitgedanken: Sind wir die Totengräber unserer informationellen Selbstbestimmung und staatlichen digitalen Souveränität?

Je schneller die digitale Transformation voranschreitet, je «praktischer» die Errungenschaften der Digitalisierung für unseren Alltag erscheinen, umso weniger Beachtung wird den Risiken geschenkt, die die Kehrseite der digitalen Transformation ausmachen: Die Digitalisierung unseres Alltags geht mit einer Intensivierung der «Überwachung» einher – freilich nicht der staatlichen Überwachung, sondern der selbstauferlegten durch vermeintlich attraktive Gadgets. Ein ähnliches Phänomen lässt sich zudem im staatlichen Kontext feststellen: Auch dort wird in der Diskussion, ob die öffentliche Verwaltung den Gang in eine (public) Cloud wagen sollte, vor allem auf die Vorteile einer solchen Lösung verwiesen. Die Autorin beleuchtet in ihren Leitgedanken dieses Phänomen, ermutigt zu einer kritische(re)n Auseinandersetzung mit der Thematik und appelliert an eine bewusstere Wahrnehmung unserer informationellen Selbstbestimmung.

Beitragsart: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz

Zitiervorschlag: Sandra Husi-Stämpfli, Leitgedanken: Sind wir die Totengräber unserer informationellen Selbstbestimmung und staatlichen digitalen Souveränität?, in: Jusletter IT 26. April 2022

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

[1] Der Motor der digitalen Transformation läuft ungebremst auf Hochtouren.[1] Eine Gesellschaft, die nicht in weiten Teilen «digitalisiert» funktioniert bzw. von der Digitalisierung profitiert, ist für viele nicht mehr vorstellbar: An unser «smart home» haben wir uns schon längst gewöhnt – es ist ja auch wirklich praktisch, dass uns der Kühlschrank daran erinnert, dass unser Lieblingsjoghurt nicht mehr vorrätig ist – noch besser, wenn die Bestellung beim Detailhändler direkt ausgelöst wird. Der Digitalisierung unserer Wohnung wird in der Literatur bzw. in der Presse mittlerweile nur noch wenig (kritische) Aufmerksamkeit geschenkt. Dass unsere Fahrzeuge im Falle einer Panne keinen Mechaniker mehr benötigen, sondern (zugegebenermassen etwas überspitzt dargestellt) einen IT-Spezialisten, und dass der Datenhunger der Automobilhersteller nicht zu verachten ist, wird ebenso stillschweigend hingenommen. Und genauso selten findet sich eine vertiefte Auseinandersetzung mit dem Umstand, dass wir uns via Smartphone(-Apps) und den dazugehörigen Gadgets (z.B. die Smartwatch oder den Fitnesstracker) je länger je stärker zu gläsernen Menschen machen.

[2] Nahezu täglich erreichen uns hingegen begeisterte Nachrichten über neue Entwicklungen, die nicht nur unser individuelles Leben, sondern unsere Gesellschaft in all ihren Aspekten «vereinfachen» oder «verbessern» sollen. Um nur zwei Beispiele des vergangenen Jahres zu nennen:

[3] Astro[2], der neue «Haushaltsroboter» von Amazon, soll bei alltäglichen Aufgaben in der Wohnung helfen und diese überwachen. Astro patrouilliert autonom im Haus bzw. in der Wohnung, und informiert seine Besitzerinnen und Besitzer via Periskop-Kamera und Mikrofon in Echtzeit über das Geschehen in den verschiedenen Räumen. Er verfügt über einen integrierten Rauchmelder, erkennt Geräusche wie bspw. zerbrechendes Glas und kann dann die Besitzerinnen und Besitzer per Telefon alarmieren. Die fahrende Alarmanlage kann aber noch mehr: Gemäss Amazon können auch pflegebedürftige Angehörige aus der Ferne «betreut» (bzw. überwacht) werden: Erinnerungen und Alarme können programmiert, Angehörige oder eine Notfallzentrale via Alexa alarmiert werden.

[4] So praktisch sich dies alles anhört: Damit Astro seine «Dienstleistungen» erbringen kann, muss er Überwachung betreiben. Viel Überwachung, und zwar nicht nur von der leeren Wohnung, sondern eben auch von den Menschen, die sich in dieser Wohnung aufhalten. Muss mein Partner wirklich jederzeit in der Lage sein zu überprüfen, in welchem Zimmer ich mich gerade aufhalte und was ich mache? Muss ich als berufstätige Mutter wirklich in der Lage sein zu wissen, was meine halbwüchsigen Kinder am Nachmittag allein zuhause anstellen? Wo bleibt das Vertrauen in die Mitbewohnerinnen und -bewohner, wo bleibt der Respekt vor der Privatsphäre? Und damit nicht genug: Muss Amazon dies alles wissen? Oder der Nachbar, der Astro allenfalls via ungesichertem Wifi ebenfalls mitnutzen kann? Sind die Vorteile eines «Hausroboters» wirklich so gewichtig, als dass wir bereit sein sollten, eines unserer Grundrechte – unsere informationelle Selbstbestimmung – derart auszuhöhlen?

[5] Ein vermeintlich ebenso praktisches Gadget wurde ebenfalls im Jahr 2021 aus dem Hause Apple präsentiert: Die AirTags seien «die einfache Art, deine Sachen im Blick zu halten»[3]. Wer also regelmässig seine Schlüssel sucht, kann diese nun via Smartphone orten. Praktisch – aber braucht man das wirklich? Und wie gross ist das Missbrauchsrisiko angesichts dessen, dass die

1 Die Autorin gibt ihre persönliche Meinung wieder.

2 https://www.netzwoche.ch/news/2021-09-29/amazons-neuer-roboter-kontrolliert-den-haushalt. Diese und die nachfolgenden Internet-Quellen wurden letztmals am 31.03.2022 kontrolliert.

3 https://www.apple.com/chde/airtag/.

AirTags ebenso leicht im Rucksack eines Kindes oder am Auto einer fremden Person angebracht werden können? In der breiten Presse aufgegriffen wurde diese Thematik erst – und auch nur kurz –, als sich einzelne Personen meldeten, die mittels AirTags verfolgt wurden[4]. Verschiedene Fach-Foren griffen das Thema etwas früher auf[5]. Apple gelobte Besserung und passte die Sicherheitseinstellungen und Notifikationen im Falle eines Stalking-Versuchs an – gleichwohl bleiben grosse Vorbehalte: Die Notifikationen funktionieren bei älteren iOS-Versionen oder anderen Smartphone-Modellen nicht und die Lautsprecher der AirTags können entfernt werden, so dass keine akustischen Hinweise auf ein mögliches Stalking abgegeben werden können[6]. Kommt hinzu, dass es ganz grundsätzlich mehr als stossend ist, wenn auf derart einfache Art und Weise Personen «gestalkt» werden können – egal, wie schnell eine Notifikation erfolgt (die ursprüngliche Einstellung für die Notifikation lag bei drei (!) Tagen)[7].

[6] Diese zwei Beispiele machen deutlich: Noch immer fehlt es in unserer Gesellschaft weitgehend[8] an einem kritischen Umgang mit der digitalen Transformation. Nach wie vor werden neue Gadgets und Möglichkeiten euphorisch aufgenommen und ein bewusster Umgang mit den eigenen Personendaten lässt sich vermissen. Mit geradezu naivem Idealismus werden die vermeintlichen Erleichterungen in den Alltag integriert: Dass diese «Erleichterungen» mit einer Beschränkung oder gar gänzlichen Aufgabe der Privatsphäre bezahlt werden, scheint den wenigsten Konsumentinnen und Konsumenten bewusst zu sein – oder sie wollen es schlicht nicht wahrhaben, denn «sie haben ja nichts zu verbergen» und willigen entsprechend grosszügig in die Nutzungsbestimmungen (und damit verbunden in die Datenbearbeitungsklauseln) ein.

[7] Es erstaunt daher – bedauerlicherweise – nicht, dass auch die politischen Diskussionen die «Digitalisierung» zwar aufgreifen, die weitreichenden und gewichtigen Fragen der staatlichen digitalen Souveränität aber nur selten[9] oder erst dann diskutiert werden, wenn einzelne Weichen schon gestellt wurden: Erst, *nachdem* im Rahmen einer WTO-Ausschreibung[10] zur Beschaffung kommerzieller Cloud-Services (das Volumen der Ausschreibung betrug über CHF 100 Mio.) Hersteller aus den USA, Europa und China, nicht aber aus der Schweiz, gewonnen hatten, regte sich in der Politik Widerstand. Der Umstand, dass der Schweizer Staat künftig zumindest einen Teil seiner Daten auf Infrastrukturen der Unternehmen Alibaba, Amazon, IBM, Microsoft oder Oracle betreiben könnte, führte immerhin zu verschiedenen parlamentarischen Vorstössen, im Rahmen derer sich die jeweiligen Unterzeichnenden besorgt über die Vergabe zeigten und vom Bundesrat

4 Eine Auflistung verschiedenster Vorfälle – die nicht nur Stalking, sondern auch versuchte Diebstähle umfassen – findet sich bspw. auf https://www.macwelt.de/news/Frau-entdeckt-Stalker-Airtag-unter-dem-Auto-Kotfluegel-11157298.html.

5 https://www.washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/.

6 Ausführlich dazu bspw. Mirko Dölle, Apple AirTags: Schutz vor Stalking und Überwachung völlig unzureichend, heise online, 18.6.2021, abrufbar unter https://www.heise.de/news/Apple-AirTags-Schutz-vor-Stalking-und-Ueberwachung-voellig-unzureichend-6069686.html.

7 Mirko Dölle (Fn. 6).

8 Weitestgehend, weil das Schweizer Stimmvolk am 7. März 2021 das Bundesgesetz über elektronische Identifizierungsdienste deutlich mit 64.4 % der Stimmenden abgelehnt hat. Als zentraler Punkt wurde von den Gegnern des Gesetzes immer wieder betont, dass die Herausgabe von Identitätsausweisen in staatlicher Verantwortung bleiben müsse und unter demokratische Kontrolle gehöre. Die Datenhoheit und somit die Daten selbst sollten vollumfänglich in staatlicher Verantwortung bleiben, und dem Datenschutz und der Selbstbestimmung müsse ein grosses Gewicht beigemessen werden, siehe dazu unter vielen https://www.e-id-referendum.ch/.

9 Positiv hervorzuheben die Motion 19.3884 Derder, «Eine Strategie für die digitale Souveränität der Schweiz», abrufbar unter https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193884.

10 https://www.it-beschaffung.ch/it/1202937/20007-608-public-clouds-bund.

verschiedene Erklärungen forderten[11]. Weitaus sinn- und verantwortungsvoller wäre es freilich gewesen, früher eine umfassende Diskussion über den Einsatz von Cloud-Services zu führen und sich zu vergegenwärtigen, welche Werte für die Schweiz und ihre Bürgerinnen und Bürger mit dem jeweiligen Entscheid auf dem Spiel stehen.

[8] Aber auch hier zeigt sich das weiter oben geschilderte Phänomen: Die technischen Vorteile der Cloud werden in den Vordergrund gerückt, mögliche unerwünschte Nebeneffekte wie die Abhängigkeit von privaten Anbietern, die sich allenfalls sogar im Ausland befinden oder das Risiko von Zugriffen ausländischer Behörden auf die in der ausländischen Cloud gelagerten Daten werden ausgeblendet. Wieso auch immer, denn vernachlässigbar sind diese Risiken zweifelsohne nicht, auch wenn beispielsweise die genannte Vergabe der «Public Cloud» durch die Bundesverwaltung an ausländische Anbieter damit beschönigt wird, dass ja keine «heiklen» Daten in diesen Cloud-Infrastrukturen bearbeitet werden sollen: Auch der Zugriff auf staatliche Geoinformationsdaten (bzw. deren Integrität!) sollte nicht vom Goodwill eines fremden Staates und vertraglichen Vereinbarungen abhängig gemacht werden. Aber damit nicht genug: Ob es wirklich wünschenswert ist, die gesamte Office-Infrastruktur einer öffentlichen Verwaltung über die Cloud eines privaten Anbieters (im Ausland) laufen zu lassen, ist, wenn auch «praktisch», mehr als fraglich: Während eine Baubewilligung tatsächlich «harmlos» sein mag (und trotzdem Personendaten enthält!), dürfte eine Einreisesperre in der Regel derart heikle (polizeiliche) Informationen enthalten, dass eine on premise-Bearbeitung weitaus sicherer erscheinen würde.

[9] Wohlgemerkt: Die digitale Transformation unserer Gesellschaft soll weder aufgehalten, noch rückgängig gemacht werden; diese Forderung wäre weder gesellschaftspolitisch noch wirtschaftlich vertretbar. Unverzichtbar ist aber, dass wir den für unsere demokratische Gesellschaft essentiellen Konzepten der informationellen Selbstbestimmung und der staatlichen digitalen Souveränität endlich wieder die gebotene Beachtung schenken und uns nicht von den neuen Möglichkeiten der Digitalisierung blenden lassen. Andernfalls werden wir als Bürgerinnen und Bürgern zu Totengräbern unserer eigenen Privatsphäre, unserer informationellen Selbstbestimmung – ein Verlust, den wir vielleicht nicht unmittelbar an Leib und Leben spüren mögen, wohl aber über kurz oder lang im Rahmen unserer politischen Deliberation, den uns zur Verfügung gestellten Informationen (Stichwort «Filter Bubble») und in der Wahrnehmung unserer Person in der Gesellschaft. Und als Staat, als politische Gesellschaft, müssen wir uns ebenso ernsthaft damit auseinandersetzen, wie wir unsere staatliche Souveränität in der digitalisierten Welt definieren und leben wollen. Auch hier dürfen die Vorteile der digitalen Transformation nicht dazu führen, dass wir uns unüberlegt in (politische und wirtschaftliche) Abhängigkeiten begeben und die Verantwortung für die Daten unserer Bürgerinnen und Bürger aus der Hand geben.

[10] Das neue Datenschutzrecht trägt diesen Gedanken Rechnung, indem es einerseits die Rechte der betroffenen Personen stärkt, andererseits aber auch die für Datenbearbeitungen verantwortlichen Personen bedeutender in die Pflicht nimmt. Es ist an uns allen, diese Bestimmungen umzusetzen und «zu leben», indem wir als Individuen unsere informationelle Selbstbestimmung und als Gesellschaft unsere politische Verantwortung hinsichtlich dem Umgang mit Personendaten in der digitalen Transformation wahrnehmen.

11 Siehe bspw. Interpellation 21.4136 Marti, «Cloud-Dienste von Microsoft», abrufbar unter https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20214163, oder aber Interpellation 21.4019 Andrey «Vergabe von Public-Cloud-Diensten an amerikanische und chinesische Unternehmen», abrufbar unter https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20214019.

[11] Einen Beitrag zu diesem dringend erforderlichen Diskurs rund um die informationelle Selbstbestimmung im digitalisierten Zeitalter und das neue Datenschutzgesetz leisten die Autorinnen und Autoren dieses Jusletters IT: Reto Fanger setzt sich damit auseinander, welche Auswirkungen das revidierte DSG auf Cloudanbieter in der Schweiz hat, während Peter Andres und die Autorin dieses Beitrags den Bogen noch einmal weiter spannen und die Frage analysieren, ob mit dem Gang in die Cloud nicht auch die staatliche digitale Souveränität in Bedrängnis gerät. Die nachfolgenden Autoren verlassen dann die Cloud, die von ihnen aufgegriffenen Themen sind aber nicht weniger brennend und zeigen auf, dass auch mit dem neuen DSG noch längst nicht alle Fragen rund um den Datenschutz im IT-Kontext geklärt sind: Marcel Griesinger und Daniel Seiler befassen sich mit der Cybersicherheit und den Anforderungen, die das neue DSG an die Datensicherheit stellt, und Ursula Uttinger beleuchtet die neuen Möglichkeiten der Überwachung im Kontext des neuen DSG. Der Themenblock wird schliesslich abgerundet mit einem Blick in die Praxis von David Rosenthal, der sich damit auseinander setzt, worauf beim Einsatz von KI in datenschutzrechtlicher Hinsicht zu achten ist.

Sandra Husi, Dr. iur., LLM, Executive MPA Unibe, Leiterin des Stabsbereichs Digital Compliance und Governance des Generalsekretariats EJPD, Datenschutzbeauftragte des EJPD, Bern.