www.jusletter-it.eu

Ursula Uttinger

Neue Möglichkeiten der Überwachung – ändert das revidierte Datenschutzgesetz etwas?

Die technischen Möglichkeiten, Personen zu überwachen, werden immer einfacher: Videokameras überall, im Arbeitsumfeld aber auch Autos, die immer mehr Daten sammeln – oft ohne Wissen der Betroffenen und Einhaltung der Datenschutz-Grundsätze. Der Schutz der betroffenen Personen wird auch mit dem revidierten Datenschutzgesetz nicht viel besser. Ethik als Teil der Lösung wird diskutiert, eine Datenschutz-Ombudsstelle könnte eine alternative Lösung sein.

Beitragsart: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz

Zitiervorschlag: Ursula Uttinger, Neue Möglichkeiten der Überwachung – ändert das revidierte Datenschutzgesetz etwas?, in: Jusletter IT 26. April 2022

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

Inhaltsübersicht

[1] Bereits in George Orwells Roman 1984[1] wird der Überwachungsstaat als Bedrohung dargestellt. Dabei werden unbequeme Daten und Fakten manipuliert. Ganz am Anfang des Buches liest man, wie die Bevölkerung einerseits ständig mit Nachrichten berieselt wird, andererseits, dass man zu sehen und zu hören war «solange man im Blickfeld der Metallplatte blieb»[2].

[2] Auch in einem weiteren literarischen Werk und Film «The Circle» von Dave Eggers[3], wird die ständige Überwachung noch verstärkt; es mündet in den Aussagen, dass Geheimnisse Verbrechen sind. Und «I'm saying that everyone should have a right to know everything, and should have the tools to know anything.»[4]

1. Video, Bodycam, Dashcam

[3] Das Thema Überwachung begleitet uns heute permanent – ganz offensichtlich im öffentlichen Verkehr[5], wofür es auch eine entsprechende gesetzliche Grundlage gibt: Videoüberwachungsverordnung ÖV[6], die das allgemeine Sicherheitsempfinden stärkt[7] – oder im öffentlichen Raum ganz allgemein. Bereits 2018 hat Humanrights CH[8] ausführlich beschrieben, wie immer mehr Videokameras den öffentlichen Raum in Beschlag nehmen, auch in der Schweiz, ohne dass der Schutz der Privatsphäre betroffener Personen gewährleistet ist[9]. Für Behörden, also öffentlich-rechtliche Akteure, bestehen auf kantonaler Ebene diverse Regelungen, die klare Vorgaben machen, beispielsweise bezüglich Dauer der Aufbewahrung von Daten, Überwachungszeiten, Ziel und Zweck[10]. Doch daneben gibt es sehr viele private Unternehmen und Personen, die ebenfalls eine Videokamera installieren, ohne dass es analoge Regelungen geben würde.

---

1 George Orwell, 1984 – veröffentlicht 8. Juni 1949.

2 George Orwell, 1984, S. 7, Ausgabe Reclam, 2021.

3 Dave Eggers, The Circle – veröffentlich am 8. Oktober 2013, als Film erschienen am 18. April 2017.

4 Dave Eggers, The Circle, S. 158, Ausgabe Mc Sweeney's Book, 2013.

5 https://www.sbb.ch/de/bahnhof-services/am-bahnhof/bahnhoefe/bahnhofordnung-regelung/datenschutz-hinweise-videoueberwachung.html – Abruf 11. Februar 2022.

6 SR 742.142.2 vom 4. November 2009.

7 https://www.sicherheitsforum.ch/digitale-technologie-steigert-die-sicherheit/ – Abruf 11. Februar 2022.

8 https://www.humanrights.ch/ – Abruf 11. Februar 2022.

https://de.wikipedia.org/wiki/Humanrights.ch - Abruf 11. Februar 2022.

9 https://www.humanrights.ch/de/ipf/menschenrechte/privatsphaere/unuebersichtliche-videoueberwachung-schweiz – Abruf 11. Februar 2022.

10 U.a. Kt. NW, Kt. OW, Kt SZ: https://www.kdsb.ch/xml_1/internet/de/application/d102/d127/f128.cfm – Abruf 11. Februar 2022; Kt ZH: Leitfaden Videoüberwachung durch öffentliche Organe – November 2020.

[4] Die Videoüberwachung durch Private auf öffentlichem Grund lässt sich hingegen kaum regeln. Dies zeigt auch die Antwort des Stadtrates Zürich auf ein Postulat bezüglich «rechtliche Regelung der privaten Überwachung im öffentlichen Raums durch Videokameras»[11]. Die Antwort des Stadtrates umfasst sowohl «klassische Videokameras» als auch Dashcams, Actionkameras bis hin zu Kameras in Smartphones. Die Klärung der Frage, inwiefern eine Videoüberwachung im öffentlichen Raum als gesteigerter Gemeingebrauch zu definieren ist, wird zwar mit Hinweis auf einzelne Lehrmeinungen[12] als möglich erachtet, weshalb eine Bewilligungspflicht geprüft, aufgrund der praktischen Umsetzbarkeit verworfen und das Postulat abgeschrieben wurde[13].

[5] Einen anderen Weg beschritt das Fürstentum Liechtenstein: Dieses kennt eine Meldepflicht der Videoüberwachung, sobald öffentlicher Raum betroffen ist. Dazu gehören auch Wege, Wald, «für den Publikumsverkehr geöffnete Flure, Treppenhäuser oder Parkgaragen bzw. Parkplätze etc.»[14] Ein vorsätzlicher Verstoss gegen diese Meldepflicht kann gemäss liechtensteinischem Datenschutzgesetz[15] gestützt auf Art. 5 Abs. 8 mit einer Busse von bis zu CHF 5'000.– geahndet werden.

[6] Auch Deutschland kennt bezüglich Videoüberwachung im öffentlichen Raum eine eigene Regelung in § 4 Bundesdatenschutzgesetz[16], wonach eine solche Installation nur unter bestimmten Gründen zulässig ist und diese möglichst früh erkennbar gemacht werden muss. Einzig darauf bezogene Sanktionen gibt es aber nicht.

[7] Das «European Data Protection Board» hat eine eigene Leitlinie zur Verarbeitung personenbezogener Daten durch Videogeräte herausgegeben[17]. Gemäss diesem Leitfaden ist im Einzelfall zu entscheiden, ob eine Videoaufnahme datenschutzkonform ist, auf alle Fälle muss Transparenz sichergestellt sein. In den meisten Fällen sollte zudem eine Datenschutz-Folgenabschätzung erfolgen. Bereits früher hat der eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ein Merkblatt zur Videoüberwachung durch private Personen herausgegeben[18]. Gemein ist diesen beiden Papieren, obwohl sie zeitlich mehrere Jahre auseinanderliegen, dass auf die allgemeinen Datenschutzgrundsätze verwiesen wird, die im Einzelfall zu prüfen sind. Im Merkblatt des EDÖB heisst es einleitend: «Es ist grundsätzlich nicht zulässig, dass Privatpersonen Videoüberwachungsanlagen auf öffentlichem Grund betreiben. Ausnahmen von dieser Regel sind nur in einem sehr engen Rahmen möglich.» Auch in der europäischen Leitlinie müssen diverse Voraussetzungen erfüllt sein, damit die Bearbeitung als datenschutzkonform beurteilet werden kann.

[8] Wiederholt hat sich das Bundesgericht mit der Auswertung von Aufnahmen durch Bodycams und Dashcams auseinandergesetzt und deren Verwertung als Eingriff in die Privatsphäre bezeichnet. Im Rahmen von Strafverfahren deren Auswertung abgelehnt, so unter anderen im

---

11 Auszug aus dem Protokoll des Stadtrats von Zürich vom 26. Oktober 2016, 846. Postulat von Peter Küng und Florian Utz betreffend rechtliche Regelung der privaten Überwachung des öffentlichen Raums durch Videokameras, Bericht und Abschreibung.

12 Lucien Müller, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung und Ahndung von Straftaten, S. 349, St. Gallen 2011.

13 Protokoll Stadtrat 26. Oktober 2016, S. 7.

14 https://www.datenschutzstelle.li/datenschutz/themen-z/videoueberwachung-fuer-betreiber – Abruf am 17. Februar 2022.

15 Lilex 235.1 Datenschutzgesetz vom 4. Oktober 2018.

16 Bundesdatenschutzgesetz vom 30. Juni 2017.

17 Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, angenommen am 29. Januar 2020.

18 Merkblatt Videoüberwachung durch private Personen, April 2014.

BGer 6B_810/2020; BGer 6B_1288/2019, BGer 6B_1188/2018, da es nicht um die Aufklärung «schwerer Verbrechen» ging.

[9] Das revidierte Datenschutzgesetz wird an den bisherigen Einschätzungen nichts ändern: Weiterhin wird im Einzelfall eine Videoüberwachung kritisch geprüft werden müssen, die Informationspflicht sowie eine Datenschutz-Folgenabschätzung werden Pflicht sein. Doch: Zwischen dem, was von Gesetzes wegen notwendig ist und dem, was in der Praxis umgesetzt wird, dürfte es einen grossen Unterschied geben. Viele Videokameras sind heute so klein und unauffällig[19], dass wohl kaum jemand Interesse hat, diese gross zu kennzeichnen. Ist nur ein kleiner Kreis über deren Existenz informiert, wird auch kaum eine Datenschutz-Folgenabschätzung vorgenommen. Insofern ist die Einschätzung des Stadtrates von Zürich aus dem Jahre 2016 auch heute noch korrekt. Die gesetzlichen Vorgaben sind das eine, die Realität das andere.

2. Überwachung im Büroalltag – nicht Science-Fiction sondern aktuell eingesetzte Technologien – Realität (die Nachfolgenden technischen Erläuterungen stammen von Stefan Willi)

[10] Eine nur bedingt wahrgenommene, indirekte Überwachung ist heute im Büroalltag Realität: Je nach Programm ist für diverse Nutzende sofort erkennbar, wann jemand gerade online ist und wer wann welches Dokument heruntergeladen bzw. angeschaut hat[20]. Insbesondere bezüglich des Herunterladens von Dokumenten lässt sich dies begründen mit der Nachvollziehbarkeit, die auch datenschutzrechtlich indirekt gefordert ist. Nicht berücksichtigt wird dabei, dass diese Nachvollziehbarkeit nicht jederzeit und für eine unbegrenzt grosse Anzahl von Personen möglich sein muss. Im Sinne der Verhältnismässigkeit sollte eine solche «Überwachung» nur einem kleinen und vordefinierten Personenkreis möglich sein.

[11] Nicht bedacht wird, dass wir bei WiFi-System zudem eine Realtime Überwachung haben: der aktuelle Standort jedes Gerätes kann jederzeit verfolgt werden. Das Tracking einer Person wird gespeichert und kann im Nachhinein eingesehen werden, da es während 2 Monaten gespeichert wird. Viele Hotspots neuer Generationen haben gleichzeitig noch Bluetooth integriert und ermöglichen so eine noch genauere Lokation des Gastgerätes. Ein Beispiel dazu ist: Hans Muster hat den Meetingraum MusterRoom für 10:00 gebucht. Ist er bis 10:00 nicht in diesem Raum angekommen (Bluetooth) sendet der Service Hans Muster per E-Mail eine Anfrage, ob er den Raum wirklich benötigt oder freigeben möchte. Ist er 10:15 immer noch nicht eingetroffen oder hat die Raumreservation nicht bestätigt, wird die Reservation vom System automatisch freigegeben[21].

[12] Zum Zweck der Lizenzbewirtschaftung werden zum Beispiel alle Applikationszugriffe aufgezeichnet, d.h. es ist nachvollziehbar, wie oft, wann und wie lange «Hans Muster» sein Word nutzt. Nutzt er es über Monate nicht, wird das Programm deinstalliert und die Lizenz freigegeben (Kostenoptimierungen). Dadurch wird klar, welche Programme von einer bestimmten Person genutzt werden.

---

19 https://www.20min.ch/story/kamera-so-gross-wie-ein-salzkorn-macht-absolut-faszinierende-aufnahmen-139359530391 – Abruf 17. Februar 2022.

20 Beispielsweise Microsoft Teams: https://support.microsoft.com/de-de/office/sehen-wer-online-in-teams-c73fd49c-a2aa-4703-8ab7-7a54b23869d7 – Abruf 17. Februar 2022.

21 Auskunft: Stefan Willi von WWZ.

[13] Dies gilt nicht nur für die Nutzung von Programmen, sondern auch für die Nutzung des Internets. Jeder Zugriff auf das Internet wird aufgezeichnet, das heisst die Anfrage auf http://www.hslu.ch geht über einen DNS Dienst,[22] welcher sicherstellt, dass www.hslu.ch zu den guten Links gehört und sich dahinter keine Malware verbirgt. Umgesetzt wird dies durch Unternehmen, welche riesige Listen von vulnerablen Linksammlungen bewirtschaften. Bekommt Hans Muster also ein E-Mail, welches einen Link beinhaltet (z.B. von seiner Bank), dann wird nach dem Klicken des Links über diesen DNS Dienst zuerst abgeklärt, ob dieser Link, der sich vordergründig wie ein echter Link der Bank präsentiert, auch wirklich ein sicheres Ziel ist. Wenn nicht, wird der Zugriff geblockt und eine Meldung angezeigt.

[14] Viele Zeiterfassungssysteme, welche über eine App gesteuert sind, zeigen die geografische Position der Erfassung an. Dies dürfte meistens bekannt sein – doch ist dieses Wissen eher passiv. Analog zu Zutrittssystemen mit Badges können solche Informationen auch genutzt werden, wenn die Arbeitgeberin wissen möchte, wer wann in welchen Gebäuden/Räumen gewesen ist, wenn es beispielsweise zu einem Diebstahl oder einem anderen nicht erwünschten Ereignis gekommen ist: Schnell kommt der Ruf an die Systemverantwortlichen, den Vorgesetzen die Information herauszugeben, wer sich zu einem bestimmten Zeitpunkt am entsprechenden Ort aufgehalten habe.

[15] Doch nicht nur bei der Arbeit im Büro, auch im Homeoffice oder Homeworking werden weitergehende Informationen aufgezeichnet, die kaum allgemein bekannt sind. Anhand der IP-Adresse kann relativ genau festgestellt werden, aus welcher Region Mitarbeitende aktuell das Homeoffice betreiben. Es ist nachvollziehbar, ob Hans Muster vom Tessin oder von Cham aus arbeitet, wo er seinen festen Wohnsitz hat. Spannend wird es dann, wenn jemand Pikett hat und innert einer vorgegebenen Zeit vor Ort sein müsste, dies aber aufgrund seines über die IP-Adresse bekannten Standortes nicht sein kann. Inwiefern Arbeitgeber dies tatsächlich überprüfen, wird zumindest öffentlich nicht kommuniziert.

[16] Nachvollziehbar und sinnvoll sind Totmann-Apps auf dem Smartphone. Arbeitet eine Person alleine, so muss diese eine solche App installieren: Bewegt sich der Mitarbeiter nicht ständig, sondern steht still, vibriert das Smartphone und nach 2 Minuten und wenn der Alarm nicht quittiert wird, sendet das Totmanngerät Position und das Bewegungsmuster an eine Notfall-Zentrale (oft Polizei oder Ambulanz direkt). Die Installation einer solchen App erfolgt zudem nicht heimlich und dient primär der Sicherheit des Mitarbeitenden. Ein Missbrauch durch den Arbeitgeber lässt sich zwar nicht ausschliessen, dürfte aber eine untergeordnete Rolle spielen.

[17] Gerade im HR-Umfeld werden vermehrt Tools eingesetzt, wie auch das Projekt «Big Data or Big Brother» der Universität St. Gallen[23] zeigt: Dabei wird unterschieden zwischen Tools zur Mitarbeiterbindung und -entwicklung, Arbeitsplatzgestaltung, Leistungsmanagement, Auswahl von Mitarbeitenden und Compliance Management. Eine Umfrage bei Unternehmen zeigte von 2018 zu 2020 eine grosse Steigerung im Bereich der verwendeten Tools im Leistungsmanagement von 37 % im Jahr 2018[24], zu 47 % im Jahr 2020[25]. Im Rahmen des Projekts wird unterschieden

22 DNS Dienst = Domain Name System = «Telefonbuch des Internets» https://www.elektronik-kompendium.de/sites/net/0901141.htm – Abruf 20. Februar 2022.

23 http://www.faa.unisg.ch/de/hr-analytics – Abruf am 20. Februar 2022.

24 Antoinette Weibel, Simon Schafheitle, Isabel Ebert, Goldgräberstimmung im Personalmanagement, in OrganisationsEntwicklung 3/2019, S 26.

25 Isabelle Wildhaber, Rechtliche Grenzen der Datenerfassung mittels Analytic Tools am Arbeitsplatz, Tagung Schulthess 1. Februar 2022.

zwischen Good Brother, also Tools, die zugunsten der Mitarbeitenden eingesetzt werden, und Big Brother. Im Resultat werden die Tools gemäss Umfrageergebnis mehrheitlich zugunsten der Mitarbeitenden eingesetzt und die Unternehmen sind sich bewusst, dass solche Tools auf das Vertrauensklima Auswirkungen haben können. Deshalb setzen die Unternehmen, die an dieser Umfrage teilnahmen, solche Tools möglichst transparent ein – ein rein numerisch-ökonomisierter Ansatz kann zu einem Verlust der Wertschätzung und damit auch der Motivation der Mitarbeitenden führen[26].

[18] Dass die Überwachung von Mitarbeitenden eine permanente Versuchung ist, zeigt das Tool der Firma Teleperformance: Primär versucht es das Kundenverhalten vorherzusagen[27], schreckt aber in Ländern mit schwächerem Datenschutz nicht vor der Überwachung der Mitarbeitenden im Homeoffice zurück[28]. Immerhin zeigen höhere Datenschutzstandards Wirkung, weshalb solche Tools vorwiegend (ausschliesslich?) in Ländern angewandt werden, die keinen hohen Datenschutz aufweisen.

[19] Ein Risiko bei der Überwachung von Mitarbeitenden besteht insbesondere darin, dass Arbeitgeber versucht sein können, eine Einwilligung für die Überwachung einzuholen. Dass dabei oft die Angst vor einem Verlust des Arbeitsplatzes eine Einwilligung zur Nutzung solcher Tools begünstigt, dürfte allgemein bekannt sein. Inwiefern eine Einwilligung bei einem Abhängigkeitsverhältnis rechtsgültig möglich ist, ist umstritten[29]. In den Erwägungen der europäischen Datenschutzgrundverordnung (DSGVO) wird ausdrücklich auf die Problematik eines möglichen Ungleichgewichts verwiesen, welches das Erfordernis der Freiwilligkeit in Frage stellen kann[30].

[20] Im Zusammenhang mit der Überwachung im Arbeitsumfeld bringt die Revision des Datenschutzgesetzes insofern eine Verbesserung, als dass die Informationspflicht umfassender geregelt ist: so müssen betroffene Personen angemessen über die Datenbearbeitung informiert werden und die Zustimmung zur Bearbeitung muss *freiwillig* erfolgen. Anders als in den Erwägungen der DSGVO wird in der Botschaft zum revidierten DSG nicht darauf eingegangen, dass es ein Ungleichgewicht geben könnte und deswegen eine Einwilligung kritisch hinterfragt werden muss. Es wird zwar darauf hingewiesen, dass «eine fünfte, besonders bedeutsam Leitlinie der Revision» die Stärkung der Rechte der Betroffenen ist und insbesondere die Voraussetzungen für die Einwilligung genauer festgelegt werden[31]. Die Stärkung beruht schliesslich darauf, dass die Formulierung angepasst wurde, eine «grundsätzliche Änderung der aktuellen Rechtslage» erfolgt deswegen jedoch nicht.[32]

[21] Es wird interessant sein zu beobachten, wie diese Informationspflicht zukünftig in der Praxis wahrgenommen (umgesetzt?) wird. Aus Praktikabilitätsgründen, aber auch weil das Interesse der

---

26 Weibel, Schafheitle, Ebert, S. 28.

27 https://teleperformance.com/en-us/services/analytics-and-consulting/advanced-analytics/ – Abruf am 20. Februar 2022.

28 https://www.20min.ch/story/call-center-ueberwacht-im-homeoffice-mitarbeitende-mit-high-tech-kamera-747996407342 – Abruf am 20. Februar 2022.https://www.golem.de/news/apple-amazon-uber-callcenter-ueberwachen-angestellte-mit-kameras-im-homeoffice-2108-158804.html – Abruf am 20. Februar 2022.

29 Tobias Fasnacht, Die Einwilligung im Datenschutzrecht , in: AISUF Band 38, S. 99, Zürich 2017.

30 Erwägungsgrund 43 zur Verordnung (EU) 2016/679 des europäischen Parlaments und Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

31 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz BBl 2017 S. 6971.

32 BBl 2017 S. 7027.

betroffenen Personen meist eher gering ist, dürfte sich eine Art Generaleinwilligung etablieren. Die Grundsätze der Datenbearbeitung ändern sich nicht und auch Art. 328b OR wird mit der Revision keine Änderung erfahren ausser dem Hinweis auf das aktualisierte Datenschutzgesetz (statt Bestimmungen des Bundesgesetzes vom 19. Juni 2020 neu vom 25. September 2020).

3. Und was machen die modernen Fahrzeuge?

[22] Der ADAC[33] hat erst kürzlich einen umfassenderen Artikel zu den umfassenden Sammeltätigkeiten der Automobilhersteller publiziert[34]. Darin wird ausführlich dargelegt, dass die betroffenen, autofahrenden Kunden nicht wissen, welche Daten konkret gesammelt und bearbeitet werden. Der Zugriff auf die Daten wird auch freien Werkstätten, also Werkstätten, die nicht eine feste Bindung zu einer bestimmten Automarke haben, oder weiteren Dienstleistern zur Verfügung gestellt. Die Autohersteller entscheiden allein, welche Daten gesammelt werden und was damit passiert. Es werden sehr viele Daten gesammelt, beginnend bei Nutzungsprofilen wie Anzahl der einzelnen Fahrstrecken, GPS-Daten, über den Fahrstil – wie oft wird heftig gebremst, wie lange wird in welchem Modi gefahren –, bis hin zur Intensität der Nutzung/Anzahl der Fahrer; dabei werden auch Dauer und Zeitpunkt von Telefongesprächen und/oder Informationen zu eingelegten Medien (CD, USB-Stick etc.) gesammelt. Der ADAC fordert zu Recht Datentransparenz, Datenhoheit durch die Möglichkeit der einfachen Abschaltung der Datenverarbeitung, Datensicherheit und Wahlfreiheit. Statt der Fahrzeughersteller sollten betroffene Personen bestimmen, ob und wenn ja, welche Daten gesammelt werden.

[23] Noch viel weiter geht Tesla bezüglich Sammelns von Daten[35]. Insbesondere der sogenannte Wächtermodus von Tesla ist datenschutzrechtlich äusserst heikel, da auch Umgebungsbilder und damit Drittpersonen erfasst werden[36] Ein Tesla ist ausgestattet mit Kameras auf allen Seiten. Diese nehmen auch permanent Umgebungsbilder von einer hohen Qualität auf. Zwar gibt Tesla an, dass diese Daten nicht systematisch gesammelt und nur so lange als notwendig aufbewahrt werden. Verschiedene Vorfälle in Deutschland zeigen aber erstaunliches: So konnten aufgrund der Bilder eines Teslas sowohl der eigene Fahrer als Verursacher eines Unfalls überführt werden, nachdem er das Auto zerstört zurückgelassen hatte, als in einem anderen Fall der Unfallhergang mit einem Velofahrer mittels Filmaufnahmen nachgezeigt werden[37]:

[24] Der Fahrzeughalter mag mit dem Kauf über diese umfassende Datenbeschaffung informiert worden sein, die weiteren Nutzer des Fahrzeuges, Mitfahrende und insbesondere Personen ohne direkten Bezug zum Fahrzeug, haben weder Kenntnis erhalten noch eine Einwilligung gegeben. Nicht erstaunlich ist zudem, dass Tesla die Verantwortung bezüglich Einhaltung des Datenschutzes ausdrücklich dem Nutzer übergibt: «Bitte beachten Sie, dass allein Sie dafür verantwortlich

33 Allgemeiner Deutscher Automobilclub – https://www.adac.de/ – Abruf 20. Februar 2022.

34 ADAC: Spion im Auto: Diese Daten werden gespeichert vom 3.2.2022.

35 https://www.zdf.de/nachrichten/wirtschaft/tesla-videoueberwachung-dashcam-datenschutz-100.html – Abruf 25. Februar 2022.

36 https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/tesla-datenschutz-autobauer-gibt-fahrdaten-an-behoerden-weiter/ – Abruf 25. Februar 2022.

37 https://www.zdf.de/politik/frontal/datenkrake-tesla-das-auto-als-spion-102.html – Abruf 20. Februar 2022.

sind, alle vor Ort geltenden Vorschriften und Eigentumsvorbehalte im Hinblick auf die Verwendung von Kameras zu prüfen und einzuhalten»[38].

[25] Grundsätzlich kann der «Wächter Modus» beim Tesla ausgeschaltet werden, dies führt dann zum Warnhinweis, dass «bei Ihrem Fahrzeug eine lediglich eingeschränkte Funktionalität, ernsthafte Schäden oder Funktionsunfähigkeit eintreten» können[39].

[26] Inwiefern die im «Owners Manual» angegebenen Zeiten der Datenspeicherung stimmen, ist kritisch zu hinterfragen; zumindest bei den vom ZDF aufgedeckten Fällen aus dem Jahr 2021 wurden viel mehr Daten gesammelt und aufbewahrt als beschrieben.

[27] Auch hier stellt sich die Frage: Was kann das revidierte Schweizer Datenschutzgesetz bewirken? Es ist nicht davon auszugehen, dass Tesla sein Konzept ändern oder es aus «Datenschutzgründen» weniger Käufer geben wird.

4. Was bringt also das Gesetz?

[28] Gemäss Botschaft zur Revision des Datenschutzgesetzes orientiert sich die Revision an sieben Leitlinien[40]:

- Risikobasierter Ansatz: Je nach Höhe der Risikoeinschätzung für die betroffenen Personen muss der Datenbearbeiter weitergehenden Pflichten nachkommen;
- Technologieneutrales Gesetz,
- Modernisierung der Terminologien,
- Verbesserung des grenzüberschreitenden Datenverkehrs,
- Stärkung der Rechte Betroffener,
- Weitergehende Pflichten der Datenbearbeiter,
- Stärkung der Kontrolle und damit Stärkung des EDÖB.

[29] Wie oben dargestellt, werden diese Leitlinien im Alltag nur bedingt zu Änderungen führen. Die sehr umfassenden Informationspflichten führen im Alltag zum Informationsparadoxon: Statt eines Transparenzgewinns kommt es zu einem Informations-Overkill. Die Informationspflicht des revidierten Datenschutzgesetzes ist nicht ganz so detailliert geregelt wie die Informationspflicht in der DSGVO. Dennoch dürften die Schlussfolgerungen, dass die Informationspflicht überschiessend ist[41], nicht von der Hand zu weisen sein. Die Bedürfnisse der Nutzenden sollten stärker miteinbezogen werden. Bekanntlich werden viele AGBs und Datenschutzhinweise nicht gelesen[42]; eine Studie aus dem Jahre 2017 in Deutschland zeigte, dass 73 % der Nutzer Daten-

38 https://www.tesla.com/ownersmanual/model3/de_us/GUID-3C7A4D8B-2904-4093-9841-35596A110DE7.html – Abruf 25. Februar 2022.

39 https://www.zdf.de/politik/frontal/datenkrake-tesla-das-auto-als-spion-102.html – Abruf 20. Februar 2022.

40 BBl, S. 6970 f.

41 Bettina Robrecht, EU- Datenschutzgrundverordnung: Transparenzgewinn oder Information-Overkill, S. 55, Edewecht 2015.

42 Bettina Robrecht, S. 64.

schutzerklärungen im Internet nicht lesen, und 77 % der Meinung sind, dass es zwecklos sei, da man auf jeden Fall zustimmen müsse[43].

[30] Mit dem baldigen Inkrafttreten der Revision des Datenschutzgesetzes werden sich sicherlich, analog zum Zeitpunkt der Anwendung der DSGVO, dem 25. Mai 2018, diverse Unternehmen vermehrt, oder sogar erstmals, mit dem Thema Datenschutz auseinandersetzen (vgl. Umfrage in Deutschland vom 15. November bis 2. Dezember 2018)[44]. Nicht im Widerspruch dazu steht die Umfrage der ZHAW vom Mai 2018[45], wonach eine Mehrheit der befragten Unternehmen dem Datenschutz einen hohen Stellenwert zuschreibt[46]. Doch schon bald nach dem ersten Hype um die DSGVO verloren sowohl Betroffene als auch Unternehmen wieder ihr Interesse am Datenschutz[47]. Dies dürfte nach der Einführung des revidierten Datenschutzgesetzes in der Schweiz ähnlich sein.

5. Fazit

[31] Der technologische Wandel führt dazu, dass immer mehr Daten und damit auch Personendaten generiert werden[48]. Die Lösung des Gesetzes und der damit einhergehenden Regulierung bringt kaum die erhoffte Verbesserung[49]. Grundsätzlich können betroffene Personen privatrechtlich klagen (Art. 32 nDSG), sofern es sich um einen Straftatbestand handelt, Strafanzeige einreichen oder hoffen, dass der EDÖB (Art. 49 ff. nDSG) nach Meldung ein Verfahren eröffnet. Der EDÖB hat zudem die weitere Aufgabe, betroffene Personen zu informieren, «wie sie ihre Rechte ausüben können (Art. 58 Abs. 1 lit.c nDSG)». Dazu kann er auch Arbeitsinstrumente und Empfehlungen erarbeiten (Art. 58 Abs. 1 lit. g nDSG), wird dazu jedoch entsprechend Personalressourcen brauchen[50]. Die drei zusätzlichen Stellen[51], die er mit der Revision des Gesetzes erhält, werden kaum genügen, um alle bisherigen und neuen Aufgaben zu erfüllen.

[32] Zivilrechtliche Klagen sind mit Kosten und Aufwand verbunden: Die klagende Partei muss grundsätzlich beweisen, dass die Daten nicht korrekt bearbeitet wurden, sodann trägt sie das Prozesskostenrisiko, selbst wenn sie gewinnt, abgesehen davon, dass es Zeit in Anspruch nimmt. Zivilrechtliche Klagen im Zusammenhang mit Datenschutz dürften weiterhin nicht in Massen zu erwarten sein.

[33] Strafrechtlich sind nur wenige Tatbestände erfasst (Art. 60ff nDSG), dabei müssen die Taten **vorsätzlich** erfolgen; es handelt sich um Antragsdelikte mit Ausnahme der Missachtung von Verfügungen des EDÖB oder einer Rechtsmittelinstanz (Art. 63 nDSG). Der Strafrahmen von

43 https://www.datenschutz-notizen.de/keiner-liest-die-datenschutzerklaerung-von-internetdiensten-aber-was-ist-das-eigentliche-problem-0623411/ – Abruf 25. Februar 2022.

44 https://www.heise-regioconcept.de/unternehmens-news/umfrage-grossteil-der-kmu-bleibt-beim-thema-dsgvo-gelassen – Abruf 25. Februar 2022.

45 Nico Ebert, Michael Widmer, Datenschutz in Schweizer Unternehmen 2018.

46 Nico Ebert, Michael Widmer, S. 10.

47 https://www.iwd.de/artikel/dsgvo-ein-jahr-allgemeine-datenverunsicherung-431188/ – Abruf 25. Februar 2022.

48 https://www.iwd.de/artikel/datenmenge-explodiert-431851/ – Abruf 25. Februar 2022.

49 Darcy W.W. Allen, Chris Berg, Sinclair Davidson, Zur Zukunft der Privatsphäre, S. 119 in: Liberalismus 2.0, Hrsg. Olivier Kessler, Zürich 2021.

50 Interpellation 16.3011, Nicht nur das Datenschutzgesetz, sondern auch die Ressourcen von Matthias Aebischer.

51 Tätigkeitsbericht 2020/2021 des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, März 2021) S. 84.

CHF 250'000.– ist 25-mal höher als bisher. Anders als in den meisten anderen Ländern sieht das Schweizer Datenschutzgesetz eine persönliche Strafbarkeit vor. Nicht die Unternehmen werden zur Rechenschaft gezogen, sondern die verantwortlichen Mitarbeitenden. Diese Schweizer Lösung wird unterschiedlich beurteilt – öfters aber auch kritisiert[52].

[34] Daten werden oft als Teil eines Geschäftsmodells betrachtet; abschreckende Bussen, wie in Art. 83 DSGVO vorgesehen, können Wirkung zeigen: Der Business-Case der nicht konformen Datenbearbeitung rechnet sich dadurch nicht. Eine solche Regelung fehlt aber im revidierten Gesetz.

[35] Insofern ist kritisch zu hinterfragen, wie viel die Revision des Gesetzes tatsächlich betroffenen Personen bringt. Das revidierte Schweizer Datenschutzgesetz, analog zur DSGVO, basiert auf einer Illusion: Die Illusion der informationellen Selbstbestimmung, zurückgehend auf ein Gutachten aus Deutschland aus dem Jahre 1971[53], durch das sogenannte Volkszählungsurteil von 1983[54] als Grundrecht anerkannt, kann nicht umgesetzt werden. Selbstbestimmt über eine Datenbearbeitung zu entscheiden, würde eine Übersicht über sämtliche bearbeiteten Daten bedingen. Viel zu viele Daten werden bearbeitet ohne Wissen der Betroffenen; ist das Wissen gegeben, fehlt eine einfache und pragmatische Handhabe.

[36] Eine weitere Frage, die nur angedeutet werden soll: Braucht es tatsächlich eine informationelle Selbstbestimmung, dies mit Blick über Europa hinaus. Die fünf grössten Tech-Giganten stammen alle aus den USA[55], China wird die neuen technischen Standards prägen[56] – das dürfte kein Zufall sein. Keinesfalls soll damit eine Absage an die Grundrechte angedacht/angedeutet werden – vielmehr sollte über neue Ansätze nachgedacht werden.

6. Alternative Lösungen heute?

[37] Datenethik ist in aller Munde und diverse Fachhochschulen bieten entsprechende Weiterbildungen an[57]. Es gibt einen Datenethikkodex der Swiss Alliance for Data-Intensive Service[58] und europaweit haben sich die Leitlinien zur digitalen Ethik von 4 im Jahre 2015 auf 42 im Jahre 2019 mehr als verzehnfacht[59] .

---

52 Matthias Glanzmann: The Good, the Bad and the Ugly: Gedanken zum neuen Datenschutzgesetz https://datenrecht.ch/the-good-the-bad-and-the-ugly-gedanken-zum-neuen-datenschutzgesetz/ – Abruf 1. März 2022.

53 W. Steinmüller, B. Lutterbeck, C. Mallmann, U. Harbort, G. Kolb, J. Schneider, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, S. 93ff., Juli 1971.

54 BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83.

55 Infografik: Das Zeitalter der Tech-Giganten | Statista – Abruf 4. März 2022.

56 Wie China mit eigenen Technologiestandards die ganze Welt prägt (handelsblatt.com) – Abruf 4. März 2022.

57 Unter anderem: CAS Digital Ethics HSLU: https://www.hslu.ch/de-ch/informatik/weiterbildung/digital-business-and-innovation/cas-digital-ethics – Abruf 1. März 2022.

CAS Digital Ethics fh- hwz: https://fh-hwz.ch/produkt/cas-digital-ethics/ – Abruf 1. März 2022.

Universität Zürich: https://www.asae.uzh.ch/de/weiterbildungskurse/ethikdigitalisierungundinnovation.html – Abruf 1. März 2022.

58 https://data-innovation.org/data-ethics/ - Abruf 1. März 2022.

59 Executive Summary/Leitlinie zur digitalen Ethik im Vergleich 2020, Institute for Digital Transformation in HealthCare, Universität Witten/Herdecke.

[38] Eine ethische Wertung von Datennutzung fordert die Gesellschaft heraus: Nun muss im Einzelfall, allenfalls beispielhaft «gutes und schlechtes» Handeln beurteilt werden. Einen Konsens zu finden, was ethisch gut ist, dürfte eine grössere Herausforderung darstellen[60]. Es gibt deshalb auch vereinzelte Kritik, da die Umsetzung im Alltag äusserst anspruchsvoll, wenn nicht gar unmöglich sein dürfte. Man ist kaum in der Lage, wie angedacht die ethische Fragestellung klar zu ermitteln, die ethisch relevanten Fakten zu sammeln, verschiedene Standpunkte und Argumentarien zu sammeln und gestützt darauf zu einer Entscheidungsfindung[61] zu kommen. Weiter ist bei der Datenethik zu berücksichtigen, dass wir immer wieder vor neuen Herausforderungen stehen, die neu beurteilt werden müssen[62].

[39] Ob Datenethik die Lösung ist, muss sich zeige, dürfte in der Umsetzung jedoch schwierig sein, da nicht einfach umsetzbar.

[40] Eine weitere Möglichkeit könnte ein Ombudsstelle für Datenschutz sein. Ombudsstellen haben den Vorteil, dass zu diesen ein niederschwelliger Zugang möglich ist; Ombudsstellen sind kostenlos, relativ schnell im Vergleich zu ordentlichen Verfahren[63] und haben das Ziel zu vermitteln, eine alternative Konfliktlösung zu finden[64]. Es geht dabei nicht um Rechtsprechung, sondern darum, ohne grossen bürokratischen Aufwand eine Lösung zu finden[65]. Ist das Verfahren erfolglos, steht der Gerichtsweg weiterhin offen.

[41] Die Schweiz kennt schon seit längerem Ombudsstellen; die älteste Schweizer Ombudsstelle wurde 1971 in Zürich errichtet[66]. Seither haben immer mehr Kantone, aber auch Branchen, eigene Ombudsstellen errichtet[67]. Ombudsstellen haben kontinuierlich mehr Fälle zu bearbeiten[68] und geniessen eine hohe Akzeptanz[69]. Eine solche Institution könnte förderlich sein, vermehrt Datenschutzverletzungen zu adressieren. Heute gibt es (zu) wenig Klagen; man hört von vielen Herausforderungen/Schwierigkeiten, die eine Verletzung des Datenschutzes vermuten lassen – doch Urteile findet man kaum.

Ursula Uttinger, lic. iur./exec MBA HSG technische Ergänzungen: Stefan Willi, CTO IT, WWZ Energie AG.

60 Johannes Fischer, Ethik als rationale Begründung der Moral, S. 19, Zürich 2010.

61 Ivo Wallimann, Ethisches Entscheiden in der Politik, im Beruf und im sonstigen Alltag, Blogbeitrag vom 20. Dezember 2016 – https://www.philosophie.ch/artikel/ethisches-entscheiden-in-der-politik-im-beruf-und-im-sonstigen-alltag – Abruf 2. März 2022.

62 David J. Hand, Aspects of Data Ethics in a Changing World: Where are we now, in Big Data 6.3, S. 176 ff.

63 Claudia Kaufmann, Zugang zum Recht: vielfältig und anspruchsvoll, S. 17 f. in Zugang zum Recht, Vom Grundrecht auf einen wirksamen Rechtsschutz, Hrsg. Claudia Kaufmann, Christina Hausamann, Basel 2017.

64 Regina Kiener, Das Recht auf effektiven Rechtsschutz, S. 33 in Zugang zum Recht, Vom Grundrecht auf einen wirksamen Rechtsschutz.

65 Wie Ombudsstellen funktionieren:«Vermittlerinnen mit begrenzter Macht » workzeitung.ch – Abruf 4. März 2022.

66 https://www.stadt-zuerich.ch/portal/de/index/service/medien/medienmitteilungen/2021/oktober/211101a.html – Abruf 4. März 2022.

67 https://www.ombudsstellen.ch/ombudsadressen/ – Abruf 4. März 2022.

68 Z.B. Jahresbericht 2020, Ombudsmann der Privatversicherung und der Suva, S. 6. Jahresbericht 2020, Ombudsstelle Stadt Zürich, S. 63.

69 Z.B. https://www.insel.ch/de/patienten-und-besucher/beratungen-und-dienstleistungen/ombudsstelle – Abruf 4. März 2022.