Die schleichende Emanzipation des Datenschutzes

Eine Spurensuche und ein Ausblick

Christian Drechsler, Rechtsanwalt, General Counsel Data & Digital, Schindler Management AG

Résumé: La révision de la loi sur la protection des données entrera en vigueur prochainement. Elle apporte une protection nettement renforcée, comme le montre aussi le débat public. Mais on oublie souvent que la révision ne change rien aux concepts de base du droit actuel, qui avaient été définis il y a une trentaine d'années lorsque la première version de la loi a été créée. Ils sont restés valables car, par un choix conscient ou non, ils avaient pour but de poser des jalons. La révision n'a pas seulement repris ces principes, mais elle les a même accentués. Grâce à eux, la loi révisée fonctionnera aussi «convenablement». Mais des signes avant-coureurs se multiplient: à l'ère des ordinateurs quantiques, des supercalculateurs, de l'intelligence artificielle et d'autres technologies de ce genre, ces principes, en tant que fondements dogmatiques, ou au moins en combinaison, ont fait leur temps. A long terme, il sera indispensable de revoir les fondements même de la protection des données.

Zusammenfassung: Das revidierte Datenschutzgesetz tritt demnächst in Kraft. Es wird gegenüber der Vorversion deutlich verschärft. Diese Verschärfung dominiert auch die Diskussion. Dabei bleibt meist unerwähnt, dass die Revision nichts an den grundlegenden Konzepten des Gesetzes geändert hat. Diese Konzepte wurden vor gut 30 Jahren definiert, als die Erstversion des Gesetzes geschaffen wurde, und sie haben es in sich, weil es sich dabei um – bewusste oder unbewusste – Weichenstellungen handelte. Die Revision hat diese Konzepte

nicht nur übernommen, sondern sogar noch akzentuiert. Damit wird auch das revidierte Gesetz «leidlich» funktionieren. Aber die Anzeichen mehren sich, dass sie als dogmatischer Unterbau des Gesetzes im Zeitalter von Quantum Computing, Hyperscalers, Künstlicher Intelligenz und dergleichen zusehends ausgedient haben – zumindest in Kombination. Langfristig wird man kaum darum herumkommen, den Datenschutz konzeptionell auf neue Beine zu stellen, wenn man dem Thema beikommen will.

I. Konzepte

1

Die Erstversion des Datenschutzgesetzes aus dem alten Jahrtausend enthält vier konzeptionelle Elemente, die den Datenschutz in der Praxis bis heute massgeblich prägen:

2

1. Man entschied sich für ein Gesetz, das sowohl für den Staat gilt (wenn er Personendaten der Bürger bearbeitet) als auch für Private, insbesondere Firmen (wenn sie Personendaten von Individuen bearbeiten). Zwingend war dieser Entscheid beileibe nicht, sondern eher ungewöhnlich, weil so öffentliches Recht und Privatrecht in ein und dem selbem Gesetz geregelt wurden. Tatsächlich waren hier ursprünglich zwei Gesetze geplant; dieser Plan wurde dann aber fallen gelassen.

3

2. Im Privatrecht, worum es in diesem Beitrag geht, wurde der Datenschutz als Persönlichkeitsrecht konzipiert. Vereinfacht gesagt war hier der Ansatz, dass eine Persönlichkeitsverletzung nicht nur dann vorliegen kann, wenn etwa das Recht auf Privatsphäre einer prominenten Person durch die Medien verletzt wird, sondern auch, wenn «wahre» Daten über einen Menschen Personen zur Kenntnis gebracht werden, die diese Daten nichts angehen.

4

3. Man war der Überzeugung, dass die Menschen mit den Rechtbehelfen des klassischen Persönlichkeitsrecht wegen dem «Einsatz von modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen» und der «enorme[n] Intensivierung der Datenbearbeitung» (Gesetzesbotschaft von 1988) nicht genügend geschützt seien und hier zusätzliche gesetzliche Schutzmechanismen erforderlich seien. Deshalb wurde eine Datenschutzbehörde ins Leben gerufen, und sie wurde nicht nur mit der Überwachung der Einhaltung des Datenschutzes durch den Staat beauftragt, sondern auch, allerdings in einem schwächeren Masse, im zivilrechtlichen Bereich. Hier wurde – ganz bewusst – ein klassisches Paradigma des Persönlichkeitsrechts im Zivilrecht durchbrochen, nämlich, dass die verletzte Person ihre Rechte immer selbst durchsetzen muss; sogar bei schweren Persönlichkeitsverletzungen. Diese Durchbrechung wurde dadurch noch verstärkt, dass einzelne dieser zivilrechtlichen Pflichten strafbewehrt sind – ihre Verletzung also durch eine vom Staat verhängte Strafe gesühnt werden kann.

5

4. Man hat die Datenbearbeiter des Privatrechts mit zusätzlichen Pflichten belegt, die Persönlichkeitsverletzungen vorbeugen sollen, z.B. die Pflicht zu geeigneten technischen und organisatorischen Schutzmassnahmen. Diese präventiven Pflichten bestehen gegenüber dem Staat, nicht gegenüber den Individuen. Wenn man diese Pflichten verletzt, verletzt man den Datenschutz, selbst wenn noch gar niemand zu Schaden gekommen ist – einfach, weil das «Dispositiv» ungenügend war. Auch solche prophylaktischen Pflichten sind dem klassischen Persönlichkeitsrecht fremd.

6

Das revidierte Gesetz hat diese Konzepte nicht nur beibehalten, sondern noch stärker betont. Auch sind diese vier Elemente mit gewissen Abweichungen fester Bestandteil der Datenschutzgesetzgebung der EU – sowohl des ersten Gesetzes von 1995 als auch der Datenschutz-Grundverordnung von 2018.

7

Weshalb sind diese Konzepte – oder ihre Kombination – für den Datenschutz zusehends unzureichend?

II. Datenschutz ist immer weniger Persönlichkeitsrecht

8

Der Datenschutz ist immer weniger Persönlichkeitsrecht, sondern zusehends ein komplexes – Aussenstehenden kaum noch zu vermittelndes – Gemenge aus klassischem Privatrecht, Privatrecht, das im Auftrag der betroffenen Personen vom Staat vollzogen wird, und reinem öffentlichen Recht. Längst hat sich das Thema, das seinerzeit als kleiner Bruder des allgemeinen Persönlichkeitsrechts an den Start ging, von seinem grossen Bruder emanzipiert und hat sich als eigenständiges Rechtsgebiet etabliert.

9

Das sieht man auch bei den Beratern, zum Beispiel bei den Anwälten: Die prototypische Anwältin, die auf Datenschutz spezialisiert ist, berät diese Spezialisierung selten in Kombination mit dem allgemeinen Persönlichkeitsrecht, sondern meist in Kombination mit IT-Recht. Hier bestehen die Synergien, nicht zum Persönlichkeitsrecht. Mit der im allgemeinen Persönlichkeitsschutz wichtigen Sphärentheorie – die Dinge sind geheim, privat oder öffentlich – werden die meisten Datenschützer wenig anfangen können; und das müssen sie auch nicht, weil sie für den Datenschutz nicht relevant

(und zu differenziert) ist. Ebenso ist der im allgemeinen Persönlichkeitsrecht anerkannte Grundsatz, wonach eine geringfügige Beeinträchtigung der Persönlichkeit noch keine Persönlichkeitsverletzung darstellt, im Datenschutz unbekannt: Eine Mindestschwelle in diesem Sinne für Bagatellverstösse kennt er nicht. Mit dem jährlich erscheinenden Mitgliederverzeichnis des Zürcher Anwaltsverbandes kann man den Trend, dass sich der Datenschutz vom Persönlichkeitsrecht emanzipiert hat, mit Zahlen untermauern: Die Zahl der Anwälte und Anwältinnen, die gemäss diesem Verzeichnis auf Datenschutz spezialisiert sind, hat sich seit 1998 um rund 500% (von ca. 20 auf 100) erhöht. Im gleichen Zeitraum stieg die Zahl der Medienrechtler (sie sind typischerweise auf allgemeines Persönlichkeitsrecht spezialisiert) nur um 30% (von ca. 60 auf 80), wobei ihre Anzahl seit über 10 Jahren stagniert. Auch die Anzahl Anwälte, die diese Themen in Kombination betreiben, nimmt laufend ab: 1998 gaben noch 30% der auf Datenschutz spezialisierten Anwälte als Expertise auch Medienrecht an; 2021 waren es nur noch 10%. Korrelation stellen diese Zahlen zwischen diesen Themen nicht her. Es ist keine sehr kühne These, dass die Verzeichnisse anderer Anwaltsverbände in der Schweiz und der EU ein ähnliches Bild zeichnen.

10

Dass der Datenschutz kein klassisches Persönlichkeitsrecht (mehr) ist, sieht man auch daran, dass das Thema in der Praxis zusehends von den Datenschutzbehörden geformt wird. Wenn sich die Zivilgerichte – überhaupt – mit datenschutzrechtlichen Fragen beschäftigen, dann sind es meistens nur akzessorische Fragen: Das Hauptthema des Prozesses ist ein anderes, oft eine arbeitsrechtliche Streitigkeit, und im Rahmen des Verfahrens werden vom Kläger dann auch Datenschutzverstösse geltend gemacht. So wichtig, dass man wegen einer vermuteten Datenschutzverletzung *allein* eine zivilrechtliche Klage einreicht, ist das Thema den wenigsten. Eher wird eine betroffene Person den Fall der Datenschutzbehörde anzeigen, in der Hoffnung, dass sie eine Untersuchung eröffnet. So lassen

sich die Kosten und das Risiko eines zivilrechtlichen Verfahrens einsparen. Der hier angebotene Service public weckt natürlich Begehrlichkeiten. Die in der Botschaft zum Erstgesetz von 1988 enthaltene Aussage, wonach die betroffenen Personen im privaten Bereich ihre datenschutzrechtlichen Ansprüche «in erster Linie selbst vor dem Zivilrichter geltend machen sollen», hat wenig Realitätsbezug und war Wunschdenken.

11

Der zunehmende Einfluss der Schweizer Datenschutzbehörde auch auf den zivilrechtlichen Datenschutz geht auch aus ihrem jährlichen Tätigkeitsbericht hervor. Obwohl die Behörde nach den gesetzlichen Vorgaben (des geltenden Rechts) im Zivilrecht nur ein (sehr) beschränktes Aufsichtsrecht hat, investierte sie gemäss den von ihr veröffentlichen Statistiken – zumindest in den letzten drei Jahren – regelmässig deutlich mehr Ressourcen in die privatrechtliche Aufsicht als in die öffentlich-rechtliche (wo das Aufsichtsrecht umfassend ist). Das mag zwar seine Gründe haben, untermauert aber gleichwohl die Beobachtung, dass die Behörden mittlerweile das «Kraftzentrum» der Entwicklung des privaten Datenschutzes sind, und nicht die Personen, deren Daten unrechtmässig bearbeitet wurden, selbst. Im Übrigen lässt sich dieses Phänomen in der EU genau gleich beobachten wie in der Schweiz, und hier sogar noch stärker.

12

Der «elephant in the room» ist in diesem Zusammenhang die Frage, ob sich die Behörden hier von den Anliegen der Menschen zusehends entkoppeln: Haben sie schon angefangen, eine eigene Agenda zu entwickeln, gemäss der sie den Menschen mittlerweile vorgeben, was unter ihren Persönlichkeitsrechten zu verstehen ist? So wie das Gesetz konzipiert ist, ist dieses Risiko systemimmanent. Es ist ein schmaler Grat.

III. Datenschutz als Grundrecht?

13

In der öffentlichen Diskussion wird mittlerweile auch im zivilrechtlichen Kontext meist pauschal vom Datenschutz als Grundrecht gesprochen. Das ist aber falsch: Nur im öffentlichen Recht, also gegenüber dem Staat, ist der Datenschutz ein – in der Verfassung garantiertes – Grundrecht. Im Zivilrecht ist er demgegenüber «nur» ein Persönlichkeitsrecht. Diese Unterscheidung ist fundamental: Im öffentlichen Recht stellt eine Datenbearbeitung durch den Staat konzeptionell einen Grundrechtseingriff dar. Dafür braucht es nach Schweizer Recht immer eine gesetzliche Grundlage, und entsprechend sieht das Datenschutzgesetz vor, dass die Bundesbehörden Personendaten nur bearbeiten dürfen, wenn dafür eine gesetzliche Grundlage besteht. Das ist im privaten Datenschutzrecht nicht erforderlich, weil es hier eben nicht um Grundrechte geht. Das gesetzliche Regime ist entsprechend – ganz bewusst – viel liberaler. Anders als der Staat können sich privatrechtliche Datenbearbeiter insbesondere auf ein «berechtigtes Interesse» berufen, um ihre Datenbearbeitung zu rechtfertigen.

14

Den Vorbehalt, dass der Datenschutz nur im öffentlichen Recht ein Grundrecht ist, hört man in der Diskussion immer seltener, oder er wird als akademisch abgetan. Die Regelung des Datenschutzes in Privatrecht und im öffentlichen Recht in ein und demselben Gesetz, mitsamt der Aufsicht von Staat und Privaten durch die gleiche Behörde, trägt dazu bei, dass diese Unterscheidung nicht mehr getroffen wird, weil sie dazu einlädt, das Thema «über den gleichen Leisten zu schlagen». Damit einher geht das latente Risiko, dass hier schleichend ein «race to the top» stattfindet, in dem Sinne, dass das strengere Verständnis des Datenschutzes aus dem öffentlichen Recht in der Praxis zusehends auch im privatrechtlichen Datenschutz Einzug hält – nicht nur in der Schweiz, sondern

auch in der EU.

15

Es wäre sachlich vielleicht nicht einmal falsch, dem privatrechtlichen Datenschutz der Zukunft auch den Charakter eines Grundrechts zuzuerkennen. Im Zusammenhang mit ESG werden solche Ausweitungen der Grundrechte auf das Privatrecht ja zurzeit auch gefordert. Konzeptionell würde die Änderung allerdings die Anerkennung der Drittwirkung von Grundrechten im Datenschutz bedeuten. Das wäre ein sehr weitreichender Entscheid und ein Paradigmenwechsel, den selbstverständlich nur der Gesetzgeber durch eine entsprechende Gesetzesänderung fällen könnte. Hier ist das Schweizer Recht dem der EU im Übrigen konzeptionell überlegen, und die Schweiz wäre deshalb schlecht beraten, sich bei einem solchen gesetzgeberischen Entscheid an der EU als Vorbild zu orientieren. Dort gilt nämlich grundsätzlich eine Drittwirkung im Datenschutz. Allerdings ist dies nur gemäss dem Gesetzeswort so, wogegen ein dogmatischer Unterbau, welcher der Tragweite der Drittwirkung von Grundrechten im Zivilrecht gerecht würde, fehlt.

16

Die gesetzliche Konzeption des privatrechtlichen Datenschutzes verträgt sich insgesamt also immer schlechter mit der Realität. In der Praxis ist er kein Persönlichkeitsrecht (mehr), obwohl das die gesetzliche Konzeption ist. In der öffentlichen Diskussion ist er (zunehmend) ein Grundrecht, obwohl das nicht die gesetzliche Konzeption ist.

IV. Die Leute «hängen ab»

17

Wie gesagt akzentuiert das revidierte Gesetz die überkommenen Konzepte, inklusive das persönlichkeitsrechtliche Konzept im Privatrecht. Das führt dazu, dass auch Individuen im revidierten Recht stärker in die Pflicht genommen werden: Viel

häufiger als früher muss man als Benutzer einer Website, einer App oder dergleichen Datenschutzerklärungen lesen, bevor man das Produkt nutzen kann. Und diese Erklärungen sind wegen den verschärften Pflichten der Datenbearbeiter deutlich länger und genauer als zuvor: Entweder muss man seine ausdrückliche Einwilligung in die Datenbearbeitung erklären oder man muss zumindest bestätigen, dass man die Datenschutzerklärung gelesen hat. Ähnliches sieht man bei den Cookies, wo man mittlerweile bei praktisch allen Websites die Cookies annehmen oder ablehnen muss, bevor man die Seite benutzen kann. Wozu das geführt hat, konnte man bereits in der EU beobachten, weil sie der Schweiz bei der Gesetzesrevision ein paar Jahre voraus ist: Die grosse Mehrheit der Leute hat keine Lust, seitenlange Datenschutzerklärungen zu studieren, bevor man eine App, eine Website etc. nutzen kann. Ohne die Datenschutzerklärung gelesen zu haben, erklärt man stattdessen einfach pauschal seine Einwilligung oder dass man die Datenschutzerklärung gelesen hat. Die Leute «hängen ab». Sie sind nicht bereit, die ihnen vom Gesetz zugeordnete Verantwortung wahrzunehmen.

18

Diese Entwicklung ist schlecht für den Datenschutz. Sie bringt das gesetzliche Konzept mitsamt seinem persönlichkeitsrechtlichen Ansatz unter Druck. Man kann die Leute nicht dazu zwingen, sich für den Datenschutz zu interessieren. Das Klicken der Kästchen verkommt zur Alibiübung. Gleichzeitig ist dieses Verhalten auch verständlich. Viele der modernen Datenbearbeitungen sind komplex und entsprechend viel Zeit müsste man in das Lesen der Datenschutzerklärung investieren, um sie zu verstehen. Warum sollte man nun ausgerechnet im Datenschutz diese Zeit investieren? Wir benutzen heutzutage im Alltag – direkt oder indirekt – alle möglichen komplexe Geräte und Maschinen (Fernseher, Kühlschränke, Flugzeuge etc.), deren Wirkungsweise wir auch nicht verstehen und auch nicht verstehen müssen. Anderseits ist dieses Verhalten auch zu respektieren: Autonomie bedeutet eben nicht nur, dass man bewusste

Entscheide fällt, sondern sie ist auch die Freiheit, unbewusste Entscheide zu fällen.

V. Der Umgang mit Daten und ihre Bearbeitung hat sich verändert

19

Die überkommenen Datenschutzkonzepte kommen auch dadurch unter Druck, dass sich die Art und Weise, wie Daten heutzutage geteilt und bearbeitet werden, gegenüber der Zeit, aus der diese Konzepte stammen, stark verändert hat: Die Prämisse des geltenden Rechts lautet: Der Datenschutz muss in dem Moment greifen, in dem ein Datensatz einem Menschen zugeordnet werden kann, weil dann das Risiko immanent ist, dass diese Zuordnung auch geschieht. Diese Gleichung mag damals ihre Berechtigung gehabt haben. Aber stimmt sie heute noch? Einerseits hat sich der Umgang der (meisten) Menschen mit ihren Daten stark verändert: Ausgelöst durch Social Media ist das Teilen von privaten Informationen über die Familie und den engsten Freundeskreis hinaus zur Selbstverständlichkeit geworden. Anderseits sind die Datenmengen, die heutzutage in den Datenzentren bearbeitet werden, wegen der gesteigerter Rechnerleistung massiv grösser als damals. Die «Zuordenbarkeit» dieser Datensätze ist für die Datenbearbeiter typischerweise zusehends irrelevant. Relevant ist nicht, wer sich hinter einem Profil verbirgt. Relevant ist, welche Profile gleichgelagert sind, und wie man diese Profile zum Massschneidern von Angeboten und Strategien (z.B. für personalisierte Werbung) verwenden kann.

20

Es stellt sich die Frage, ob hier der persönlichkeitsrechtliche Ansatz des geltenden Rechts, der das Individuum davor schützen soll, dass seine Daten ihm effektiv zugeordnet werden, noch sachgerecht ist. Oder wären hier andere Ansätze, eventuell eine kollektive Rechtsdurchsetzung,

zielführender?

VI. Wie weiter?

21

Den Datenschutz auf eine robustere dogmatische Grundlage zu stellen, wäre eine komplexe Aufgabe. Einfache Antworten gibt es hier nicht. Immerhin gibt es erste Ansätze – und sie sind auch nicht unbedingt neu:

22

Ein (weitergehender) Ansatz wäre, dass man den Datenschutz konsequent zum öffentlichen bzw. regulatorischen Recht macht, mit entsprechenden Kompetenzen der Behörden. Neue «datenschutzlastige» Produkte müssten in diesem Modell der Behörde vorgelegt und von ihr bewilligt werden, so wie man das zum Beispiel im Medizinalbereich kennt, wo neue Medikamente von einer Behörde für ihre Zulassung bewilligt werden müssen. Als Konsument des Medikaments kann man sich dann darauf verlassen, dass das Medikament wirkt und sicher ist, und man muss sich dazu nicht selbst eine Meinung bilden.

23

Ein anderer Ansatz – am anderen Ende des Spektrums – wäre, dass man den Datenschutz im Privatrecht wieder konsequent zum Persönlichkeitsrecht macht, dass man hier die Individuen mit anderen Worten wieder ins Zentrum stellt. Die Datenschutzbehörden würden sich in diesem Modell wieder stärker auf die Einhaltung des Datenschutzes im öffentlichen Bereich fokussieren: Der Staat verfügt in unserem System über das Gewaltmonopol. Er kann Zwangsmassnahmen anordnen, insbesondere in Form von Untersuchungshaft und Freiheitsstrafen. Private Akteure können das selbstverständlich nicht – auch Google und Meta nicht. Die Risken für die Bürger werden hier wegen dem Gewaltmonopol des Staates in Verbindung mit dem möglichen Einsatz neuer Technologien (Gesichtserkennung, Big Data etc.) in Zukunft

gewiss nicht kleiner. Funktionieren würde dieser Ansatz im Privatrecht allerdings nur, wenn man die Rechtsdurchsetzung für Individuen attraktiver macht, z.B. indem das Verfahren für den Kläger kostenlos oder zumindest günstig wäre (ähnlich wie zur Zeit z.B. schon bei arbeitsrechtlichen Streitigkeiten unter einem gewissen Streitwert oder bei Verfahren nach dem Gleichstellungsgesetz). Um einen allfälligen Rechtsmissbrauch durch solche Klagen zu vermeiden, wäre denkbar, eine gewisse Mindestanzahl an Klägern für eine solche Klagen zu verlangen (die sich für diesen Zweck allenfalls beim der Datenschutzbehörde melden könnten). Zusätzlich dazu wäre vorstellbar, dass bei einer erfolgreichen Klage das Urteil unter gewissen Voraussetzungen als «allgemeinverbindlich» erklärt wird, dass es also nicht nur gegenüber dem Kläger, sondern gegenüber allen betroffenen Personen mit gleicher Ausgangslage gilt. Dieser Ansatz hätte auch den Vorteil, dass er sicherstellen würde, dass nur dann ein Verfahren angestrengt wird, wenn es Personen gibt, die sich durch die betreffende Datenbearbeitung wirklich in ihren Rechten verletzt fühlen.

24

Denkbar wären auch Mischformen zwischen diesen beiden Extremen, die allerdings mehr Profil als das jetzige Konzept haben müssten. Als mögliche Vorlage könnte hier das Kartellrecht dienen: Auch hier kann neben der Behörde, die über die Einhaltung des Gesetzes wacht, auch eine Partei des Privatrechts, die von einer Gesetzverletzung betroffen ist, Klage erheben. Allerdings hat die Behörde, die Weko, doch eine deutlich profiliertere und klarere Rolle bei der Überwachung der Einhaltung des Gesetzes als der EDÖB, was sich unter anderem darin manifestiert, dass viele Vorgänge, die potenziell das Kartellrecht verletzen, vorab von der Weko genehmigt werden müssen.

25

Auch ganz andere Ansätze wären hier selbstverständlich denkbar

und vielleicht sogar zielführender, inklusive Ansätze, bei denen das Persönlichkeitsrecht als der konzeptionelle Grundpfeiler des Datenschutzes fallen gelassen wird. Aber eine grundsätzliche Auseinandersetzung mit den Konzepten «hinter» dem Datenschutz und der Frage, was eigentlich genau geschützt werden soll, wird sich langfristig kaum vermeiden lassen. Auch das gilt nicht nur für die Schweiz, sondern auch für die EU – wo diese Diskussion zum Teil schon geführt wird.

Christian Drechsler vertritt in diesem Beitrag seine persönliche Meinung.

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International Lizenz.