Die Borkenstruktur des Datenschutzes am Baum der Privatheit im Wald der Datenmacht

von Kai von Lewinski

In unserem Graduiertenkolleg haben wir in den letzten neun Jahren eine große Zahl von Perspektiven diskutiert, um Lösungen für die Fragen der Privatheit und Digitalisierung zu finden. Diese Lösungen aber haben jeweils immer nur eine Perspektive eingenommen – wie es ja auch das Ziel von Dissertationen ist. Was eine solchermaßen auf Promotionen fokussierte Einrichtung wie ein Graduiertenkolleg nicht leisten kann (und ja auch nicht soll), ist eine Kritik der methodischen Fokussierung. Die Abschlusstagung bot Gelegenheit, auf die Begrenztheiten der Begrenzung auf eine privatheitsbezogene bzw. persönlichkeitsrechtliche oder datenschutzrechtlichen Perspektive hinzuweisen.

Perspektivenmehrzahl

Wenn man die Perspektive(n) unserer Forschung(en) in den Blick nimmt, erkennt man auch ihre jeweiligen Begrenztheiten.

Die Mikroperspektive des Datenschutzes

Das Informationsrecht hat auf informationelle Vermachtungen bislang fast ausschließlich mit den Mitteln und Instrumenten des Datenschutzes reagiert. Gerade im angewandten Datenschutzrecht – also und zum Glück außerhalb des Graduiertenkollegs – ist das besonders fühlbar, wo das Volkszählungsurteil des Bundesverfassungsgerichts so inflationär im Munde geführt wird, dass es solchermaßen zum am weitesten verbreiteten Blindzitat des deutschen Rechts geworden sein dürfte. Wegen der doch recht abgeschlossenen Dogmatik des Datenschutzrechts bei gleichzeitig praktischer Bedeutsamkeit strahlt diese Perspektive auch auf andere Fächer aus.

Jedenfalls haben der Datenschutz und das Datenschutzrecht eine ganz spezifische Mikroperspektive. Fokussiert wird auf den einzelnen Datenverarbeitungsschritt in Bezug auf eine bestimmte ›betroffene Person‹. Diese Perspektive überfordert sich selbst, denn bei einem Prozessortakt von vielen Gigahertz kommt man selbst mit juristischem Prädikatsexamen mit den Notwendigkeiten, die das Datenschutzrecht eigentlich erfordern würde, nicht mehr mit.

Entstehungsgründe und Entstehungsvoraussetzungen

Die Erklärung für diese Perspektive ist rasch gegeben und der daraus folgende Regelungsansatz rasch erzählt und schlüssig: Das Datenschutzrecht ist vorangestürmt, als Privatheit und Digitalisierung begannen, in Konflikt zu geraten. Von der Ende der 1960er, Anfang der 1970er noch sehr diffusen Gefahr durch ›den Computer‹ hatte weder der Gesetzgeber noch die Wissenschaft noch das tagespolitische Schrifttum ein wirkliches Bild. Wahrscheinlich war es gerade dieses ungenaue, aber auch ungute Gefühl, das für die initiale und bis heute prägende Struktur des Datenschutzrechts maßgeblich war.

Die Datenschutzgesetzgebung und damit das Thema Datenschutz überhaupt kamen (in Deutschland) aufs Tapet, weil ein SPD-Politiker sich einen F.A.Z.-Leitartikel zu Herzen genommen hatte. Flankierend zum Ausbau der Kommunalen Gebietsrechenzentren (KGRZ.en) hatte der damalige hessische Ministerpräsident Albert Osswald das Gefühl, dem damals noch in den Windeln liegenden ›Großen Bruder‹ (im Orwell'schen Sinne) ein Gitterställchen spendieren sollen zu müssen. Weil es noch an einem Use Case und einer klaren Problemlage fehlte, setzte sich eine von den Rechenmaschinen her gedachte Konzeption durch, die in Bayern erst einmal EDV-Gesetz hieß, in Hessen, das damals ›vorn‹ war, aber namensgebend ›Datenschutz‹.

Technik- und Verfahrensregelungen

Weil anfangs die Gefahr, vor der der Datenschutz schützen sollte, aber noch diffus war und sich nur in solchen Bildern wie dem ›Großen Bruder‹ oder ›dem Computer‹ überhaupt transportieren ließ, war es folgerichtig, nicht bei der Gefahr (die man ja nicht richtig beschreiben konnte), sondern bei den anfassbaren Rechenmaschinen der Automatisierten Datenverarbeitung (ADV) und später dann Elektronischen Datenverarbeitung (EDV) anzusetzen. Und heute noch (und in der Datenschutzgrundverordnung (DSGVO) wieder etwas mehr) gibt es technik- und verfahrensbezogene Regelungen wie Zertifizierungen und die Datenschutzfolgenabschätzung.

Paternalistischer Ansatz

Der Datenschutz denkt nicht nur vom Datenverarbeitungssystem her, sondern auch von der (hierfür) ›verantwortlichen Stelle‹ bzw. ›Verantwortlichen‹, jedenfalls aber nicht von Betroffenen, die in kennzeichnend passivisierender Weise eben nur ›Betroffene‹ heißen. Diese bemutternde Terminologie, die in vielerlei Hinsicht den Geist der 1970er Jahre atmet, offenbart einen paternalistischen Ansatz, denn die Betroffenen treten in den Datenschutzgesetzen terminologisch nur als Betroffene (wenngleich durchaus auch mit Betroffenenrechten), nicht (auch) als Akteure in Erscheinung, es sei denn, sie entfernten sich mittels der ›Einwilligung‹ aus dem staatlich-klugen Schutzschirm der Datenschutzgesetze.

Handeln im Ungewissen

Bezeichnend für die damalige Unsicherheit darüber, was denn die Computer-Gefahr eigentlich sein soll, ist das Regelungsprinzip des Verbots mit Erlaubnisvorbehalt. Es ist ein Kennzeichen für ein Risikorecht, für ein Recht des Handelns im (Noch-)Nichtwissen.

Dies manifestierte sich in den ersten Datenschutzgesetzen in administrativen Genehmigungsvorbehalten (und nicht nur, wie heute, gesetzlichen Erlaubnisvorbehalten), die in den ganz alten Datenschutzgesetzen (und heute nur noch in Spuren) noch als technikrechtliche Fossilien entdeckt werden können. Die sind dem anlagenrechtlichen Ansatz der (letztlich preußischen) Dampfkesselgesetzgebung nachgebildet, wie wir sie heute etwa noch im Bundes-Immissionsschutzgesetz (BImSchG) finden. Dieser Ansatz ging und geht davon aus, dass bestimmte

Gerätschaften gefährlich und für die Umwelt potentiell schädlich sind. Deshalb sind sie zunächst einmal (präventiv) verboten und stehen unter einem Erlaubnisvorbehalt.

Aber schon bald begannen Computer sich derart zu verbreiten, dass dieser Regelungsansatz nicht mehr durchzuhalten war. Auch sein verdünnter Aufguss, die Melde- und Registerpflicht für Datenverarbeitungsanlagen, ist angesichts der Ubiquität nicht (mehr) praktikabel und fast überall nun abgeschafft.

Ebenfalls eine risikorechtliche Ausprägung zeigt sich im Selbstverständnis des Datenschutzrechts konzeptionell als Vorfeldschutz, nämlich im Vorfeld von Persönlichkeitsrechtsverletzungen, wie es ausdrücklich früher in § 1 Abs. 1 BDSG a.F. formuliert war.[1]

Umfassender Regelungsansatz

Ebenfalls aus der Entstehungszeit des Datenschutzrechts haben wir den Ansatz geerbt, dass die Datenschutzgesetze einen umfassenden Geltungsanspruch haben. Weil damals die informationellen Gefährdungen noch so unscharf und diffus waren (und man die Rechner noch abzählen konnte), ist es nachvollziehbar, dass die Regelungen für weitestgehend alle personenbezogene Datenverarbeitung gelten sollten.

Der – wie ich als Jurist sage – ›sachliche und personale Anwendungsbereich‹ kennt nur ganz wenige Ausnahmen. Genannt werden kann eigentlich nur noch das Medienprivileg (Art. 85 DSGVO) und die Haushaltsausnahme (Art. 2 Abs. 2 lit. c DSGVO). Auch das Ordens- (§ 86 BDSG) und Gnadenwesen kann ohne datenschutzrechtliche Erlaubnisnormen nicht mehr funktionieren. Für Gäste vom Mars mag es wie ein Witz klingen, dass selbst Spione datenschutzrechtlichen Bindungen unterliegen, ebenso in Zeiten größter Not sogar der Katastrophenschutz (wie sich an der deutschen Corona-Warn-App zeigt, die hohes Datenschutzniveau und geringe Nützlichkeit miteinander unglücklich kombiniert).

Noch eine Weiterung hat der Datenschutz in Gestalt des personenbezogenen Datums erfahren, das bekanntlich auch die personenbeziehbaren Daten umfasst. Was ursprünglich als ein Schutz vor Umgehung des Datenschutzrechts gedacht war, hat im Zeitalter weltweiter Vernetzung und Big Data nun zur Folge, dass kaum noch eine Datenverarbeitung nicht dem Datenschutzrecht unterfällt. Dies wird auch nicht durch den alten Glaubenssatz des Datenschutzes relativiert, dass es kein belangloses Datum gibt, wiewohl dieser Satz auch in seiner Umkehrung richtig ist, weil es kein Datum gibt, das in jedem Kontext von Belang wäre. Damit wird zu Recht betont, dass es auf den Kontext ankommt und dass abhängig von diesem jede Information eine Relevanz bekommen kann. Hieraus hat sich aber keine ernsthafte und praktikable Bagatellausnahme entwickelt. Was es freilich eher gibt, sind kontextabhängige Verschärfungen der Datenschutzvorgaben für sensitive Daten (Gesundheit, Geschlechtsleben sowie – offensichtlich ähnlich frivol – die Gewerkschaftszugehörigkeit).

Konzeptionelle Defizite des Datenschutzes

Das (geltende) Datenschutzrecht hat eine spezifisch verengte und verarbeiterzentrierte Mikroperspektive, die lediglich im Reflex betroffenenbezogen ist und Datenstrukturen ausblendet. Wie die Angabe der Herkunft einer Person verarbeitet wird, ist minutiös geregelt; für die (Nicht-)Abbildung von Merkmalen für Personen, Gruppen und die Gesellschaft in Datenbanken ist das Datenschutzrecht blind; für den Aspekt struktureller informationeller sowie symbolischer Gewalt fehlt dem Datenschutz die Perspektive.

Auch adressiert der Datenschutz nicht die Planung und Vorbereitung und damit nicht das ›schleichende‹ Entstehen von Datenagglomerationen, sondern er beschränkt sich situativ auf die Regelung der Nutzung der Datensammlungen im und auf einen Einzelfall. So wurde bei der Diskussion um das Registermodernisierungsgesetz (RegMoG) mit der Einführung einer einheitlichen Identifikationsnummer (ID-Nr.) in der rechtspolitischen Diskussion bis in die Sachverständigenanhörung hinein fast nur das Personenkennzeichen thematisiert, nicht aber die dahinterstehende Registertopographie.

Ferner begünstigt die unterschiedslose Regulierung von Datenverarbeitern, jedenfalls bei dem verfahrensbezogenen und damit bürokratischen Ansatz des geltenden Datenschutzrechts, die großen Anbieter und verstärkt sogar deren Datenmacht, weil kleinere Anbieter, die den Wettbewerb auch mit datenschutzfreundlichen Produkten befeuern könnten, hier Skalennachteile haben.

Die Glaubwürdigkeit des Datenschutzes leidet auch darunter, dass auf außergewöhnliche Situationen – wie etwa die Corona-Pandemie – und offensichtliche bürokratische Härten – etwa die Einführung der DSGVO selbst – nur mit Vollzugsdefizit wie dem zeitweisen Verzicht auf Bußgelder und Kontrollen reagiert werden kann.

Mesoperspektive von Privatheit

Einige dieser Defizite des deutschen und kontinentaleuropäischen Datenschutzrechts vermeidet eine privatheitsbezogene Betrachtung. Sie hat – zumal aus liberaler Perspektive – den Charme, dass sie vom Einzelnen her denkt, der also nicht nur ein bloß ›Be-

troffener‹ ist.

Individualisierung

Privatheit ist, wie das Persönlichkeitsrecht zeigt und die Informationelle Selbstbestimmung vorgibt, vom Individuum her konzipiert. Mit dem Denken vom Betroffenen einher geht die Vorstellung, dass Privatheit bzw. das von der Privatheit Geschützte unverrückbar und unveräußerbar der Person zugeordnet ist. Jedenfalls auf dieser Seite des Atlantiks werden Privatheit und Datenschutz jedoch nicht als Freiheit gedacht, sondern als Teil der Menschenwürde.

Es ist – noch liberaler – nämlich denkbar, Privatheit als individuelle Freiheit zu begreifen, dass also informationell jeder tun und lassen darf, was er möchte. Das würde dann auch die Möglichkeit eines Verzichts auf Privatheit bedeuten (wie es von den Vertretern der Post Privacy-Richtung ja tatsächlich auch vertreten wird). Und jedenfalls auf der anderen Seite des Atlantiks ist das ja durchaus auch die dogmatische Basis des Right to Privacy.

Übersteigert jedenfalls wird das Konzept der Privatheit, wenn man sie – wie es im politischen Bereich mit einer gewissen Portion an Pathos gerne geschieht – als ›digitale Souveränität‹ bezeichnet. Denn der Begriff der ›digitalen Souveränität‹ ist mehrdeutig und in Bezug auf Individuen eigentlich auch nicht recht passend. Wenn man informationelle Autonomie meint, sollte man diese auch so bezeichnen.

Kommerzialisierungspotential

Dieses unterschiedliche Verständnis von Privatheit manifestiert sich bei der ganz praktischen Frage, ob man mit Daten bezahlen kann, was ja die Geschäftsgrundlage der Großzahl der Dienste im Internet darstellt. Hier zeigt sich, dass die bewusste Entscheidung des deutschen und europäischen Datenschutzrechts, personenbezogene Daten nicht zu kommerzialisieren, dysfunktional sein kann.

Denn die datenschutzrechtliche Einwilligung verwirklicht die Privatautonomie insoweit und juristisch gesprochen nur auf der Ebene des Delikts, wonach ich mir informationelle Unverschämtheiten und Unerlaubtheiten verbitten kann. Ich kann also nur binär ›Ja‹ oder ›Nein‹ sagen, nicht aber ›Wie viel‹. Ökonomisch drückt dies ein Aushandeln des Austauschs von Daten gegen Dienste (Market Privacy), der ja prägend für die Internetökonomie ist, auf Steinzeitniveau, weil eine Preisbildung auf Seiten des Datenpreisgebenden erschwert wird. Betroffene haben rechtlich keine Möglichkeit, den ›Wert‹ ihrer Daten selbst zu bestimmen.

So sind bis heute keine Immaterialgüter an personenbezogenen Daten geschaffen worden. Dabei könnte dies ein Baustein eines umfassenderen Datenrechts sein und die Voraussetzung dafür, Lizenzen für die Nutzung von Daten zu erteilen und so das eigene Profil zu verwerten (oder jedenfalls rational entscheiden zu können, für bestimmte Internetinhalte dann eben einen höheren Preis in Geld zu zahlen). Dass ein solches marktgängiges ›Recht an den eigenen Daten‹ vielfältige Anschlussfragen auf den Gebieten des Verbraucherschutzes und des Datenverkehrsrechts aufrufen würde, sei hier nur angemerkt.

Konzeptionelle Defizite von Privatheit

Die Privatheitsperspektive, die vom Individuum her denkt, ist allerdings nur schlecht in der Lage, überindividuelle Aspekte zu erfassen. Insoweit teilt sie eine Schwäche mit dem Datenschutz.

Dies zeigt sich etwa am Rechtsschutz, der für die Einzelnen natürlich individuell ist. Der gerichtliche Rechtsschutz ist im Persönlichkeitsrechtsrechtsschutz (bislang) ganz auf das Individuum hin berechnet und vom Betroffenen her gedacht. Dies bedeutet aber auch, dass strukturelle Fragen auf diesem Wege nicht unmittelbar angegangen werden können. Selbst einem hartleibigen Aktivisten wie Maximilian Schrems gelingt es nicht, die rechtlichen Defizite des transatlantischen Datenverkehrs zu beenden, weil die Entscheidungen – den Regeln des Prozessrechts entsprechend – immer nur für den konkreten Fall und damit für eine begrenzte Konstellation gelten. Kollektive Durchsetzungsmechanismen gibt es bislang nicht. (Allerdings wird dieses Durchsetzungsdefizit durch die administrativen Einwirkungsbefugnisse der Datenschutzaufsichtsbehörden teilweise kompensiert.)

Makroperspektive auf informationelle Vermachtungen

Wegen der Fixierung auf die Datenverarbeitungsanlagen (= Datenschutz) und auf das Individuum (= Privatheit) haben lange Zeit weder das Recht noch dieses Graduiertenkolleg noch überhaupt kaum jemand die wachsende Datenmacht konzeptionell erfasst. Erst seit relativ kurzer Zeit realisieren wir, dass datenmächtige Akteure das Wissen (innerhalb einer Netzwerkgesellschaft) ›kuratieren‹. Ministerpräsident Osswald hat zwar das Gitterställchen des Datenschutzes aufgestellt, dort liegt auch noch das Spielzeug des ›Großen Bruders‹. Doch der selbst ist längst (und erst einmal unbemerkt) herausgeklettert.

Inzwischen hat die digitalpolitische wie auch die Fachdiskussion diese Konstellation erkannt und ändert bzw. erweitert ihre Perspektive. So werden im

Datenschutz neuerdings wieder stärker Regelungsaspekte betont, die auch einen gesamthaften Ansatz oder jedenfalls eine strukturelle Wirkung haben.

Struktureller Datenschutz

Dies sind etwa das Gebot der Datensparsamkeit – im Graduiertenkolleg dann sogar zu einer ›Datenfrugalität‹ gesteigert. Hierdurch soll dann eine Reduzierung der Datenfelder bewirkt werden, auch wenn sich solche Regeln regelungstechnisch nicht auf die Datenfelder, sondern die ›Befüllung‹ richten. Ebenfalls, obwohl als subjektiver Anspruch formuliert, ist das Recht auf Datenportabilität auf die Ermöglichung bzw. Wiederherstellung von Wettbewerb zwischen Anbietern gerichtet. Dies soll – so jedenfalls die optimistische Annahme – datenschutzfreundliche Regelungen stärken.

Kartellrecht

Aus juristischer und regulierungswissenschaftlicher Perspektive sehen wir ein verstärktes In-Stellung-Bringen des Kartellrechts – es sollen jetzt also die großen Jungs und harten Kerle die Sache richten anstatt der eher der Birkenstockfraktion zuzuordnenden Datenschutzbeauftragten.

Datenstrukturenrecht

Was mich kürzlich ein Forschungssemester lang beschäftigt hat, waren Regelungen von Datenformaten und Datenformatierungen. Dies kann mit dem einen Beispiel illustriert werden, dass es mir komisch vorkam, dass wir liebevoll ziselierte Regelungen zur Verarbeitung des Geschlechts als sensitives personenbezogenes Datum haben, die Definitionsmacht über das, was als Geschlecht informationstechnisch und informationell abgebildet wird, aber ungeregelt gelassen haben. Die Entscheidung des Bundesverfassungsgerichts (BVerfG) zum Dritten Geschlecht kratzt hier immerhin an der Oberfläche.

Konzeptionelle Defizite der Datenmachtperspektive

Eine gesamthafte Perspektive steht natürlich immer in der Gefahr, die Einzelnen und die unterschiedlichen Präferenzen von Einzelnen aus dem Blick zu verlieren. Ein Beispiel ist die Diskussion um die Corona-Warn-App: Hier mag es aus Seuchen- und Bevölkerungsschutzerwägungen gesamthaft sinnvoll sein, Nachverfolgungskomponenten u.ä. in die App einzubauen. Unterschiedliche Bereitschaften und Befindlichkeiten innerhalb der Bevölkerung finden dann aber keine Abbildung.

Holistische Perspektive

Wir betrachten also nicht nur die Textur einer Borke (Datenschutz), sondern stehen vor einem Baum (Privatheit), der Teil eines Waldes (Datenmacht) ist. Und erst wenn wir den ganzen Wald sehen, wissen wir, wohin er sich überhaupt und überall erstreckt. Und nur, wenn wir wissen, dass wir einen Wald vor uns haben, können wir sinnvoll beurteilen, ob wir den konkreten Baum, dessen Borke wir datenschutzrechtlich betrachtet haben, umhauen sollen oder ihn stehen lassen und einfach um ihn herumgehen. Auch können wir dann nur erkennen, wo es sich lohnt, eine Schneise durch den Wald zu schlagen. Um Wald, Baum und Borke als Ökosystem zu verstehen, braucht es einen gesamthaften Blick, der dann auch interdisziplinär sein muss. Wer einen Forst zu pflegen hat, muss Borke, Baum und Wald gleichermaßen im Blick haben. Die Kollegiatinnen und Kollegiaten als Adjunkten aus der höheren Lehranstalt für die Forsten der Privatheit, die unser Graduiertenkolleg gewesen war, werden deren Pflege nun an ganz verschiedenen Stellen in Wissenschaft und Praxis fortsetzen.

Prof. Dr. Kai von Lewinski

Inhaber des Lehrstuhls für Öffentliches Recht, Medien- und Informationsrecht
Sprecher des DFG-Graduiertenkollegs 1681/2 "Privatheit und Digitalisierung"

Endnote

1 Bundesdatenschutzgesetz, alte Fassung: »Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten *in seinem Persönlichkeitsrecht beeinträchtigt* wird.« (Herv. K.v.L.)