Nikolaus Forgó

Strukturwandel des Datenschutzes und des Datenschutzrechts – oder: alter Wein in neuen Schläuchen?[1])

Übersicht:

I. Einleitung

Die gestellte Frage nach einem „Struktur**wandel**" setzt voraus, dass die Struktur dessen, was sich möglicherweise wandelt, einigermaßen bekannt ist. Dieser Beitrag entfaltet (nur) das triviale Argument, dass dies nicht der Fall ist, weil Datenschutzrecht immer in Abgrenzung zu anderen Grundrechten betrieben wird und diese Abgrenzung in ihren Voraussetzungen und Folgen weiterhin unbestimmt ist.

II. Geschichte des Datenschutzrechts

1. Frühzeit

Als in den 60-er und 70-er Jahren des 20. Jahrhunderts auch außerhalb enger Fachkreise absehbar wurde, dass Computer die Welt verändern würden, begannen recht bald auch (einige) JuristInnen, sich für die neue Technologie zu interessieren. An deutschen juristischen Fakultäten trat eine Generation junger

[1]) Dies ist die Zusammenfassung und nachträgliche Verschriftlichung eines ausschließlich durch Folien unterstützten, ohne Manuskript gehaltenen freien Vortrags. Diese Form wurde beibehalten, auf vertiefende Nachweise daher weitgehend verzichtet.

Männer (Frauen waren an den Universitäten insgesamt im Professorenrang noch kaum vertreten), jenseits der tradierten Fächergrenzen, an, sich mit Informationstechnologie und ihrem Recht zu befassen. Dabei standen von Beginn an zwei Aspekte im Vordergrund: Einerseits ging es darum zu erforschen, wie die neuen Maschinen den JuristInnen helfen könnten, ihr Tun effizienter zu gestalten und damit der schon damals konstatierten Informationskrise des Rechts besser Herr zu werden.

Andererseits war schon bald deutlich, dass mit den neuen Möglichkeiten auch Gefahren einher gingen, weil durch die neu gewonnene Effizienz des Staates dieser auch besser seine Bürger überwachen konnte. Die Furcht vor der staatlichen Überwachung, kaum zwanzig Jahre nach Ende des Nationalsozialismus, ließ insb in Deutschland schnell das Datenschutzrecht als Nucleus von „Recht und IT" entstehen. Der Umstand, dass Computer riesige, teure, komplexe Maschinen waren, die sich an wenigen, ausgesuchten Stellen der öffentlichen Verwaltung befanden, legte nahe, das Primärziel des neu entstehenden Rechtsgebiets in der Sicherung der informationellen Selbstbestimmung gegenüber (wenigen) staatlichen Akteuren zu sehen. Volkszählung, Sozialversicherung, Steuerverwaltung sind die Themen und Instrumente einer automatisierten, effizienten Verarbeitung; Aussonderung, Verfolgung, Diskriminierung die Befürchtungen.

Aus dieser Schwerpunktsetzung heraus ist erklärlich, dass die erste Generation der „Rechtsinformatik" sich einerseits als Wissenschaft von der Informatik des Rechts (und somit als angewandte Informatik) verstand und andererseits als Wissenschaft von der Bewältigung der Datenschutzrisiken der (staatlich verwalteten) Informationstechnologie.

Viele der damals entstandenen datenschutzrechtlichen Prinzipien machen damals identifizierte Ziele wie Gefahren deutlich: Das Verbot mit Erlaubnisvorbehalt verbietet (in der Regel) jede Verarbeitung personenbezogener Daten, sofern nicht (ausnahmsweise) eine gesetzliche Grundlage oder eine informierte Einwilligung vorliegt. Der Zweckbindungsgrundsatz sieht vor, dass Daten nur für Zwecke verarbeitet werden dürfen, die mit den Zwecken, derethalben sie erhoben wurden, vereinbar (oder gar identisch) sind. Unabhängige Datenschutzbehörden sollen ex ante und mit Instrumenten der öffentlichen Verwaltung Rechtmäßigkeit garantieren und Gefahren einhegen.

In den 70-er Jahren entstand somit eine erste Schicht datenschutzrechtlicher Normen, die sich mitunter ausschließlich auf öffentliche Verarbeitungsvorgänge bezogen. Zu nennen ist insb das Hessische Datenschutzgesetz vom 7. 10. 1970, das sich schon aus kompetenzrechtlichen Gründen nur an die Landesverwaltung richtet.[2]) Zur ersten Generation der Datenschutzgesetze zählt insb auch das erste österreichische Datenschutzgesetz 1978, das jedoch, insoweit vorausgreifend, auch bereits inter privatos einen Grundrechtsschutz konstatierte, der im ordentlichen Rechtsweg geltend zu machen war.[3])

Die noch heute geltenden Grundsätze sind in diesen Gesetzen bereits angelegt.

---

[2]) http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1.

[3]) § 1 Abs 6 DSG 1978 in der Stammfassung, BGBl 1978/565.

Wenig später fasste das deutsche Bundesverfassungsgericht mit seiner Entscheidung zum Grundrecht auf informationelle Selbstbestimmung auch die schon seit Längerem diskutierten verfassungsrechtlichen Erwägungen zusammen. Wichtig ist dabei, dass das BVerfG sich nicht nur darauf beschränkte, ein Grundrecht zu konstatieren, das (ausdrücklich) im Grundgesetz nicht enthalten war, sondern sich dazu einer Ableitung aus Art 1 und Art 2 Abs 1 GG bediente – also buchstäblich von der Spitze der Verfassung weg argumentierte und ausführte: „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art 2 Abs. 1 GG in Verbindung mit Art 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

2. Mittlere Periode

Mit der raschen Verbreitung des Internets und der Verfügbarkeit von Rechnern in jedem Wohnzimmer begann eine zweite, nunmehr stark europäisch und europarechtlich geprägte Phase der datenschutzrechtlichen Regulierung, die insb in der RL 95/46/EG kulminierte und Teil eines größeren Unterfanges einer regulatorischen Einhegung des Internets (von elektronischen Signaturen über E-Commerce bis Urheberrecht) war. Hier war insoweit ein deutlicher Schwenk vollzogen, als nicht mehr primär Verarbeitungen durch öffentliche Stellen im Interesse standen, sondern zunehmend auch die tatsächlich wichtiger werdenden Verarbeitungen durch Private gleichberechtigt berücksichtigt wurden. Allerdings wurde dies weder zum Anlass genommen, die Instrumente der 70-er Jahre anzupassen, noch erst recht damit begonnen, die Frage systematisch zu vertiefen, ob die öffentlichrechtlich geprägten Schutzgedanken und Instrumente auch inter privatos zu greifen hätten. Insbesondere das Verbotsprinzip blieb weiterhin bestehen, wurde allerdings durch eine sehr umfassende Generalklausel samt Interessensabwägung auch inter privatos erst faktisch handhabbar gemacht.

Die akademische Durchdringung der Fragen scheiterte aus mehreren Gründen. Einerseits war es der Wissenschaft von der Informatik des Rechts – anders als etwa der Medizin- oder der Wirtschaftsinformatik – nicht gelungen, sich an juristischen Fakultäten zu etablieren. Andererseits entwickelte sich das Datenschutzrecht zu einer von einigen wenigen Spezialisten betriebenen Materie, die, wurde sie akademisch verortet betrieben, stets auch eine Orientierung in einem „Hauptfach" verlangte. Die Etablierung eines das Datenschutzrecht beinhaltenden, aber über dieses hinausgreifenden Informationsrechts als eigenes juristisches Fach, war entweder gar nicht versucht worden oder misslungen, von wenigen Ausnahmen abgesehen. Auf diese Situation traf nun ein Strom von aus Hauptfächern heraus betriebenen Modethemen und Begriffsunschärfen (von Cyberlaw bis Computerrecht), die zu einer systematischen Einhegung des Themas nicht geeignet waren.

3. Heute

Nach den intensiven Bemühungen der 90-er und 00-er Jahre, die in der RL 2002/58/EG und in der Kodifizierung des Grundrechts auf Datenschutz in der EU-Grundrechtecharta nochmals einen Gipfelpunkt fanden, trat dann eine Phase relativer Ruhe und Stagnation ein, die 2012 endete, als die Kommission den Vorschlag zur DSGVO erstmals präsentierte.

In dieser rechtlich vergleichsweise ruhigen Lage griffen jedoch umfangreiche Veränderungen im technischen Umfeld Platz. Waren in den 70-er Jahren wenige, teure Großrechner prägend, so wurden schon in den 90-er Jahren zunehmend Daten durch Private verarbeitet; allerdings fanden diese Datenverarbeitungen isoliert und unvernetzt statt. Von Festplatte bis Floppy-Disc oder CD, waren die Daten auf Datenträgern gespeichert, die physisch kontrolliert werden konnten und die Übermittlung personenbezogener Daten inter privatos war deshalb mehr die Ausnahme als die Regel. Erst mit dem Internet und – erst recht – mit dem Smartphone änderte sich dies. Der permanente, massenhafte, grenzüberschreitende Austausch (auch) personenbezogener Daten unter Privaten ist ein – auch gemessen an der Geschichte des Datenschutzrechts – vergleichsweise junges Phänomen. Das gilt auch für das damit einhergehende Entstehen weniger großer Unternehmen, die – zunehmend – alle Daten aller Lebensbereiche erfassen.

Diese faktischen Änderungen werden jedoch normativ kaum gespiegelt. Auch in der DSGVO sind die wesentlichen datenschutzrechtlichen Grundgedanken kaum verändert weiterhin beibehalten, insb Art 5 DSGVO enthält kaum weiterführende Prinzipien (mit Ausnahme des wenig neuen Grundsatzes der Accountability, Art 5 Abs 2 DSGVO). Weiterhin werden Transparenz, Treu und Glauben, Datenvermeidung, Richtigkeitsgewähr und Datensicherheit grundsätzlich gefordert, weiterhin findet sich ein Verbot mit Erlaubnisvorbehalt (Art 6 Abs 1 DSGVO) mit einer generalklauselartig weiten Öffnungsklausel qua Interessensabwägung (bei nicht sensiblen Daten, Art 6 Abs 1 lit f DSGVO) verbunden.

Jedoch werden durch das Recht und seine Grundsätze nun technische Verhältnisse geregelt, die sich sehr nachhaltig verändert haben: Cloud Computing, Big Data, Internet der Dinge, Always On, usw führen zu einer umfassenden Verarbeitung und Übermittlung von (auch personenbezogenen) Daten, die nicht mehr vor allem durch staatliche Behörden erfolgt und auch nicht mehr durch den Betroffenen (physisch) kontrollierbar ist.

In der universitären Bewältigung entstehen erneut Widersprüche. Während einerseits zahlreiche Digitalisierungsprofessuren und Cluster entstehen und kaum ein Strategiepapier ohne diesen Schwerpunkt auskommt, ist es andererseits schwieriger denn je zu erfassen, welche juristischen Kompetenzen hier erfasst und beherrscht werden müssen. „Digitalisierung" und „Vernetzung" durchdringen inzwischen unser ganzes Leben, wo und wie bedarf es daher einer separierten systematischen Erfassung? Nach meiner Meinung kann ein Grund nur in der Systematik zutage tretenden Durchdringung inhärenter Grundrechtskonflikte liegen. Damit wird Rechtsinformatik erneut zu einer (inter- und transdizsiplinär angelegten) Grundlagendisziplin.

III. Beispiele

1. Heterogenität

Der Komplexität und Geschwindigkeit der technischen Entwicklung mag auch geschuldet sein, dass die großen Versprechungen der DSGVO – Vereinheitlichung des Datenschutzrechts in Europa, Anpassung an die veränderten technischen Rahmenbedingungen und Universalität der Anwendbarkeit der Regeln – nur sehr eingeschränkt erreicht werden konnten. Es finden sich im Datenschutzrecht weiterhin nationalstaatliche Partikularismen erheblicher Zahl, die einerseits auf nationale Besonderheiten, andererseits auf eine große Zahl an Öffnungsklauseln im Kompromisstext der Verordnung zurückzuführen sind. Ein besonders krasses Beispiel für ersteres mag der Umstand sein, dass § 1 DSG weiterhin – unverändert – einen Grundrechtsschutz auch für juristische Personen vorsieht, obwohl schon aus der Überschrift der DSGVO deutlich wird, dass diese nur natürliche Personen erfassen will. Hintergrund ist hier der mit dem Datenschutzrecht nichts zu tun habende Umstand, dass es politisch nicht möglich war, die für eine Änderung von § 1 DSG erforderliche Verfassungsmehrheit zustande zu bringen, trotz dreier Anläufe.

Wie „offen" die DSGVO trotz ihres rechtsvereinheitlichenden Anspruchs geblieben ist, mag zeigen, dass allein in Österreich mehr als 300 Seiten des BGBl gefüllt wurden mit Datenschutz-Anpassungsgesetz 2018 (BGBl I 2017/120), Datenschutz-Deregulierungs-Gesetz (BGBl I 2018/24), Datenschutz-Anpassungsgesetz 2018 – Wissenschaft und Forschung (BGBl I 2018/31), Erstes Materien-Datenschutz-Anpassungsgesetz 2018 (BGBl I 2018/32) und Zweites Materien-Datenschutz-Anpassungsgesetz 2018 (BGBl I 2018/37). Rechnet man die hier notwendige Seitenzahl fiktiv auf alle Mitgliedstaaten hoch, gelangt man zu tausenden nationalen Gesetzblattseiten zur Anpassung an einen Rechtszustand, der der Vereinheitlichung hätte dienen sollen.

2. Verbot algorithmischer Entscheidungen

Hinsichtlich der Anpassung an die veränderten technischen Rahmenbedingungen stellen sich erhebliche Probleme. Nicht nur ist es trivialerweise so, dass europäisches Datenschutzrecht auf nichteuropäische Verantwortliche nur unter sehr eingeschränkten Bedingungen überhaupt anwendbar ist und ein Export europäischer Schutzstandards in das nichteuropäische Ausland spätestens dann nicht mehr goutiert wird, wenn daraus Normkonflikte mit dem Recht des Sitzstaats des Unternehmens einhergehen, sondern es treten technische Innovationen auf, die die tradierten Prinzipien insgesamt vor kaum bewältigbare Herausforderungen stellen. Ein besonders deutliches Beispiel mag hier Art 22 DSGVO sein, der es verbietet, zum Objekt einer ausschließlich automatisiert getroffenen Entscheidung zu werden.

Die Norm ist schon ob ihres kompromisshaften Charakters bemerkenswert. Das Verbot algorithmischer Entscheidungen gilt nämlich mitnichten absolut,