Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Weichenstellung“
–
In welcher digitalen Welt leben wir?

CCC-Kongress

Berlin, den 30. Dezember 2019

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,
liebe CCCler,

im Bereich des Datenschutzes und im Bereich der Informationsfreiheit werden derzeit schwer umkehrbare Weichenstellungen vorgenommen, die weitreichende Konsequenzen für unsere Gesellschaftsordnung haben.

Als Bundesdatenschutzbeauftragter setze ich mich mit der Durchsetzung der Datenschutz-Grundverordnung, der Regulierung von Verbraucher-Scoring und –Profiling, zahlreicher bereichsspezifischer Gesetzgebung und der Weiterentwicklung des europäischen Datenschutzrechts auseinander.

Besonders beschäftigen mich dabei auch die Debatten um digitale Überwachung und massiv ausgeweitete Befugnisse der Sicherheitsbehörden.

Ich will, dass auch die digitale Gesellschaft eine freiheitliche, liberale und diverse Gesellschaft ist.

Dabei sind aus meiner Sicht technische und ökonomische Aspekte genauso zu berücksichtigen wie datenschutzrechtliche und gesellschaftspolitische.

Die stattfindenden und kommenden Weichenstellungen der digitalpolitischen Debatte in Europa leben von Vergleichen und der Konzentration auf technische und ökonomische Aspekte. Immer wieder kommt bspw. der Hinweis auf die weit entwickelten Digitalökonomien in China oder den USA, deren Vorsprung im Bereich bspw. der KI-Technologien als quasi „uneinholbar“ und wohlstandsgefährdend beschrieben wird.

Dies soll als Druckmittel für eine schnelle und wirtschaftlich möglichst ertragreiche Entwicklung neuer Modelle der Datenverwertung mittels KI genutzt wird.

Zweifelsohne bewegen sich China oder die USA in manchen Sektoren in anderen Phasen der technologischen Entwicklung, zumindest aber der Einführung und verfügen dort über deutlich höhere finanzielle Mittel, staatlich und privat, als wir in Europa.

China arbeitet bekanntlich gerade daran, mithilfe von Künstlicher Intelligenz und Social Scoring ein gigantisches Kontrollsystem aufzubauen, das den althergebrachten Polizeitstaat zur vollen Blüte bringen soll.

Hierbei wird das Verhalten jedes einzelnen Bürgers sowohl im Netz als auch im digital verschränkten realen Leben genau unter die Lupe genommen und ausgewertet. Wer sich im Sinne des Systems verhält, dem winken Prämien. Wer aber nicht dem Bild eines Musterbürgers entspricht, der muss mit Sanktionen rechnen. Spannend, wer diese Standards setzt und wie diese auch wechseln können. Man kann sich nie unbeobachtet fühlen und nie sicher sein, wie das eigene Verhalten interpretiert werden wird.

Das ist eine Entwicklung, die in Europa nur eine Minderheit will, auch wenn eine Studie interessanterweise unter jungen Menschen eine bestimmte Zustimmung ermittelt. Wir sollten das auch nicht in Teilbereichen akzeptieren. Weder vom Staat, noch von privaten Konzernen. Also weder das chinesische, noch das US-amerikanische Modell.

Aber wir sehen doch, wie dieses Überwachungsgift in unsere Gesellschaft einträufelt, weil es so einfach technisch möglich geworden ist. Weil Sensoren, Speicher und Verarbeitungsmöglichkeit immer besser, schneller und billiger werden.

Wir sehen, wie der Vorrang für Geschäftsmodelle der Verlage gefordert, Komfort gegen Daten getauscht, Sicherheit vor Freiheit gesetzt wird. Die Bewertung von Verhalten und Gesinnung beherrscht Debatten über Geschäftsmodelle und Sicherheitsgesetzgebung.

Im Zentrum: KI

Im Zentrum der technologischen Entwicklung stehen dabei Methoden, die – meist ziemlich ungenau – als KI zusammengefasst werden.

Wir haben deshalb als Datenschutzbeauftragte in der Hambacher Erklärung und in der Datenethikkommission für die KI wichtige Leitsätze beschrieben, die bei uns gelten sollen:

- KI darf den Menschen nicht zum bloßen Objekt machen.
- KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben.
- KI muss transparent, nachvollziehbar und erklärbar sein
- KI muss Diskriminierungen vermeiden
- Auch für KI gilt der Grundsatz der Datenminimierung
- KI braucht Verantwortlichkeit
- KI benötigt technische und organisatorische Standards

Ist es nicht absurd, dass hier in Deutschland, wo wir Erfahrung mit Datenschutz haben und diesen aus den Grundrechten ableiten, von Wirtschaftsverbänden und Politik über Datenschutz als Wettbewerbshindernis gejammert wird, während in den USA, mehr oder minder glaubwürdig, Firmen zunehmend mit Datenschutz für sich werben? Weil diese Firmen verstanden haben, dass Vertrauen die entscheidende Währung im Digitalzeitalter sein wird.

Von Wirtschaft, vielen Tekkies und großen Teilen der Politik steht der immer gleiche Wunsch weit oben auf der Agenda: Deutliche Erhöhung der Menge an nutzbaren, qualitativ hochwertigen Daten im Rahmen innovativer IT-Anwendungen, um dadurch eine Optimierung von Prozessen in fast allen Lebensbereichen zu ermöglichen und im Wettlauf der digitalen Entwicklung mitzuhalten.

Das lehne ich keineswegs ab. Ich will aber noch etwas: Die Absicherung, dass Persönlichkeitsrechte, das Recht auf informationelle Selbstbestimmung und andere Grundrechte nicht verletzt werden.

Eine Regulierung von KI, von algorithmischen System, sollte da erfolgen, wo Gefahren für die Rechtsgüter des Einzelnen oder der Allgemeinheit drohen. Das haben wir als Gesellschaft schon immer so gemacht. Bei Dampfkesseln, medizinischen Geräten und Handys. Das muss auch im Software-Zeitalter gelten.

Dies betrifft beispielsweise das Verbot von Algorithmen mit unvertretbarem Schädigungspotenzial. Für den Einsatz algorithmischer Systeme ist also ein risikoadaptierter Regulierungsansatz zu wählen, der sich am Schädigungspotenzial des algorithmischen Systems ausrichten. Das bedeutet, dass alle Komponenten einer algorithmischen Anwendung, einschließlich aller beteiligten menschlichen Akteure bei der Bewertung berücksichtigt werden müssen.

Datenschutz soll technische Innovationen möglich machen, gleichzeitig aber eben auch Fehlentwicklungen vorbeugen. Auch der datenschutzrechtliche Grundsatz der Datenminimierung ist für die Weichenstellung zum Einsatz innovativer Systeme obligatorisch zu berücksichtigen.

Niemand hat das Recht, personenbezogene Daten zu erheben, die er nicht für die eigentliche Dienstleistung benötigt. Ein äußerst sinnvolles Instrument liegt bspw. in der situationsgerechten Anonymisierung oder Pseudonymisierung personenbezogener Daten. Auch Modelle dezentralen Lernens oder datenschutzkonforme data spaces ermöglichen viele Formen der Datennutzung in der KI.

Allzu oft wird der Datenschutz polemisch als ein „Bremsschuh für Innovationen“ bezeichnet. Datenschutz bremse technologischen Fortschritt und wirtschaftliche Entwicklung oder schrecke Investoren ab, so das falsche Mantra. Laxere Datenschutzvorgaben sollen Deutschland und Europa den technologischen Vorsprung von USA und China aufholen lassen.

Da habe ich eine Gegenfrage: Wer glaubt denn wirklich, als Silicon Valley 2 oder China 2 erfolgreich sein zu können?

Wir brauchen für die Digitalisierung einen europäischen Weg, der unsere Werte widerspiegelt und mit dem wir in den wissenschaftlichen, technologischen, gesellschaftlichen und wirtschaftlichen Wettbewerb eintreten.

Google – besonders Android –, Facebook & Co. (und schleichend auch die chinesischen Anbieter mit ihren auf einem riesigen Heimatmarkt erprobten Angeboten) sammeln unter Standardeinstellungen fast ungehemmt persönliche Daten und schränken somit die Privatsphäre der Benutzer ein.

Auch wenn viele große Anbieter ihre Datenschutzrichtlinien vereinheitlichen und formal deklarieren, DSGVO-compliant zu sein, bedeutet dies in Wirklichkeit keinen aktiven Schutz der Privatsphäre des Nutzers.

Letztlich muss jeder Nutzer ein technisches Know-how mitbringen, um die diversen Optionseinstellungen zu finden und derart zu handeln, dass ein bestimmter Service seinen persönlichen Belangen entspricht. Aus dem Prinzip Opt-in wurde vielfach in der Praxis Opt-out.

Dieses Know-how ist hier im Saal sicherlich vorhanden, für die allermeisten „Normal-User“ gilt dies aber keinen Fall. Und über Drittangebote wird mittels Trackingtools, Plugins und SDK auch außerhalb der eigenen Angebote das Profil der Nutzerinnen und Nutzer vervollständigt.

Viele Funktionen lassen sich gar nicht ausschalten, d.h. bei der Nutzung von bestimmten Systemen werden zwangsweise Daten an die Server der Anbieter gesendet. Ein „technisches Abschalten“ ist nicht vorgesehen.

Wir brauchen hier die Durchsetzung bestehenden Rechts, Zertifizierung und Labeling datenschutzfreundlicher Angebote und mehr digital literacy, also bewusstere Auswahl und Nutzung von Angeboten.

Auch der technische Schutz durch PMT und PIMS ist wichtig. Anbieter müssen diese Standards dann aber auch bedienen und einhalten. Wer den Do-not-Track-Standard ignoriert, muss sich über die Forderung nach gesetzlichen Verboten nicht wundern.

Ein wichtiger Schritt wäre aus meiner Sicht außerdem die Pflicht zur – datenschutzfreundlich ausgestalteten - Interoperabilität bzw. Interkonnektivität in bestimmten Sektoren – etwa bei Messenger-Diensten und sozialen Netzwerken. Sie könnte dazu beitragen, die Olipolisierung in diesem Bereich aufzuheben und Markteintrittsbarrieren für neue Anbieter zu senken. Dies wäre auch eine Voraussetzung dafür, bestimmte Basisdienstleistungen der Informationsgesellschaft in Europa neu aufzubauen bzw. zu stärken.

Ein so ausgestalteter Datenschutz könnte zu einem wichtigen Differenzierungsmerkmal im globalen Markt werden.

Datenschutz durch Technikgestaltung und Voreinstellung sollte bei uns von Anfang an als Kernbestandteil beim potenziellen Einsatz neuer Systeme und neuer Software implementiert werden. Die öffentliche Hand könnte durch Vergabe und Förderung datenschutzfreundlicher Angebote, z.B. einen Messenger der deutschen Verwaltung auf Basis bestehender Open-Source-Systeme, Vorbild sein.

Aus Sicht des technologischen Datenschutzes unterliegen alle Systeme – unabhängig ob innovative Technologien wie KI/Blockchain, Betriebssysteme oder Alltagsgegenstände – **den gleichen Regeln und der gleichen Aufsicht. Es gibt keine rechtsfreien Räume. Im Rahmen meiner Zuständigkeit werde ich dies bei entsprechenden Kontrollen prüfen und im Rahmen meiner Befugnisse ggfs. entsprechend beanstanden und transparent darstellen.**

Aufgrund der Unabhängigkeit meiner Behörde schließen diese Kontrollen auch Sicherheitsbehörden ein.

In diesem Bereich wachsen unsere Kontrollbefugnisse auf Grund der immer neuen Sicherheitsgesetze sogar an. Wobei ich an dieser Stelle wieder einmal deutlich machen muss, dass wir seit drei Jahren auf eine europarechtskonforme Ausgestaltung des Bundespolizeigesetzes warten.

Es ist schön für meine Behörde, dass wir wegen der laufenden Sicherheitsgesetzgebung zusätzliches Personal bekommen; die immer neuen Befugnisse für die Sicherheitsbehörden sind aus meiner Sicht schon deswegen nicht notwendig, weil die Behörden selbst die schon vorhandenen Instrumente kaum nutzen.

Es fehlt in der Regel nicht an den Instrumenten sondern am geschulten Personal. Immer wieder stellen sich Datensammlungen auch als weitgehend irrelevant für die Arbeit der Sicherheitsbehörden da.

Besser wäre also ein Sicherheitsgesetz-Moratorium, eine Evaluierung der seit 2001 beschlossenen Gesetze und nicht ein Immer-Mehr.

Das täte den Bürgerrechten und der Sicherheit gut.

Weitere grundsätzliche politische Aspekte:

Regulierung versus Digitalisierung? – Regulierung dient dem Schutz der Grundrechte!

Noch einmal: Starker Datenschutz ist unabdingbar für eine ethische und gerechte Ausgestaltung unserer digitalen Zukunft. Es ist außerdem ein Irrglaube, dass es der Digitalisierung helfe, möglichst wenig zu regulieren und bestehende Regulierungen/ gesetzliche Vorgaben weitestgehend abzuschaffen.

Regulierung dient dazu, die Werte unserer Rechtsordnung zu gewährleisten und Grundrechte zu schützen. Daher muss Regulierung insbesondere dort ansetzen, wo die Gefahren für die Rechtsgüter besonders hoch sind. Nachschärfung im Datenschutzrecht muss dort ansetzen, wo Gefahren für die Rechtsgüter des Einzelnen oder der Allgemeinheit drohen. Dies betrifft beispielsweise klarere Vorgaben und mehr Transparenz bei Profilbildungen, das Verbot von Algorithmen mit unvertretbarem Schädigungspotenzial oder spezifische Regelungen zum Datenhandel.

Die Datennutzungen sind heute so komplex und umfassend geworden, dass der Einzelne häufig nicht mehr in der Lage ist, einen Überblick über die Nutzung seiner Daten zu gewinnen und viele dies lieber gar nicht mehr versuchen und „aufgeben“.

Datenschutzhinweise werden gar nicht mehr gelesen und es wird einfach zu allem ein Einverständnis erteilt. Oder mancher Bürger – gerade der älteren Generation – verzichtet aus Angst vor Datenmissbrauch gar ganz auf digitale Teilhabe.

Beides kann nicht die Lösung sein. Weder digitaler Fatalismus noch digitale Askese. Vielmehr sollten gezielte Transparenzpflichten und klare Grenzen für das Erlaubte den Bürgerinnen und Bürgern ihre digitale Selbstbestimmung über ihre Daten zurückgegeben.

Scoring und Profiling – Nachschärfung erforderlich

So fordert der BfDI im Bereich von Profilbildung und insbesondere Scoring seit Jahren eine wirksamere Regulierung und mehr Transparenz. Die Bildung von persönlichen Profilen sowie deren kommerzielle und politische Auswertung werden in Zukunft sogar eine immer größere Bedeutung haben.

Obwohl diese Entwicklung diverse datenschutzrechtliche Grundprinzipien herausfordert – z. B. das Gebot der Datenminimierung und das der Zweckbindung – bleibt die DSGVO gerade in diesem Punkt vage und weitgehend auf dem Stand von 1995. Bei den Verhandlungen zur Schaffung der DSGVO ist es leider nicht gelungen, die Bildung von Profilen und das Scoring einer modernen europäischen Regelung zuzuführen. Hier sollten wir die Evaluierung für einen neuen Anlauf nutzen.

Ziel der Neuregelungen sollte eine Verschärfung des geltenden Rechtsrahmens sein, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen. Die betroffenen Personen sollten von einem größeren Maß an Transparenz bezüglich der erstellten Profile profitieren und zugleich eine größere Kontrolle über die Verarbeitung ihrer Daten zur Profilbildung erhalten.

Diesen Forderungen hat sich auch die Datenethikkommission angeschlossen.

Informations- und Transparenzpflichten – Einzelne Praxiserleichterung denkbar

Bei den Informations- und Transparenzpflichten nach Art. 13 und 14 DSGVO haben sich in der Praxis aber auch vermehrt Umsetzungsprobleme gezeigt.

Es wurden Bedenken geäußert, dass die Erfüllung der Informationspflichten für Verantwortliche (v.a. KMU bzw. Start-Ups) möglicherweise zu aufwendig sei.

Die Aufsichtsbehörden befürworten grundsätzlich einzelne Praxiserleichterungen, warnen aber vor generellen Ausnahmen. Denn auch kleine Einrichtungen können Datenverarbeitungen vornehmen, die tiefergreifende Auswirkungen für die betroffenen Personen haben.

Beispiel für Erleichterung: Bei der telefonischen Datenerhebung oder beim sog. Medienbruch könnte eine allgemeine Information an zentraler Stelle ausreichen. Daneben könnten auch Art und Umfang der Informationspflichten anwendungsfreundlicher gestaltet werden.

Unsicherheit in vielen Unternehmen - Auslegungshilfen durch DSK und Guidelines auf europäischer Ebene

In deutschen Unternehmen besteht teilweise noch immer eine große Rechtsunsicherheit, die beseitigt werden muss. Hierfür dient auch die Sensibilisierung und Aufklärung durch die Aufsichtsbehörden.

So formulierte die DSK als Hilfe bei der Anwendung bereits sehr frühzeitig eine Vielzahl von Kurzpapieren zur Auslegung zentraler Vorschriften der DSGVO und Orientierungshilfen für den Umgang mit typischen Anwendungsszenarien. Beispielsweise die Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten oder die zu Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung.

Der europäische Datenschutzausschuss EDSA hat nunmehr auch bereits eine Reihe von umfangreichen Leitlinien verfasst, die den Anwendern, aber auch den Betroffenen Hinweise zur Auslegung und Anwendung geben. Weitere sind in Arbeit und werden folgen.

Nachschärfung bei Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen erforderlich

Die Verpflichtungen, die Datenverarbeitung datenschutzfreundlich zu gestalten (Art. 25 DSGVO), bringt grundsätzlich einen entscheidenden Vorteil für die europäische Digitalwirtschaft. Data protection by design findet allerdings leider in der Praxis kaum Resonanz.

Denn die DSGVO stellt mit data protection by design und by default zwar Grundsätze auf, die sich in der Sache an die Hersteller selber richten, nimmt diese aber nicht als Verantwortliche in die Pflicht.

Datenschutz muss bereits vor und während der Produktentwicklung dafür sorgen, dass Verbraucherfreundlichkeit und Schutz der personenbezogenen Daten Teil der Produktentwicklung werden. Deshalb ist es notwendig, nicht nur diejenigen Unternehmen und Behörden in die Verantwortung zu nehmen, die IT-Produkte und -Verfahren einsetzen, sondern es müssen auch die Hersteller in die Pflicht genommen werden.

Es bleibt also noch jede Menge zu tun und ich bin sicher, dass auch Sie alle mich und meine Behörde dabei weiter wohlwollend kritisch begleiten werden, was ich sehr begrüße.

Wir brauchen Sie als Unterstützerinnen und Unterstützer, als Kritikerinnen und Kritiker, als Beispielgeberinnen und Beispielgeber für datenschutzfreundliche Technologien und auch als Mitarbeiterinnen und Mitarbeiter. Ich finde, auf der hellen Seite der Macht ist man gut aufgehoben.

Ich danke Ihnen für Ihre Aufmerksamkeit und wünsche uns allen einen guten Verlauf dieses Kongresses.