Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Key Note

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Fremdbestimmung durch Digitalisierung, Künstliche Intelligenz, Algorithmen?“

bei SPD-Bundestagsfraktion
1 Jahr DSGVO

Deutscher Bundestag, Reichstagsgebäude, Otto-Wels-Saal 3. Etage,
Raum 3 S 001, Berlin, Freitag, den 7. Juni 2019

12.00 bis 16.30 Uhr

Es gilt das gesprochene Wort

Liebe Genossinnen und Genossen,

sehr geehrte Damen und Herren,

I. Einführung

Ich danke herzlich für die Einladung in meine alte Fraktion. Es ist ein gutes Gefühl, hier an meiner früheren Wirkungsstätte mit vielen Freundinnen und Freunden gemeinsam über die Zukunft des Datenschutzes nachzudenken.

Es freut mich, hier mit Ihnen und mit Euch meine ersten Erfahrungen aus nicht einmal einem halben Jahr im Amt des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auszutauschen.

Ich bin mir sicher, dass wird nicht die letzte Gelegenheit zu einer intensiven Diskussion sein.

Bevor ich in die Abgründe von Algorithmen und Künstlicher Intelligenz klettere, möchte ich doch ein paar Anmerkungen zum Thema der Tagung **„1 Jahr DSGVO“** machen. Wir werden sehen, wie eng beide Bereiche **– neue rechtliche Rahmenbedingungen und wachsende technische Herausforderungen** - miteinander verwoben sind.

II. DSGVO: Erste Erfolge und bleibende Herausforderungen

Der Start der DSGVO war - mit dieser Feststellung trage ich hier sicher Holz in den Wald – ziemlich ruckelig; Man kann auch neudeutsch sagen „**suboptimal**“.

Trotzdem möchte ich Sie und Euch davon überzeugen, dass die Grundverordnung eine gute Sache ist. Sie hat schon Gutes bewirkt – und sie kann noch mehr.

Dazu drei Stichpunkte:

1. Die DSGVO war überfällig und sie leistet schon in ihrem ersten Jahr viel für einen wirkungsvolleren Datenschutz,
    - national
    - auf EU-Ebene
    - und weltweit

2. Die DSGVO muss die technologischen Herausforderungen meistern. Beispiele:
    - Künstliche Intelligenz
    - Algorithmen

3. Der Datenschutz und die mit ihm befassten Aufsichtsbehörden sind auf die Vernetzung mit anderen Politikbereichen angewiesen.

Zu 1.
Erste Erfolge national und international

1.1. Nationale Erfolge

Vor einem Jahr, genau am 25. Mai 2018, wurde die Grundverordnung nach einer Übergangsphase von 2 Jahren „scharf gestellt“.

Das Internet war voll mit gezielt verbreiteter Verängstigung, aber auch glatten Fehlinformationen. Eine Abmahnwelle wurde heraufbeschworen – ein Tsunami an Kostenbescheiden und Bußgeldern gegen kleine Unternehmen und an Vereine zog am dunklen Horizont herauf.

Heute wissen wir: Viele dieser Besorgnisse und Ängste waren unbegründet oder zumindest deutlich überzogen.

Manche Unsicherheiten konnten durch die hervorragende Aufklärungsarbeit der Aufsichtsbehörden gerade gerückt werden. **Dank auch an die Kolleginnen und Kollegen der Länder.**

Angesichts noch immer bestehenden Befürchtungen und Vorurteile möchte ich daran erinnern: Erst auf der Grundlage der DSGVO haben die Betroffenen

- mehr Kontrolle
- und Transparenz bei der Datenverarbeitung erlangt,

und das ist gerade im digitalen Zeitalter von großer Bedeutung.

Die DSGVO „schlägt an“. Das zeigt sich u.a. am Beschwerdeverhalten der Menschen.

Es gibt eine spürbar steigende Bereitschaft, die neuen Rechte in Anspruch zu nehmen. So erreichten meine Behörde vom 25. Mai bis zum

Ende des letzten Jahres 6.507 allgemeine Anfragen und 3.108 schriftliche Beschwerden. Das waren binnen sieben Monaten mehr als doppelt so viele wie im gesamten Jahr 2017. Zudem wurden dem BfDI seit Anwendungsbeginn der DSGVO etwa 7.300 Datenschutzverstöße von öffentlichen Stellen des Bundes, Post- und Telekommunikationsunternehmen gemeldet.

Eine deutliche Steigerung verzeichnen auch die Aufsichtsbehörden der Länder. Auch dort haben die **Beschwerden, allgemeinen Anfragen und Meldungen von Datenschutzverstößen** erheblich zugenommen.

Das macht viel Arbeit – ist aber wichtig und ein gutes Zeichen. Es ist eine gewaltige Herausforderung für die Aufsichtsbehörden, dieses Vertrauen in ihre Arbeit nicht zu enttäuschen.

Zu einer bürgernahen Umsetzung des Datenschutzrechts gehört auch eine kritische Sicht auf Mängel und Unzulänglichkeiten. Auch hier müssen wir auf die Menschen hören und ihre Einwände aufnehmen. Auch ich sehe manche bürokratische Überregulierung kritisch – sie gehört auf den Prüfstand. Es geht nicht darum, ehrenamtliche Vereinsvorstände und Start-Ups mit unnötiger Verwaltungsarbeit zu verärgern. **Die opfern genug Freizeit zum Wohl der Allgemeinheit.**

Wo Bürokratie zum Selbstzweck wird und für den effektiven Schutz personenbezogene Daten nichts bringt, muss sie eingedampft werden!

Die DSGVO hat diesen Optimierungsprozess im Übrigen selbst geplant. Vorgesehen ist eine Evaluierung bis zum Jahre 2020, an der ich mich sehr engagiert beteilige. Die Europäische Kommission ist nach Art. 97

DSGVO gehalten, die Aufsichtsbehörden in den Evaluierungsprozess einzubeziehen. Deshalb haben die deutschen Aufsichtsbehörden einen Unterarbeitskreis eingerichtet, der den Evaluierungsbedarf zu ermitteln und die entsprechenden Schlussfolgerungen zu ziehen. Auf diese Weise werden wir gut vorbereitet sein, wenn die Kommission die Aufsichtsbehörden in den Evaluierungsprozess einbezieht. Ich hoffe auf einen Erfolg dieses Prozesses.

Bei der Evaluierung stehen natürlich nicht (nur) Erleichterungen für KMU, Vereine und Ehrenamtliche im Mittelpunkt, sondern auch Verbesserungen des Datenschutzes:

Mit Blick auf die Zeit möchte ich hier vor allem zwei Punkte herausgreifen:

- Die Bildung von Profilen und deren Auswertung ist eines der zentralen Themen der Zeit. Die Werkzeuge der Datenverarbeitung ermöglichen das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten. Verbunden mit immer weiter verfeinerten Möglichkeiten des Einsatzes selbstlernender Mechanismen eröffnet dies vielfältige Möglichkeiten, Verhalten von Einzelnen (vermeintlich) vorherzusagen und ggf. zu steuern. Obwohl diese Entwicklung diverse datenschutzrechtliche Grundprinzipien herausfordert – z. B. das Gebot der Datenminimierung oder die Zweckbindung – bleibt die DSGVO gerade in diesem Punkt vage und weitgehend auf dem Stand von 1995. Bei den Verhandlungen zur Schaffung der DSGVO war es nicht gelungen, die Bildung von Profilen und das Scoring einer modernen europäi-

schen Regelung zuzuführen. Hier sollten wir die Evaluierung für einen neuen Anlauf nutzen.

- Der zweite Punkt betrifft die Verpflichtung zum Einsatz datenschutzfreundlicher Technologien. Warum setzt diese erst bei den datenschutzrechtlich Verantwortlichen an, d. h. den Unternehmen oder der Behörde, die die Technologie nutzen? Sie haben in manchen Fällen gar keine oder nur eine geringe Auswahl, welche IT sie verwenden. Wäre es deshalb nicht eher zielführend, hier viel früher, nämlich bei den Herstellern von IT-Verfahren und -Produkten anzusetzen? Auch hierzu hatte es bereits bei den Verhandlungen zur DSGVO Vorschläge gegeben, die ich gern wieder aufgreifen würde.

1.2 DSGVO wirkt auf der internationalen Ebene

Die globale Vernetzung in allen Bereichen lässt die Spielräume für nationale Politik deutlich schrumpfen.

Wir können das auch positiv formulieren und uns darüber freuen, dass mit der DSGVO der Grundstein dafür gelegt wurde, auch auf internationaler Ebene mit einem den Menschenrechten verpflichteten Datenschutz voran zu kommen.

- **DSGVO wirkt international in zwei Richtungen:**
    - Zum einen ist sie ein Exportschlager, der in die Rechtsordnung anderer Länder ausstrahlt.
    - Die DSGVO wirkt auch über den EU-Raum hinaus unmittelbar.

An der DSGVO **orientieren sich nach und nach auch andere Weltregionen.** Die Entwicklungen in Japan, aber auch das hohe Interesse weiterer Staaten in Lateinamerika und Asien belegen dies eindrucksvoll. Besonders freut mich der **"California Consumer Privacy Act".** Unternehmen müssen dann ab dem 1. Januar 2020 offenlegen, welche Kunden- und Nutzerdaten sie speichern. Kalifornien ist der Sitz zahlreicher Technologiekonzerne, Von daher hat das neue Gesetz eine wichtige Pilotfunktion. **Die USA sind glücklicherweise nicht nur Donald Trump!**

Das substantiell Neue an der DSGVO ist, dass sie auch außerhalb der EU gilt.
Sie verbessert vielfach den Rechtsschutz gerade auch für die Datenverarbeitungen beispielsweise in den USA.

Im Vergleich zur alten Datenschutzrichtline von 1995 hat die DSGVO nach Artikel 3 einen deutliche erweiterten räumlichen Anwendungsbereich.

~~Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung wird in Art. 3 DSGVO geregelt. Er ist deutlich weiter gefasst als in der früheren Datenschutzrichtlinie der EU aus dem Jahre 1995.~~

Erfolgt die Verarbeitung personenbezogenen Daten im Rahmen einer Tätigkeit einer Niederlassung innerhalb der EU, gilt die Grundverordnung. Dabei ist es nicht einmal erforderlich, dass die Verarbeitung der personenbezogenen Daten innerhalb der EU stattfindet. Sie muss lediglich im Rahmen einer Tätigkeit innerhalb der EU erfolgen.

Das hört sich alles sehr abstrakt an, ist aber praktisch höchst bedeutsam. Hat also die Firma XY eine Zweigstelle oder Filiale in der EU, in der Daten verarbeitet werden können, gilt die Grundverordnung.

Richtet beispielsweise Google in einem EU-Lande ein Büro ein, gilt für dessen Datenverarbeitung die EU-DSGVO.

Es geht aber noch weiter. Bietet ein Unternehmen Waren und Dienstleistungen in der EU an, muss es sich an das europäische Datenschutzrecht halten. Dabei spielt es keine Rolle, obwo das Unternehmen seinen Sitz irgendwo in der weiten Welt hat. Besteht ein tatsächliches Angebot für EU-Länder, gilt die DSGVO.

Wir sehen also, die DSGVO schützt auch personenbezogene Daten im nichteuropäischen Ausland. Es wird eine enorme Herausforderung für die Datenschutz-Aufsichtsbehörden sein, diese neuen Regelungen auch durchzusetzen.

~~Die DSGVO fragt nicht nach der Staatsangehörigkeit der Betroffenen, auch nicht nach dem Ort, an dem die Datenverarbeitung erfolgt. Entscheidend für ihre Geltung ist entweder die Niederlassung oder der Aufenthaltsort des Betroffenen. Gibt es von dort aus einen tatsächlichen Zusammenhang zur Verarbeitung von personenbezogenen Daten, gilt die DSGVO - auch außerhalb der EU.~~

~~Auch Unternehmen, die trotz fehlender Niederlassung in der EU auf dem europäischen Markt tätig sind, müssen für alle Aktivitäten, die damit in~~

~~Zusammenhang stehen, die DSGVO anwenden und befolgen. Unternehmen aus Drittstaaten müssen sich unter Umständen höheren Anforderungen unterwerfen, als es ihr nationales Recht vorsieht.~~

Das Ziel des europäischen Gesetzgebers, den Anwendungsbereich der DSGVO möglichst breit zu gestalten, ist damit erfolgreich umgesetzt. Wir haben es im positiven Sinne mit einem „**Weltrecht"** zu tun.

Zu 2.

Erfolgreich die technologischen Herausforderungen bestehen

Ich habe bislang eine positive erste Bilanz der DSGVO gezogen – und nationale wie internationale Beispiele genannt.

Die eigentliche Herausforderung für den europäischen Datenschutz liegt aber an anderer Stelle.

2.1 Neue Technik als bleibende Herausforderung

Findet der Datenschutz eine Antwort auf die großen technischen Herausforderungen?
Schafft er es, auch in der digitalisierten Welt die Privatsphäre zu schützen und die allgegenwärtigen Datenkraken einigermaßen im Zaume zu halten?

Scheitert Datenschutz an diesen gewaltigen Herausforderungen, verliert er das Vertrauen der Menschen und damit seine politische und schließlich auch rechtliche Gestaltungskraft. Dann beschweren sich die Menschen nicht mehr mit dem Ziel, dass Abhilfe geschaffen wird. Sie wenden sich dann nur noch resigniert ab mit dem Gefühl, ohnehin nichts ändern zu können.

Dann hat nicht nur der Datenschutz ein Problem, sondern auch die Demokratie.

Die Datenschutz-Aufsichtsbehörden haben die ~~Pflicht~~Aufgabe, Behörden und Unternehmen zu kontrollieren, ob diese die Bestimmungen des europäischen Datenschutzrechts einhalten. Bei Zuwiderhandeln drohen Bußgelder. Die Aufsichtsbehörden sollten sich aber nicht mit dieser Kontrollfunktion begnügen, sondern sich auch proaktiv für mehr Datenschutz einsetzen. Das gilt für eine bessere Information der Öffentlichkeit, die Bildung in den Schulen bis hin zu Entwicklung datenschutzfreundlicher Produkte.

Ich selbst verstehe mi~~t~~cht jedenfalls nicht als Lordsiegelbewahrer bestehender Vorschriften, sondern als Bundesdatenschutzbeauftragter mit einem umfassenden Auftrag, für den besseren Schutz der Persönlichkeitsrechte in Zeiten der Digitalisierung zu sorgen.

~~Die Datenschutzaufsicht sollte sich keinesfalls hinter der DSGVO in Deckung zu bringen wollen. Dann hätten wir verloren – und der Datenschutz gleich mit.~~

2.2 Technische Rahmenbedingungen

Lassen Sie mich die **technologischen Rahmenbedingungen anhand einiger Stichworte umreißen.**

- In den Daten liegt das Potential für digitale Innovationen
- Selbstfahrenden Autos,
- Intelligente Stromzähler (sogenannte Smart Meter)
- elektronische Rechnungen und Abrechnungssoftware.

Digitale Speichermedien sammeln nicht nur immer größere Datenmengen. Sie können diese auch in immer größerem Umfang speichern und auswerten.

Nach aktuellen Prognosen wird sich das Volumen der jährlich generierten Datenmenge weltweit im Zeitraum von 2016 bis 2025 mehr als verzehnfachen. Im Jahr 2016 lag das jährlich generierte Datenvolumen bei 16,1 Zettabyte. 2025 wird es bei 163 Zetabyte liegen. Ein Zetabyte ist eine Zahl mit 21 Nullen. Wenn Sie für jede Null einen Drops lutschen, sind sie überzuckert.

Mit der Menge der verfügbaren Daten werden immer feinkörnigere Analysen möglich. Geschäftsmodelle und neue Wertschöpfungsketten werden geschaffen. Zugleich verändern sich eingefahrene Arbeitsprozesse. Digitalisierung verändert, Staat, Gesellschaft, Wissenschaft, Arbeitsleben und Alltag.

~~**Der Datenschutz wiederum betont die Prinzipien der Datensparsamkeit und der Zweckbindung.** Was aber heißt das in Zeiten von **Big Data**? Big Data lebt von der Verknüpfung und Auswertung riesiger Datenmengen aus verschiedenen Quellen. Möglichst in Echtzeit sollen neue Erkenntnisse daraus gewonnen werden. Befördert wird diese rasante Entwicklung durch die enormen Fortschritte in der Informationstechnik.~~

2.3 Künstliche Intelligenz als Herausforderung

Künstliche Intelligenz (KI) und Datenschutz war das Leitthema der ersten nationalen Datenschutzkonferenz 2019.

KI schafft vielfältige digitale Innovationen, deren gesellschaftlicher Mehrwert teilweise jedoch kontrovers diskutiert wird. So kann die Versicherungswirtschaft etwa mit KI neue anreizorientierte – und damit grundsätzlich gesundheitsfördernde – Beitragsmodelle anbieten. Wer hier zunächst von günstigen Versicherungsbeiträgen profitiert, spürt aber möglicherweise schnell die Ambivalenz moderner KI-Datenanalysen, wenn

eine Veränderung von Lebensgewohnheiten oder eine bekannt werdende gesundheitliche Disposition sich vollautomatisch im nächsten Beitragsbescheid niederschlägt – oder gar zu einem Versicherungsausschluss führt.

Will der Datenschutz wirksam sein, brauchen wir eine politische und gesellschaftliche Diskussion um KI im Sinne einer proaktiven Gestaltung der Technik. Datenschutz als nachsorgende Kontrolle käme hier viel zu spät.

Wir müssen die Technik von Anfang an mitgestalten, dass sich die KI grundrechtsverträglich entwickeln.
Das ist moderner, proaktiver Datenschutz zur Sicherung der Grundrechte – und keine grämliche Nachsorge, wenn der Zug abgefahren und alles zu spät ist.

Gemeinsam mit den Kolleginnen und Kollegen aus den Bundesländern habe ich in der "Hambacher Erklärung" der DSK sieben Anforderungen an Systeme der KI aufgestellt. Die Erklärung setzt sich für eine datenschutzfreundliche Technikgestaltung von KI ein und formuliert die entsprechenden Voraussetzungen. Das Papier soll in den kommenden Monaten um weitere Papiere zu spezifischen Aspekten des Datenschutzes erweitert werden.

Wir bereiten gerade ein Symposium zum Thema "Datenschutzrechtliche Ansprüche an den Einsatz von KI" für den 24. September 2019 in Berlin vor.

Nicht zuletzt bringe ich die datenschutzrechtlichen Grundprinzipien auch in die Diskussionen der Datenethikkommission ein, deren Mitglied ich bin.

Folgen Kernbotschaften sind mir besonders wichtig:

- KI darf Menschen nicht zum Objekt machen.
- Auch für KI gelten selbstverständlich die Datenschutzgrundsätze. Dies ist auch gut so, denn Datenschutzrecht ist „in Form gegossener“ Grundrechtsschutz.
- KI muss transparent, nachvollziehbar und erklärbar sein – nur so kann es gelingen, Diskriminierungen einen Riegel vorzuschieben.

Wie aber sieht es bei vernetzten, weitgehend autonom arbeitenden und selbstlernenden Systemen mit der Verantwortlichkeit aus?

~~Wem werden die einzelnen Verarbeitungsprozesse zu einzelnen Beteiligten sowie im Hinblick auf Transparenz und Überprüfbarkeit zugerechnet? Die im Entstehen begriffenen Infrastrukturen für das autonome Fahren oder die Gesundheitstelematik zeigen geben darauf bereits erste Antworten. Das kann aber nur der Anfang einer breiten Debatte sein.~~

Die 40. Internationale Konferenz der Beauftragen für den Datenschutz am 23. Oktober 2018 in Brüssel hat dazu festgehalten, dass die Schaffung, Entwicklung und Nutzung von Systemen der künstlichen Intelligenz die Menschenrechte, insbesondere das Recht auf den Schutz personenbezogener Daten und auf den Schutz der Privatsphäre, sowie die Menschenwürde, das Diskriminierungsverbot und die Grundwerte uneinge-

schränkt achten muss und Lösungen bieten soll, die dem Einzelnen ermöglichen, die Kontrolle über die Systeme der künstlichen Intelligenz zu bewahren, und diese Systeme zu verstehen.

Ich teile diese Einschätzung ohne Wenn und Aber. Ich werde auf dieser Grundlage arbeiten.

2.4 Algorithmen und Scoring

In China, aber nicht nur dort, wird derzeit intensiv mit sog. „Super-Scores“ experimentiert. Bis 2020 sollen alle Bürgerinnen und Bürger einem Sozial-Kredit-Regime unterworfen werden. Dieser Score soll auch für Unternehmen gelten. Ziel ist eine umfassende Bewertung sozialer und politischer Verhaltensweisen. Braves und regimetreues Verhalten soll auf diese Weise belohnt und Widerborstigkeit mit Sanktionen belegt werden.

Eine solche Politik ist nicht allein ein Angriff auf personenbezogene Rechte Einzelner, sondern ein Großangriff auf die Struktur und das innere Gefüge von Staat und Gesellschaft.

Das Beispiel China zeigt, was an Missbrauch möglich ist. Wir müssen daher den gesamten Bereich **Scoring und Profiling** unter die Lupe nehmen. Sonst dringen Teilelemente dessen, was wir in China erleben auch hierzulande durch. Es geht dabei um weit mehr, als den Schutz persönlicher Daten vor staatlichen Zugriffen oder der Nutzung durch internationale Anbieter.

Auch in Europa ist die liberale Zivilgesellschaft im Kern ihres Selbstverständnisses herausgefordert, diese Form der Kontrolle des Einzelnen wirkungsvoll und energisch zu regulieren und zu kontrollieren.

Ich sprach es schon an -l~~L~~eider hat die von mir heute so gepriesene DSGVO bei Scoring und Profiling wenig zu bieten. Artikel 22 DSGVO kommt einer allgemeinen Regelung des Scorings noch am nächsten. Ich teile aber die skeptische Einschätzung des Sachverständigenrates für Verbraucherfragen im BMJV (Gutachten, Se. 113). Die DSGVO verzichtetet leider darauf, an die Definition von „Profiling“ Rechtsfolgen anzuknüpfen. Insbesondere fehlt es an rechtlichen Voraussetzungen, unter denen Profile überhaupt angelegt werden dürfen. Es bestand auf europäischer Ebene keine Einigkeit darüber, mehr als nur den Tatbestand selbst festzuschreiben.

- Ich schätze die Chancen, hier im Rahmen der Evaluierung die DSGVO noch zu ergänzen realistisch ein.
- Wir werden im Rahmen des möglichen ggf. eher den nationalen Gesetzgeber in die Pflicht nehmen müssen.
- Darüber hinaus sollten die Datenschutz-Aufsichtsbehörden die ihnen schon heute bestehenden Rechte zur Durchsetzung der Verbraucherinteressen konsequent nutzen.

Nicht ganz unumstritten ist es, ob der nationale Gesetzgeber die Möglichkeit hat, diese Lücke wenigstens teilweise zu schließen. Ungeachtet dessen leistet das der neue § 31 BDSG in seiner jetzigen Fassung allerdings auch nicht. Was sollte geschehen? Hier ein paar Anregungen:

- Die in Art. 15 Abs. 1 lit. h DSGVO vorgeschriebenen Anforderungen an die Verständlichkeit score-basierter Prozesse für den durchschnittlichen Verbraucher sollten jetzt zeitnah umgesetzt werden.

- Die Scoring-Anbieter – und das sind nicht nur die Auskunfteien! - müssen ihre Transparenzpflichten bei der Darstellung ihrer score-basierten Entscheidungen deutlich erweitern. Abgesehen davon, dass ~~In jedem Fall haben~~ die Verbraucherinnen und Verbraucher möglichst weitgehend darüber informiert sein müssen, was sich hinter dem Score verbirgt, müssen in jedem Falle ~~einen Anspruch darauf, dass~~ der Score und seine Eigenschaften gerade auch gegenüber den Aufsichtsbehörden offen gelegt und von diesen kontrolliert w~~e~~rden. Denn die Verbraucherinnen und Verbraucher werden oftmals nicht in der Lage sein, die komplexen Vorgänge der Score-Bildung vollständig zu durchschauen. An dieser Stelle soll mir übrigens niemand mit dem Einwand der Betriebs- und Geschäftsgeheimnisse kommen. **Wenn wir als Aufsichtsbehörden bis zu einem bestimmten Punkt auch Regierungsstellen und sogar Geheimdienste kontrollieren dürfen, lassen sich die Aufsichtsbehörden von Bund und Ländern weder von der Schufa noch einem anderen Anbieter die Tür weisen.**

- Die Verbraucher müssen wissen, wie die Scores zwischen verschiedenen Gruppen mit unterschiedlichen geschützten Merkmalen verteilt sind. Nur so können sie eine mögliche algorithmische Diskriminierung erkennen und dagegen angehen. Auch an diesem

Punkt müssen die Aufsichtsbehörden gestärkt werden. Sonst laufen die Rechte der Betroffenen schnell ins Leere.

- Die Anbieter sollten insbesondere in sensiblen Bereichen gegenüber den Aufsichtsbehörden die Qualität ihrer Verfahren darlegen müssen. Das muss dann auch überprüfbar sein. Gleiches gilt auch für die Verbesserung der Datenqualität. Hier liegt noch Vieles im Argen.

- Ich teile die Auffassung des Sachverständigenrats, dass zu Bekämpfung von Diskriminierungen ein Verbandsklagerecht für Antidiskriminierungssachverhalte im Bereich des Scorings zu schaffen ist.

Die genannten Aufgaben lassen sich nur bewältigen, wenn die Aufsichtsbehörden ein entsprechend hoch qualifiziertes Personal einzustellen können. Eine Aufsicht ohne Augenhöhe ist keine wirksame Kontrolle, sondern Augenwischerei.

3. Vernetzung mit anderen Politikbereichen unerlässlich

Ich habe zuletzt am Beispiel des **Scorings versucht zu erläutern,** wie sehr uns technische Entwicklungen fachlich und organisatorisch herausfordern. Es wird zum eigentlichen Elchtest für die Zukunft des europäischen und nationalen Datenschutzrechts, ob und wie die Datenschutz-Aufsichtsbehörden mit den neuen technologischen Herausforderungen

zurechtkommen und ob sie die großen internationalen Konzerne wie Google, Microsoft, Amazon und Facebook in den Griff bekommen.

Die DSGVO schafft zwar unabdingbare Voraussetzungen dafür, die Menschen vor einer Verletzung ihrer Privatsphäre zu schützen.
Der Datenschutz allein wird angesichts der Machtstellung dieser Unternehmen eine nachhaltig wirksame Kontrolle dieser Konzerne nicht allein stemmen können. Wir brauchen dazu eine andere EU-Wirtschafts- Wettbewerbs- und Steuerpolitik.

Solange Facebook EU-Länder gegeneinander ausspielen kann, kann auch der Datenschutz auf sich gestellt zwar Teilerfolge erringen, aber diese US-Konzerne nicht wirksam in ihre Schranken verweisen. Solange deren Geschäftsmodell, die Weiterverarbeitung personenbezogener Daten zu Werbe- oder anderen mit der Erbringung der jeweiligen Dienstleistungen nicht zu vereinbarenden Zwecke, unangetastet weitergeht, werden Bußgelder etc. an der einen oder anderen Stelle nicht genügen, die Missstände abzustellen.

Der Datenschutz muss sich mit den anderen genannten Politikfeldern vernetzen, um den Konzerne wirksam und nachhaltig Paroli bieten zu können.

Datenschutz allein wird es nicht richten können – aber ohne den Datenschutz läuft es auch nicht.

Ich danke für Ihre Aufmerksamkeit.