Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Weiter denken – aktuelle Herausforderungen für den (Verbraucher-)datenschutz“

beim Verbraucherpolitischen Kongress 2020
des Landes Nordrhein-Westfalen
"Verbraucherschutz digital: Datensouveränität im Fokus“

23.11.2020
10.50 h (Dauer: 15 Min.)

Es gilt das gesprochene Wort

Sehr geehrte Frau Ministerin,

Sehr geehrte Damen und Herren,

ich bedanke mich ganz herzlich für die Einladung, auf Ihrem heutigen Verbraucherpolitischen Kongress sprechen zu dürfen. Verbraucherschutzpolitik und Datenschutzpolitik bewegen sich ja bereits seit vielen Jahren in einer bedeutenden Schnittmenge von Themen, und nicht zuletzt mit den Verbraucherzentralen streiten wir Aufsichtsbehörden oft Seite an Seite erfolgreich für die Rechte der Bürgerinnen und Bürger in der Digitalisierung.

I. Einleitung

Meine Damen und Herren, die Corona-Pandemie hat uns – auch was diese Veranstaltung als hybrides Format heute angeht - fest im Griff.

Die Pandemie bewirkt trotz ihrer wahrhaft globalen katastrophalen Folgen auch einen Digitalisierungsschub, den unser Land nötig hat.

Aber Corona macht damit vor allem –wieder einmal - Facebook, Amazon, Google und Co. mit ihren Plattformen und digitalen Diensten zu den eigentlichen Gewinnern dieser gravierenden Krise, in der wir uns heute befinden. Eine Herausforderung für den Datenschutz, denn die Beschwerden über die Geschäftsmodelle gerade dieser Unternehmen und die daraus entstehenden Risiken beschäftigen uns seit Jahren.

Einer kürzlich veröffentlichten Studie eines deutschen Geldinstituts zufolge sind und bleiben wir Deutschen aber – man ist fast an die tapferen Gallier und ihr Dorf erinnert – beim Umgang mit unseren persönlichen Daten gewissenhaft. So gaben etwa 82 % der Befragten an, nur die Daten zur Nutzung freizugeben, die unbedingt notwendig sind. Das ist eine wie ich finde bemerkenswerte Zahl.

Und als Kontrapunkt zu dieser sehr erfreulichen Haltung vieler Bürgerinnen und Bürger räumen immerhin 38 % der Befragten ein, dass sie die Allgemeinen Geschäftsbedingungen bestenfalls überfliegen. Warum das so ist, wissen wir alle nur zu gut aus eigener Erfahrung. Die Zeitung „Der Standard“ aus Wien rechnete dazu kürzlich vor:

Würde man alle Privacy Policies, die man in einem Jahr vorgesetzt bekommt, lesen, dann würde das, wie errechnet wurde, 76 Tage dauern und allein in den USA 781 Milliarden Dollar (fiktiver) Arbeitskosten pro Jahr generieren. Die Privacy Policies nur der 20 populärsten Apps zu lesen dauert bei hohem Lesetempo mehr als sechs Stunden.

Es wird uns Verbraucher*innen systematisch schwer bis unmöglich gemacht zu verstehen geschweige denn zu entscheiden, wer wann was im Web, bei Diensten und Plattformen, aber auch bei Smart Toys oder etwa anderen Smart Devices mit unseren persönlichen Daten macht. Der Nebel um den Kern vieler digitaler Geschäftsmodelle verdeckt zumeist die lückenlose Datenerfassung der Kundinnen und Kunden, vom ersten Kontakt, über den Chat bis hin zur Verfolgung der Kunden bei Verlassen der eigenen Plattform. Selbstbestimmung und Kommunikationsgeheimnis sind hier de facto aufgehoben. In der Folge drohen Fremdbestimmung und Manipulation.

Dieser digitalen Wirtschaft stehen allerdings unsere Werte in Gestalt der Europäischen Grundrechtecharta ebenso wie das Grundgesetz entgegen. Das Grundrecht auf Datenschutz als auch das Recht auf informationelle Selbstbestimmung, ferner das Telekommunikationsgeheimnis und das sog. Computergrundrecht (Integrität und Sicherheit informationstechnischer Systeme) entfalten Drittwirkung bis tief in die Kundenbeziehung. Den Gesetzgeber treffen Schutzpflichten für eine verbraucherfreundliche und datenschutzkonforme Ausgestaltung von IT-Systemen und eine wirksame Gewährleistung der Rechte der Verbraucher. Das Ziel ist mehr Teilhabe, Selbstbestimmung und ja, Freiräume. Digitalisierung muss auch ohne Ausspioniertwerden möglich sein.

Erlauben Sie mir an dieser Stelle einen Hinweis: der Begriff „Datensouveränität“ ist eine Worterfindung des politischen spin doctoring und bedient zuallererst eine wirtschaftspolitische Perspektive. Er beschreibt meist das Bestreben nach weniger Abhängigkeit von Drittanbietern, seien sie nun aus China oder den USA. Das macht auch aus Datenschutzsicht durchaus Sinn: die Datenschutzkonferenz etwa hat kürzlich dazu eine wichtige Entschließung verabschiedet. Nur würde ich diesen Begriff nicht in unserer heutigen auf individuelle Verbraucherrechte bezogenen Debatte verwenden. Denn der Begriff verschleiert, dass es manchen Playern eher darum geht, eine wirtschaftliche Verwertungsautonomie des Einzelnen an die Stelle des letztlich immateriell begründeten Rechts auf informationelle Selbstbestimmung zu setzen. Es verspricht insoweit zu viel, und hält zu wenig.

II. DSGVO als Meilenstein und Vollzugsprobleme

Wo stehen wir also heute in diesem Ringen um eine digitale Gesellschaft der Verbraucherrechte? Wo es um die Menschen gehen soll und nicht umgekehrt allein um das Funktionieren der Wirtschaft? Wie steht es also um unseren Versuch, sowohl unseren Fortschrittsglauben eng mit der Digitalisierung zu verbinden, als auch zugleich an unserem Menschenbild des Grundgesetzes festzuhalten?

Mit der Datenschutzgrundverordnung ist der Europäischen Union eine weltweit respektierte Grundlegung im Verbraucherdatenschutz gelungen.

Sie ist mehr als bloßes Ordnungsrecht. Sie bildet eine auch geopolitische Verortung der Europäischen Union und stellt sich einer digitalen Übernahme Europas entgegen. Auf der Grundlage der Werte unserer gemeinsamen Verfassung.

Lassen sie mich deshalb auch deutlich aussprechen: die mit Verabschiedung der DSGVO rasch auftauchenden Vorschläge, wie z.B. das Recht auf Dateneigentum, stellten kein Weiterdenken dar. Sie drohen sich vielmehr gegen das gerade Erreichte zu wenden. Der Gegenwind war dementsprechend deutlich. Mein Eindruck ist: so könnte es auch den geforderten sog. allgemeinen Datenteilungspflichten ergehen.

Wie jedes große Gesetzeswerk ist die DSGVO „work in progress“. Ganz vorne in unseren Prioritäten liegt die Umsetzung des Vollzugapparates der DSGVO. Wie Sie vielleicht wissen, hat das Landgericht Bonn in der vergangenen Woche ein von uns gegen ein TK-Unternehmen verhängtes Bußgeld dem Grunde nach – mit Ausnahme der Höhe – in allen wesentlichen und grundsätzlichen Punkten bestätigt. So wie wir schreiten europaweit die Aufsichtsbehörden voran. Die Zahlen der Verfahren steigen und wir leisten mit Blick auf viele ungelöste Rechtsfragen Pionierarbeit.

Es ist nun lange bekannt, dass ausgerechnet in Irland, wo die europäischen Zentralen der ganz großen Unternehmen der Tech-Branche ansässig sind, praktisch wenige bis keine Verfahren abgeschlossen und entschieden werden. Wir Aufsichtsbehörden brauchen deshalb mit Blick auf die Verbindlichkeit mehrheitlicher Beschlüsse des Europäischen Datenschutzausschusses und deren Durchsetzbarkeit weitere Reformschritte des gemeinsamen Datenschutzrechts auf Brüsseler Ebene.

Ebenfalls wird bereits länger diskutiert, ob unsere nationale föderale Aufsichtsstruktur einen update vertragen kann. Ich sage Ihnen: grundsätzlich ja, und wir arbeiten daran in der Datenschutzkonferenz, also der Konferenz der zuständigen Datenschutzbehörden des Bundes und der Länder. Aber der einfachste Weg, da muss ich den Ball an die Bundesländer zurückspielen, läge im konsequenten Ausbau der für die Wirtschaftsaufsicht primär zuständigen, aber zumeist viel zu dürftig ausgestatteten Landesbehörden. Damit diese die Rechte der Verbraucher*innen durchsetzen, die Unternehmen aber auch beraten können. Eine gute Investition!

III. Tracking, Profiling und Scoring der Verbraucher

Und ja, es hat sich mittlerweile doch herumgesprochen, die DSGVO bietet für einige sehr aktuelle und bedeutsame Fragen, wie zum Beispiel das aus Verbrauchersicht besonders problematische Tracking von Verbrauchern durch Profiling und Scoring, keine hinreichenden Antworten. Hier muss zumindest der europäische Gesetzgeber bald nachbessern. Dies betrifft zum einen eine Änderung des Art. 22 DSGVO dahingehend, dass bereits die Profilbildung an sich und nicht erst die darauf beruhende Entscheidung dem Verbot der Datenverarbeitung mit Erlaubnisvorbehalt (also z.B. Einwilligung oder gesetzliche Vorgabe) unterfällt.

Zum anderen sollte in Anlehnung an die Vorschläge der Datenethikkommission bei algorithmenbasierten Entscheidungen je nach Risikoeinschätzung eine gestaffelte Regulierung greifen, die dem Einzelnen angemessene Schutzgarantien und Verteidigungsmöglichkeiten gegen Fehler und Bedrohungen seiner Rechte vermittelt. Vom freien Markt bis zu Ex-ante-Genehmigung oder Verbot.

IV. Europäischer Verbraucherdatenschutz

Wir Datenschützer*innen sind natürlich auch gespannt, was der Europäische Gesetzgeber mit dem Digital Services Act präsentieren wird. Die DSGVO stellt ja, wenn sie so wollen, eine Art Plattformregulierung 1.0 dar. Es würde den Verbrauchern helfen, wenn das Recht auf Datenportabilität eine Erweiterung erführe oder wir endlich in den Bereich der Herstellerhaftung für fehlendes privacy by design gelangten.

Den datenschutzrechtlich Verantwortlichen obliegt nämlich die Pflicht des „privacy by design“ („Datenschutz durch Technikgestaltung“) gemäß Art. 25 DSGVO. Softwarehersteller aber sind für Datenverarbeitungen mithilfe von Software nicht verantwortlich. Faktisch verfügen sie über Einfluss auf die Datenschutzkonformität von Datenverarbeitungsprozessen, entscheiden aber nicht über Mittel und Zweck der Datenverarbeitung. Damit obliegt ihnen nicht die Pflicht des „privacy by design“ und sie können gerade nicht für Software haftbar gemacht werden, die eine datenschutzkonforme Verarbeitung personenbezogener Daten gar nicht erst ermöglicht.

Eine realistische Möglichkeit für eine die Verbraucherdatenschutzrechte ganz erheblich stärkende Einigung bietet eine ambitionierte E-Privacy-Verordnung. Wie Sie vielleicht wissen, sollte diese den Online-Bereich und besonders das Kommunikationsgeheimnis im Digitalen absichernde Verordnung bereits mit der DSGVO an den Start gehen. Dazu kam es auch deshalb nicht, weil der politische Wille im Sperrfeuer des Lobbying großer Medienunternehmen mehr und mehr schwand. Ein Entwurf der deutschen EU-Ratspräsidentschaft, der wichtige Elemente dieses Vorhabens Aufrecht erhielt, bekam letzte Woche leider keine Mehrheit im EU-Rat.

Besonders wichtig wäre das bei der heute noch oft verwendeten schwammigen Rechtsgrundlage „berechtigte Interessen für die Verarbeitung von Metadaten“. Denn im Mittelpunkt des Verbraucherdatenschutzrechts steht die informierte Einwilligung aus echter Wahlfreiheit. Ich freue mich, dass der Europäische Gerichtshof (EuGH) bislang kaum eine Chance auslässt, um dies den Verantwortlichen mitzugeben.

Mit der kürzlich ergangenen Entscheidungen zur Zulässigkeit von tracking cookies als auch zur Rechtfertigung von weitergehenden Datenspeicherungen hat er deutlich gemacht, dass er jedenfalls die vorangekreuzten Einwilligungshäkchen für nicht mehr zulässig erachtet. Das sind bedeutende Weichenstellungen für das Verbraucherdatenschutzrecht.

Aber nicht alles, was aus Brüssel kommt, kann glänzen. Tiefgehende, dem Datenschutz oft gegenläufige Interessen, zumeist aus dem Sicherheitsbereich, werfen ihre Schatten auch auf den sonst in Brüssel so hochgehaltenen Verbraucherschutz. Mit Entsetzen mussten wir deshalb Vorschläge aus dem EU-Ministerrat zur Kenntnis nehmen müssen, wieder einmal Hintertüren oder Vordertüren oder sonstige Schwachstellen bei Ende-zu-Ende-Verschlüsselung etwa von Messengerangeboten für den Zugang von Sicherheitsbehörden einzuführen.

Den Schutz der Bürger und Bürgerinnen auch in ihrer Rolle als Verbraucher*innen vor Ausspähung im Internet würde ein solcher Schritt weitgehend verunmöglichen. Und zugleich die Glaubwürdigkeit des EU-Gesetzgebers erheblich beschädigen. Vielmehr muss das Recht auf Verschlüsselung noch konsequenter eingefordert und von den Verantwortlichen gewährleistet werden. Denn die Risiken in Bezug auf IT-Sicherheit als auch Ausspähung der Verbraucherinnen und Verbraucher haben eher zu- als abgenommen. Verschlüsselungen bieten insoweit einen unverzichtbaren Grundschutz für alle Formen der Kommunikation online. Jede Tür, jede Schwachstelle wird ausgenutzt werden, durch fremde Staaten, durch übermäßige Überwachung des eigenen Staates, durch Missbrauch im Staat, durch Einzelpersonen und durch Kriminelle.

Das war so und das wird immer so sein. Es gibt keine, ich wiederhole keine, technische Lösung, die das verhindern könnte.

V. Verbraucherfreundliche Ausgestaltung

Die E-Privacy-Verordnung könnte auch bei der Frage der datenschutzfreundlichen Technikgestaltung eine gewichtige Rolle spielen: Wenn eine Regelung für den Einsatz von privacy icons mit herauskäme, wäre das zu begrüßen. Einen kleinen Katalog von standardisierten Bildsymbolen hatten wir ja bereits in der Entwurfsphase der DSGVO vorliegen. Doch der war noch nicht nutzungsreif.

Die Klarheit und Verständlichkeit der Angaben von datenschutzrechtlich Verantwortlichen sind zwingende Anforderungen. Artikel 12 DSGVO regelt diese Vorgaben vergleichsweise deutlich für den Anwendungsbereich der DSGVO.

Doch schon der konkret die privacy icons ansprechende Artikel 12 Absatz 7 wirft viele interpretatorische Fragen auf. Sie können sich vorstellen, dass für den Online-Bereich mit seinen noch flüchtigeren Begegnungen und Praktiken des Austausches das Problem der einfachen Erläuterung bei gleichzeitigem Erhalt der Präzision der rechtlich bedeutsamen Aussagen eine Herausforderung darstellt. Wir wissen von einigen Forschungsprojekten zu dieser zentralen Frage verbraucherfreundlicher Gestaltung. Ein Erfolg bei Gestaltung überzeugender privacy icons würde in jedem Fall zugleich eine bedeutende Stärkung unserer auf informierten Einwilligungen basierenden europäischen Datenschutzkultur bedeuten.

Dort, wo Einwilligungen bloß noch als lästige Formalität durchgeklickt werden, könnte durch beeindruckende Bildsymbole also auch das immer wieder angegriffene Konzept der Einwilligung gestärkt werden, wenn eine bloße Illusion von Sicherheit vermieden werden kann.

Als weitere Beispiele für datenschutzfreundliche Ausgestaltungsmöglichkeiten möchte ich an dieser Stelle auch noch die sog. layered notices erwähnen. Sie bieten ebenfalls Spielräume für Verantwortliche, um einen overkill an Informationen für Nutzer und den gefürchteten consent fatigue zu vermeiden. Abgeschichtete Informationen der Betroffenen können die Angst vor weiterer Befassung nehmen und schnell informieren, ohne die aus rechtlicher Sicht notwendige Genauigkeit aufzugeben.

VI. Datenstrategie und Verbraucherdatenschutz

Ich komme damit zum letzten Punkt meines Impulses, den Datenstrategien von EU und Bundesregierung und den Folgen aus Verbraucher*innensicht. Die Kommission hatte auf EU-Ebene vorgelegt, nun wartet zunächst alles gespannt auf den Aufschlag aus Berlin. Die Debatte um die Datenstrategie hebt ja gewissermaßen auch die Frage des präventiven Verbraucherschutzes auf die Infrastrukturebene.

Zur Datensouveränität hatte ich mich ja bereits geäußert, sie bildet ja gewissermaßen die zugrundeliegende Zielsetzung. Eng mit all diesen Fragen verknüpft sind natürlich auch Regelungsfragen rund um Künstliche Intelligenz bzw. das maschinenbasierte Lernen.

Aus Datenschutzsicht sind viele der im Rahmen von politischen Datenstrategien verfolgten Bestrebungen mehr als nachvollziehbar. Wenn es gelänge, viele der verarbeiteten Daten in Europa zu halten und fließen zu lassen, wäre damit auch der Schutz der Rechte der Bürger und Bürgerinnen einfacher realisierbar. Erlauben Sie mir die Bemerkung: Denn nicht zuletzt das jüngste begrüßenswerte Urteil des EuGH mit Namen Schrems II stellt uns Aufsichtsbehörden gerade vor massive Probleme der Umsetzung.

Die sich abzeichnenden Konzepte des vereinfachten Datenpooling durch Verwaltung und Unternehmen, die Schaffung eines zumindest cloudähnlichen europäischen Datenverbundes wie Gaia-X sowie die erwartbare Offensive für Open Data können also gewissermaßen auf einer Metaebene auch von uns Datenschützern Unterstützung erfahren.

Doch die erwartbaren Zielkonflikte liegen ebenfalls auf der Hand: neue Begehrlichkeiten entstehen, bestehende Datenschutzstandards für diesen europäischen Markt abzusenken. Wie können Zweckbindung und Einwilligung bei den Gesundheitsdaten verbleiben, die in großen Forschungsdatenpools für Big Data zur Verfügung stehen sollen?

Und wo Daten zukünftig in zentralisierten Strukturen verarbeitet werden sollen, verlassen sie gerade die Herrschaftsbereiche der Verbraucher*innen, die bislang unangetastet blieben. Denken Sie zum Beispiel an die von ihrem KFZ mit Hunderten Sensoren geschaffenen Informationen und Daten, die sie womöglich nicht so einfach einer Vielzahl von Dienstleistern und Unternehmen hergeben wollen.

Vor diesem Hintergrund muss von Beginn an klar sein: ohne kompensierende Datenschutz-Innovationen zum Schutz der Verbraucher kann eine nationale Datenstrategie keinen Erfolg haben.

Viele der in der Diskussion befindlichen Vorschläge hatte bereits die Datenethikkommission aufgegriffen und positiv kommentiert. Die Idee der Datentreuhand kann Spielräume eröffnen, wenn dadurch tatsächlich mehr Kontrolle und Teilhabe und letztlich eine Stärkung der Rechte der Verbraucherinnen erzielt werden kann. Auf einer mehr technischen Ebene können die sog. Privacy-Konnektoren sicherstellen, dass Daten an die richtige Stelle gelangen und Authentifizierung ermöglichen. Eine tatsächlich umsetzbare Datenportabilität böte den Verbrauchern endlich die Chance, Anbieter zu wechseln und damit einen Markt zu schaffen. Verteiltes Lernen auf Daten im Herrschaftsbereich der Verbraucher*innen könnte große zentralisierte Datensammlungen überflüssig machen.

Ich hoffe, ich konnte Ihnen damit einen kleinen Überblick in die außerordentliche Vielfalt und Dynamik des Feldes Verbraucherdatenschutz geben. Ihre Konferenz heute leistet einen wichtigen Beitrag, um Öffentlichkeit und notwendigen Austausch dazu auch in schwierigen Umständen zu gewährleisten.

Ich danke Ihnen für Ihre Aufmerksamkeit.