Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Keynote

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Digitaler Daten- und Verbraucherschutz“

Forum Verbraucherinformatik 2021

Verbraucherdatenschutz – Technik und Regulation
zur Unterstützung des Individuums

Hochschule Bonn-Rhein-Sieg

online
23. September 2021

Es gilt das gesprochene Wort

Sehr geehrter Herr Professor Stevens,

Sehr geehrter Herr Professor Boden,

Sehr geehrter Herr Doktor Bala,

sehr geehrte Damen und Herren,

vielen Dank für die freundliche Einladung zum heutigen Forum Verbraucherinformatik.

Nach vielen Monaten der digitalen Vorträge und Diskussionsrunden freue ich mich, dass heute zumindest eine hybride Veranstaltung möglich ist. Die digitalen Konferenztools haben uns durch die letzten Monate getragen, können aber den zwischenmenschlichen Kontakt nicht ersetzen.

I. Einleitung

Der heutige Workshop steht unter dem Thema „Technik und Regulation zur Unterstützung des Individuums“. Der Fokus liegt somit auf dem Individuum und nicht auf der Technik. Dies ist eine Perspektive, die in der öffentlichen Diskussion häufig zu kurz kommt.

Digitalisierung ist kein Selbstzweck. Es geht nicht per se darum, immer mehr Daten zu sammeln und immer mehr Prozesse zu digitalisieren, damit wir eine möglichst digitale und technisierte Welt erreichen. Wie bei allem Fortschritt sollte das Ziel sein, unser aller Leben zu verbessern.

Neue digitale Anwendungen sollen unser Leben vereinfachen, erleichtern und neue Dinge möglich machen.

Um dieses Ziel langfristig zu erreichen, muss aber der Mensch wieder mehr in den Mittelpunkt gerückt werden. Alle Akteure müssen wieder mehr in dem Bewusstsein handeln, dass die Technik dem Menschen dienen soll und nicht der Mensch der Technik.

Die Entwicklung hin zu einer menschenzentrierten Digitalisierung, die die Bedürfnisse der Bürgerinnen und Bürger / der Kundinnen und Kunden ernstnimmt und Individuen nicht nur als potentielle Einnahme- und Datenquelle betrachtet, muss das Ziel der kommenden Jahre sein.

II. Digitale Entwicklung

Die letzten eineinhalb Jahrzehnte waren von einer zunehmenden Digitalisierung gerade auch im Privatbereich geprägt. Immer mehr digitale Produkte und Dienstleistungen für Verbraucher und Verbraucherinnen wurden entwickelt und auf den Markt gebracht.

Den Anfang machten soziale Netzwerke wie studiVZ und Facebook Mitte der 2000er, die sich ausgehend von den jungen Erwachsenen über alle Altersschichten ausbreiteten und der sozialen Interaktion über das Internet einen gewaltigen Schub versetzten, der bis heute anhält. Die Nutzung des Internets und sein Erscheinungsbild haben sich dadurch nachhaltig verändert.

Messenger wie WhatsApp, Threema oder Telegram eroberten dann in den letzten 10 Jahren den Markt. Im Privatbereich wurden E-Mails und SMS weitgehend durch Messenger ersetzt.

Und auch in den eigenen vier Wänden hat die Digitalisierung Einzug gehalten. Smart Speaker, Staubsaugerroboter und Smart-TV gehören heute in vielen Haushalten zur gängigen Ausstattung.

III. Die Mär vom mündigen Verbraucher

Diese an Verbraucherinnen und Verbraucher gerichteten digitalen Produkte und Anwendungen sind regelmäßig mit einer massiven Datenverarbeitung verbunden. Personenbezogene Daten werden gesammelt und ausgewertet. Die Auswertung erfolgt häufig nicht nur durch den Anbieter selbst, sondern Daten werden an zahlreiche Drittfirmen weitergegeben, die diese dann beispielsweise zur Erstellung von Profilen verwenden, um personalisierte Werbung auszuspielen und die Bürgerinnen und Bürger in Kategorien auch für andere Zwecke einzuordnen.

Es wird 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 ihren persönlichen Daten macht. Selbst erfahrene Datenschützerinnen und Datenschützer sind nach dem Lesen der Datenschutzbestimmungen der großen Player häufig nicht schlauer, sondern haben große Fragezeichen im Kopf.

Viele Anbieter stützen sich zur Legitimation ihrer Dienste auf die Einwilligung. Von einer informierten und freiwilligen und damit rechtskonformen Einwilligung kann jedoch oft kaum ausgegangen werden.

Verbraucherinnen und Verbraucher willigen in vielen Fällen nicht ein, weil sie die hinter dem Dienst stehenden Datenverarbeitungen verstanden haben und mit diesen einverstanden sind. Sie willigen ein, weil sie von ellenlangen unverständlichen Datenschutzerklärungen „erschlagen“ werden und aufgeben. Oder lesen Sie alle Datenschutz- und Cookie-Hinweise, bevor sie auf einer Website surfen oder eine neue App installieren oder sich zu einer Veranstaltung wie der heutigen anmelden? Nicht selten werden wir etwa durch Dark Patterns zudem zu Einwilligungen geführt, die wir bei nutzergerechter Gestaltung nicht abgeben würden. Vielfach halten Einwilligungen auch sonst einer genauen Überprüfung nicht stand, ob sie tatsächlich freiwillig abgegeben worden sind.

Es ist daher eine Mär, dass mündige Verbraucherinnen und Verbraucher im heutigen Digitalzeitalter selbstbestimmt über ihre Daten entscheiden.

Hier besteht dringender Aufholbedarf! Den Verbraucherinnen und Verbrauchern müssen Informationen und Hilfsmittel an die Hand gegeben werden, die es Ihnen ermöglichen, die Hoheit über Ihre Daten zurückzugewinnen. Das Ziel muss mehr Teilhabe, bessere Selbstbestimmung und größere Freiräume für die Nutzenden sein. Digitalisierung muss auch ohne „Ausspioniert werden“ möglich sein.

Aber wie ist eine Transformation hin zu einer menschenzentrierten und datenschutzfreundlichen Digitalisierung möglich? Im Folgenden möchte ich auf einige Bereiche eingehen, die aus meiner Sicht gute Ansatzpunkte bieten.

Und bei der genaueren Umsetzungen sind dann unter anderem Sie als Wissenschaft gefragt, herauszuarbeiten, wie die Umsetzung dann im Detail erfolgen könnte.

IV. Stellschrauben

a. bessere Datenschutzerklärungen und nutzerfreundliches Einwilligungsmanagement

Eine erste Stellschraube sind die bereits erwähnten Datenschutzerklärungen und die Ausgestaltung, wie Einwilligungen eingeholt werden. Es kann nicht sein, dass ich mich als Verbraucher erst durch seitenlange Datenschutzerklärungen „quälen“ muss, um zumindest eine Ahnung davon zu bekommen, welche meiner Daten erfasst werden sollen und wozu. Das muss auch einfacher gehen. Hier bedarf es kreativer Ansätze und auch technischer Unterstützung, um zu besseren Ergebnissen zu kommen.

Eine Möglichkeit sind sog. layered notices. Sie bieten Spielräume für Verantwortliche, um einen overkill an Informationen für Nutzer und den gefürchteten consent fatigue zu vermeiden. Abgeschichtete Informationen können den Betroffenen die Angst vor weiterer Befassung nehmen und schnell informieren, ohne die aus rechtlicher Sicht notwendige Genauigkeit aufzugeben.

Zu diesem Ergebnis kam auch die vom Bundesministerium der Justiz und für Verbraucherschutz beauftragte Studie „Innovatives Datenschutz Einwilligungsmanagement“ aus 2020. Die Studie hat gezeigt, dass ein nutzerfreundliches Einwilligungsmanagement möglich ist.

Und auch die rechtlich notwendigen Informationspflichten müssen nicht in Form ellenlanger, unverständlicher Datenschutzerklärungen erfolgen. Informationen stehen am besten jeweils an der Stelle, an der die Datenverarbeitung erfolgen soll. Es werden zunächst nur die wichtigsten Stichpunkte auf der Bedienoberfläche angezeigt und weitere Informationen können die Nutzerinnen und Nutzer über Pop-Ups erhalten. Diese Art der Information fand auch unter den Befragten große Zustimmung.

Das oft gehörte Argument, dass eine nutzerfreundliche Umsetzung der DSGVO-Pflichten nicht möglich sei, wurde durch die Studie eindeutig widerlegt. Und auch die beteiligten Unternehmen konnten dieser Herangehensweise viel abgewinnen.

Jetzt bedarf es innovativer und mutiger Unternehmen, dies in die Praxis umsetzen. Und auch von politischer Seite muss die Umsetzung nutzerfreundlicher Datenschutzerklärungen und eines entsprechenden Einwilligungsmanagements gefordert und gefördert werden, damit diese eine Chance haben, sich am Markt durchzusetzen.

b. Privacy icons

Eine zusätzliche Verbesserung könnte durch privacy icons erreicht werden. Einen kleinen Katalog standardisierter Bildsymbole gab es bereits in der Entwurfsphase der DSGVO. Doch dieser war noch nicht nutzungsreif.

Privacy icons sind in der DSGVO bereits angelegt (Art. 12 Abs. 7 DSGVO). Sie könnten dabei helfen, auf den ersten Blick einen Eindruck über zu erwartende Datenverarbeitungen zu erhalten. Beispielsweise könnten sie auf der Verpackung von Smart-Home-Geräten angebracht werden und so bei der Kaufentscheidung einen Vergleich der Geräte bezüglich Datenschutz und Datensicherheit erleichtern.

Und einprägsame Symbole, die vor ausufernder Datenverarbeitung warnen, könnten den ein oder anderen vielleicht doch davon abbringen, im Online-Kontext immer seine Einwilligung zu erteilen.

Auch Forschung und Entwicklung in diesem Bereich sollte weiter gefordert und gefördert werden.

c. Mehr Transparenz und Selbstbestimmung durch neue „Verbraucherdienste“ (z.B. PIMS)

Großes Potenzial sehe ich in sogenannten Personal Information Management Systems (PIMS) und Privacy Enhancing Technologies (PETs).

Hierbei handelt sich um digitale Anwendungen, die zum Ziel haben, den Betroffenen Kontrolle über ihre personenbezogenen Daten zu ermöglichen und sie von Entscheidungen zu entlasten, die sie überfordern, sei es technisch (Einstellungen), fachlich (Forschung) oder auch nur zeitlich.

Eine Spielart sind Einwilligungsmanagementsysteme, bei denen Nutzer erteilte Einwilligungen zentral nachvollziehen und steuern können. Auch Datenschutzcockpits fallen unter diese Kategorie. Datenschutzcockpits für Verbraucherinnen und Verbraucher ermöglichen diesen, über ein zentrales Tool einen Überblick darüber zu erhalten, wie ihre Daten durch einen Anbieter verarbeitet werden. Denkbar sind auch Datentreuhand-Modelle. Der Datentreuhänder würde die Daten der Nutzenden nach deren Vorgaben für diese verwalten.

Voraussetzung bei allen Spielarten der PIMS ist, dass diese selbst datenschutzkonform betrieben werden. Im Interesse der Rechts-sicherheit wäre wünschenswert, wenn die Aktivitäten im Rahmen von PIMS rechtlich klar geregelt wären.

Der rechtliche Rahmen für alle diese Systeme muss aus datenschutzrechtlicher Sicht so ausgestaltet werden, dass Interessenkonflikte ausgeschlossen werden. Datentreuhänder z.B. müssen eindeutig den Interessen der betroffenen Personen dienen und dürfen nicht an der Nutzung der Daten verdienen. Diese Forderung wurde durch mich auch in das Gutachten der Datenethikkommission (DEK) eingebracht.

Erste Vorschläge für die Regulierung von Datentreuhändern finden sich im Entwurf der Kommission zum Data-Governance-Act. Der derzeitige Vorschlag ist aus Datenschutzsicht noch unausgereift. Datentreuhänder, die sich an Verbraucherinnen und Verbraucher richten, müssen als Dienstleister für diese tätig werden und dürfen nicht zu Datenhändlern oder „Zweckänderungsagenturen“ werden. Auch Unabhängigkeit und Neutralität der Datenmittler sind Grundlage für Verbrauchervertrauen. Hier setze ich mich auf politischer Ebene dafür ein, dass der Data-Governance-Act noch entsprechend angepasst wird.

PIMS werden sich flächendeckend nur dann durchsetzen können, wenn Kommunikationsprotokolle etc. standardisiert und offene Schnittstellen geschaffen werden. Hierzu bedarf es eines gewissen Drucks durch rechtliche Vorgaben. Zudem sollten Projekte zur Entwicklungen verbraucherfreundlicher PIMS gefördert werden.

d. Privacy by design

Aber nicht nur zusätzliche Anwendungen in Form von PIMS verbessern den Daten- und Verbraucherschutz, auch bei den eigentlichen Anwendungen und Produkten muss angesetzt werden.

Es darf nicht sein, dass Smarthome-Geräte und Apps sich regelmäßig als Datenstaubsauger gerieren. Staubsaugerroboter, die nicht nur fleißig den Staub, sondern auch genüsslich persönliche Daten aufsaugen und über eine ungesicherte Verbindung die Hersteller oder Dritte weiterleiten, sollte es nicht geben.

Datenschutz und Datensicherheit müssen bei smarten Produkten und digitalen Anwendungen von Anfang an mitgedacht werden. Das ist es ja, was mit „privacy by design“ gemeint ist. Sowohl Geräteherstellen wie auch Softwareentwickler wie auch Prozessverantwortliche müssen den Datenschutz und die Datensicherheit schon in den ersten Entwicklungsstufen mitdenken und umsetzen. Datenschutz und Datensicherheit sollten durch die Hersteller endlich nicht mehr als lästiges Beiwerk, sondern als Baustein für Produktsicherheit und Kundenfreundlichkeit gesehen werden.

Um dies zu erreichen, sollte der europäische Gesetzgeber aktiv werden und eine datenschutzrechtliche Herstellerhaftung für fehlendes privacy by design einführen. Derzeit obliegt den datenschutzrechtlich Verantwortlichen nämlich die Pflicht des „privacy by design“ („Datenschutz durch Technikgestaltung“) gemäß Art. 25 DSGVO. Softwarehersteller aber sind für Datenverarbeitungen mithilfe von Software regelmäßig nicht verantwortlich. Faktisch haben sie aber maßgeblichen Einfluss auf die Datenschutzkonformität von Datenverarbeitungsprozessen. Es wäre daher nur konsequent, sie auch in die Haftung zu nehmen.

e. Interoperabilität

Auch mein letzter Punkt betrifft die technische Ausgestaltung digitaler Anwendungen und smarter Produkte. Die Geräte und Anwendungen müssen interoperabel werden. Das bedeutet für mich, dass neue Geräte und Software nicht nur mit der Vorgängerversion kompatibel sind, sondern auch mit den “Nachbarn“.

Das Gleiche z.B. für Messenger. Wäre es nicht ein Traum, wenn ich auch als datenschutz-sensible Person, mit allen meinen Kontakten über die gleiche App kommunizieren könnte, zumindest mit den grundlegenden Funktionalitäten? Dann wäre auch Schluss mit dem ständigen Gruppenzwang im Privatbereich, der all jene trifft, die nicht jene weit verbreiteten kostenlosen aber dafür datensaugenden Messenger-Apps installiert haben. Eine Kommunikation über Anbieter hinweg wäre wieder möglich.

In den alten Zeiten von Mobilfunk und SMS wollte mich ja auch niemand dazu zwingen, den Mobilfunkanbieter zu wechseln, bevor er mir eine Einladung per SMS schickt. Hier muss der Gesetzgeber Interoperabilität vorschreiben, auch damit neue Wettbewerber das Oligopol der Datenkonzerne herausfordern können. Natürlich darf der Preis für die Interoperabilität nicht ein Downsizing des Datenschutzniveaus bedeuten. Maßstab sollte der Standard des datenschutzfreundlichsten Anbieters sein.

V. Vorteile datenschutzfreundlicher Lösungen auch für Unternehmen

Ein wichtiger Faktor, warum datenschutzfreundliche Lösungen scheitern, sind die Unternehmen. Fast alle großen amerikanischen und vermutlich alle chinesischen Anbieter sehen ihren Vorteil in der Sammlung, Auswertung und Weiterverwendung möglichst vieler Daten. Und die meisten europäischen Unternehmen wollen diesen nacheifern und sehen die DSGVO und andere Vorschriften primär als Hemmschuh.

Aus meiner Sicht macht es aber keinen Sinn, amerikanischen oder chinesischen Firmen „hinterher zu hecheln“. Europäische Unternehmen müssen echte Alternativen entwickeln und da können datenschutz- und nutzerfreundliche Produkte und Anwendungen eine echte Alternative sein. Natürlich möchten Verbraucherinnen und Verbraucher ein benutzerfreundliches und innovatives Produkt. Vielen Verbraucherinnen und Verbrauchern weltweit ist auch der Schutz Ihrer Daten wichtig, das belegen Umfragen seit Jahren. Sie haben nur zum Teil schon aufgegeben. Alternativen könnten, durch gute Rahmenbedingungen wie z.B. eine kritische Masse an Benutzerinnen durch Nutzung in öffentlichen Einrichtungen, hier ein riesiges Marktpotenzial entwickeln.

Die Entwicklung der Corona-Warn-App zum Beispiel hat gezeigt, dass Datenschutz und Innovation sich nicht ausschließen. Neue Anwendungen, die den Menschen gleichzeitig einen Mehrwert bringen, müssen nicht zwangsläufig gleichzeitig personenbezogenen Daten unkontrolliert absaugen.

In vielen Bereichen fehlt es derzeit noch an datenschutzfreundlichen Alternativen. Dabei könnte die Wirtschaft mit datenschutzfreundlichen Lösungen auf den nationalen-, europäischen und weltweiten Märkten durchaus punkten. Verbraucherinnen und Verbraucher könnten wieder Vertrauen in digitale Anwendungen fassen. Zudem müssen Unternehmen, die Datenschutz von Anfang an mitdenken, nicht mit dem Risiko leben, dass Aufsichtsbehörden mittels Bußgeldern oder Anordnungen das Recht entsprechend durchsetzen.

VI. Fazit

Ich bin der festen Überzeugung, dass eine menschenzentrierte Digitalisierung möglich ist, wenn sich in Wirtschaft, Forschung und Politik genügend Unterstützer finden, die nicht nur daran glauben, sondern auch rational die tatsächlichen Vorteile erfassen und darauf basierend den Mut aufbringen, die notwendigen Schritte zu gehen. Und hierzu können Sie als Forschende im Bereich der Verbraucherinformatik einen wichtigen Beitrag leisten.

Ich danke Ihnen für Ihre Aufmerksamkeit.