Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Sicher im Netz!? Wie machen wir Kinder und Jugendlichen stark für die digitale Welt?“

als Impuls zur Podiumsdiskussion
beim Kinderschutzbund Köln

im Klarissenkloster Köln-Kalk

16. September 2022

Es gilt das gesprochene Wort

Meine sehr geehrten Damen und Herren!

Ich freue mich, dass so viele von Ihnen heute den Weg hier ins Klarissenkloster gefunden haben, um über ein wichtiges Thema zu sprechen. Denn die Auseinandersetzung mit der digitalen Welt und die hierfür erforderlichen Kompetenzen sind für Kinder und Jugendliche genauso relevant wie das Erlernen einer Fremdsprache und wichtiger als später ein Autoführerschein.

Deshalb bin ich auch Herrn Hüttler und dem Kinderschutzbund Köln sehr dankbar, dass sie dieses Thema im Rahmenprogramm des diesjährigen Weltkindertages in den Fokus rücken.

I. Einleitung

Meine Damen und Herren,

Themen wie Datenschutz und Medienkompetenz für Kinder haben für mich immer eine besondere Bedeutung. Ich betrachte diese Themen immer aus zwei verschiedenen Richtungen.

Zum einen als Datenschutzbeauftragter mit einem gesetzlich vorgeschrieben besonderen Schwerpunkt für diesen Bereich. Hier habe ich – zumindest in der Theorie – einen nüchternen, objektiven Blick auf die Dinge. Zum anderen bin ich aber auch der Vater von 5 Kindern, drei davon noch schulpflichtig und Großvater von zwei Enkeln.

Damit stehe ich, wie viele andere hier sicherlich auch, vor der Herausforderung, das theoretisch Richtige auch im täglichen Austausch mit meiner Familie um- und manchmal auch durchzusetzen. Hier wird man dann gerne schnell einmal von der Realität eingeholt.

Zwei Erkenntnisse, die ich sowohl als Datenschutzbeauftragter als auch als Vater dabei gewonnen habe, sind: Man kann nie früh genug damit anfangen, wichtige Dinge zu vermitteln und man darf nie müde werden, diese Dinge immer wieder zu wiederholen.

Und das bringt mich dann auch schon zu dem ersten Punkt, auf den ich hier kurz eingehen möchte. Die Information über potentielle Risiken in der digitalen Welt.

II. Potentielle Risiken

Dabei möchte ich eines direkt vorweg klarstellen: Schon von meinem beruflichen Hintergrund als Informatiker her bin ich ein absoluter Digitalisierungs-Fan! Die Chancen und Vorteile der Digitalisierung sind gigantisch und absolut unstrittig.

Anders als noch vor 20 Jahren können wir heute weltweit quasi umsonst kommunizieren, wenn gewünscht sogar per Video. Künstliche Intelligenz hilft uns, Krankheiten früher und besser zu erkennen als die erfahrensten Ärzte es könnten und GPS-Informationen helfen dabei, Logistik effizienter und damit auch klimafreundlicher gestalten zu können.

Doch viele Vorteile der Digitalisierung haben auch eine Kehrseite in Form von Risiken. In nicht wenigen Fällen – und hier liegt das eigentliche Problem – sind diese Risiken für die Anwenderinnen und Anwender von neuer Technik nur schwer erkennbar. Wie aber kann ich die notwendige Abwägung zwischen Vor- und Nachteilen sinnvoll treffen, wenn mir nur einseitige und unzureichende Informationen vorliegen?

Oder um mal eine überspitzte Analogie zu verwenden: Würden sie in eine medizinisch nicht zwingend erforderliche Operation unter Vollnarkose einwilligen, ohne vorher über die damit verbundenen Risiken aufgeklärt worden zu sein? Wohl kaum…

Trotzdem treffen die meisten von uns ähnliche Entscheidungen auf Basis einer ebenfalls dünnen Informationsgrundlage oder weil es doch alle so machen, wenn es um die Nutzung von digitalen internetgestützten Diensten geht.

Ich frage einmal in die Runde hier: Wer von Ihnen benutzt (regelmäßig) einen digitalen Sprachassistenten wie z.B. Alexa, Siri oder den Google Assistant oder nutzt die Diktierfunktion seines Handys um Textnachrichten zu schreiben oder Internetrecherchen durchzuführen?
[Reaktion des Publikums/Handzeichen abwarten]

Und wie viele von Ihnen haben sich vorab darüber informiert, was mit den aufgenommenen Sprachnachrichten passiert? Also wohin sie überall übermittelt werden, wer zu welchen Zwecken Zugriff auf sie hat, wie lange sie gespeichert werden, ob sie nur automatisiert oder auch von „echten“ Menschen abgehört und ausgewertet werden, welche Rechte Sie mit der Nutzung des Dienstes dem jeweiligen Unternehmen an der Verwendung der Sprachdateien einräumen, und so weiter?

[Reaktion des Publikums/Handzeichen abwarten]

[*Alt. 1 (wenn wenige aufzeigen):*] Tatsächlich ist dies äußerst repräsentativ, denn wie hier kümmern sich nur die wenigsten Menschen um diese Fragen, bevor sie Alexa und Co. in ihren Alltag integrieren.

[*oder Alt. 2 (wenn viele aufzeigen):*] Das freut mich zu sehen, dass hier ein so datenschutzaffines Publikum sitzt. Aber leider sind sie hier keine repräsentative Gruppe, weil sich nur die wenigsten Menschen um diese Fragen kümmern, bevor sie Alexa und Co. in ihren Alltag integrieren.

Und das bringt mich dann auch wieder zu der Gruppe über die wir hier eigentlich sprechen wollen: den Kindern und Jugendlichen. Wie sollen sie die vor allem im Netz drohenden Risiken erkennen und richtig einschätzen, wenn dies schon den meisten Erwachsenen schwerfällt?

1. Grooming und Cyberbullying

Denn Risiken gibt es viele. Zunächst denken wir da natürlich immer an Dinge wie Online-Grooming oder Cyberbullying. Gerade, weil hier die dadurch drohenden Gefahren und Folgen so gravierend sein können, ist eine Sensibilisierung von Kindern und Jugendlichen essentiell.

Allerdings gibt es neben diesen vermeintlich offensichtlichen Risiken noch viele weitere, die eben nicht auf den ersten – und manchmal auch nicht auf den zweiten oder dritten – Blick erkennbar sind und deren Folgen sich oft erst nach einer langen Zeit offenbaren.

2. Erst denken, dann klicken

Zum einen ist hier ein vernünftiger grundsätzlicher Umgang mit den eigenen Daten im Internet zu nennen. Das Partyfoto von gestern ist heute vielleicht cool oder lustig. Aber wie heißt es so platt aber richtig: Das Internet vergisst nie. Wenn in ein paar Jahren ein potentieller Arbeitgeber im Rahmen einer Internetrecherche über die Bewerberin oder den Bewerber entsprechende Bilder findet, ist der Spaß vielleicht nicht mehr so groß.

3. Profiling im Internet

Doch selbst wenn man penibel darauf achtet, wie in sozialen Netzwerken die Privatsphäre-Einstellungen gewählt wurden und was man im Internet preisgibt, kann man nicht unbedingt verhindern, dass dort mitunter massenhaft Daten über einen gesammelt werden, ohne dass man es überhaupt mitkriegt.

Unternehmen wie Facebook und Co. werten nicht nur das aus, was wir als Bilder posten oder im Netzwerk schreiben. Sie analysieren zum Beispiel auch, wie wir schreiben. Algorithmen bewerten anhand unserer Tippgeschwindigkeit und der Art, wie wir tippen (also z.B. ob wir viele Fehler machen oder Worte und Satzteile immer wieder neu formulieren), wie unsere aktuelle Stimmungslage ist. Sind wir erregt und verärgert, oder traurig oder depressiv… der Algorithmus findet es heraus und das Unternehmen lässt es in das Profil einfließen, das es über jeden seiner Nutzerinnen und Nutzer anlegt (und eventuell auch über die, die die Plattform nicht nutzen).

Warum? … Daten bedeuten Informationen und Wissen und daraus wiederum kann man letztendlich Profit schlagen. Dabei endet es nicht bei der personalisierten Werbung, an die die meisten jetzt denken werden.

Die Profile der Unternehmen werden dabei so aussagekräftig, dass sie ein ziemlich genaues Bild unseres Lebens wiederspiegeln. Das beschränkt sich nicht nur auf Informationen wo wir wohnen und uns gerne in unserer Freizeit aufhalten, was wir am liebsten essen und was unsere Hobbies sind oder wo wir gerne einmal Urlaub machen würden.

In den Datenbanken schlummern auch Informationen, die wir vielleicht nicht einmal mit unseren engsten Freunden oder Verwandten teilen würden, z.B. unsere politische Einstellung, depressive Gedanken oder Angstzustände, oder potentielle Krankheiten.

Alles zusammengestellt von einem Algorithmus, der unsere Posts, Internetrecherchen, Webseitenbesuche und eben Dinge wie die Tippgeschwindigkeit auswertet.

Wie gläsern man im Internet wirklich sein kann, hat beispielsweise der Dokumentarfilm „Made to Measure“ eindrucksvoll belegt. In diesem wird gezeigt, wie anhand der Daten einer Person, die sich hierzu bereit erklärt hat, ein fast identischer Doppelgänger erstellt werden kann. Wer diesen Film noch nicht gesehen hat, sollte dies unbedingt nachholen. Aktuell ist er in der ARD-Mediathek oder unter www.madetomeasure.online frei verfügbar.

III. Mögliche Lösungen

Meine Damen und Herren, wie sie sehen gibt es viele Risiken. Die Frage die sich nun stellt ist, wie reagieren wir darauf, insbesondere mit Blick auf unsere Kinder und Jugendlichen?

Da wir genau darüber gleich diskutieren wollen will ich hier nur ein paar kurze generelle Ansätze vorstellen, die ich als BfDI aus datenschutzrechtlicher Sicht verfolge beziehungsweise als sinnvoll erachte.

1. Aufsichtsrechtliche Regulierung

Zunächst müssen wir Datenschützer uns da natürlich an die eigene Nase fassen. Deshalb ist der erste Punkt, den ich hier nennen will, die aufsichtsrechtliche Regulierung.

Die Datenschutzgrundverordnung gibt uns Aufsichtsbehörden zumindest in der Theorie mittlerweile einen großen Werkzeugkasten an Möglichkeiten, um das geltende Recht auch durchzusetzen. Die Reichweite liegt dabei von Warnungen über Datenverarbeitungsverbote bis hin zu hohen Geldbußen.

Leider hat sich herausgestellt, dass die Anwendung dieser möglichen Maßnahmen in der Praxis oft nur schleppend umgesetzt werden kann – insbesondere wenn es gegen die großen globalen Digitalunternehmen geht. Das hat verschiedene Gründe, die ausreichen um fünf weitere Vorträge zu füllen und die ich mir an dieser Stelle daher spare.

Aber ungeachtet der Anlaufschwierigkeiten zeigt sich auch hier mittlerweile Bewegung. Wie einige vielleicht mitbekommen haben, ist Instagram gerade mit einem Bußgeld in Höhe von über 400 Millionen Euro belegt worden. Grund war eine Möglichkeit, Statistiken über die Abrufe des eigenen Profils zu erhalten, die aber mit einem Wechsel der Privatsphäre-Einstellungen einherging, der für die meisten Nutzerinnen und Nutzer nicht hinreichend klar wurde. Auf diese Weise wurden vor allem Profile von Kindern und Jugendlichen, oft inklusive derer Telefonnummern und E-Mailadressen, auf einmal für alle Besucher offen einsehbar.

2. Klare Gesetze

Die Aufsicht als Exekutive kann allerdings nur dort tätig werden, wo gegen Gesetze verstoßen wird.

Ob und wo dies der Fall ist, ist gerade im Datenschutzrecht nicht immer schwarz und weiß. Insbesondere wenn es darum geht, dass eine Datenverarbeitung durch eine vermeintliche Einwilligung der oder des Betroffenen legitimiert ist, gibt es regelmäßig unterschiedliche Ansichten und Auslegungen.

Vor diesem Hintergrund wäre es wünschenswert, wenn der Gesetzgeber an der ein oder anderen Stelle noch einmal nachschärft.

So setze ich mich seit langem – leider bislang erfolglos – dafür ein, dass nicht nur die Nutzung von den vorhin angesprochenen Profilen, die beispielsweise von Betreibern sozialer Netzwerke erstellt werden, rechtlich reguliert wird, sondern bereits die Erstellung dieser Profile gesetzlich untersagt wird. Dieses Ausspionieren ist unerträglich.

Gleiches gilt für eine bislang fehlende datenschutzrechtliche Produkthaftung. So kann – und das ist jetzt ein fiktives Beispiel –ein Softwarehersteller ein Praxisverwaltungssystem für Ärzte anbieten, dass nur eine rechtswidrige Verarbeitung der sensiblen Patientendaten ermöglicht. Dieser Hersteller würde datenschutzrechtlich keinerlei Verantwortung für die mit seinem Produkt erfolgende Datenverarbeitung tragen, während der das Produkt einsetzende Arzt belangt werden würde und das, obwohl er in den meisten Fällen nicht einmal das Verständnis oder eventuell sogar die Möglichkeit hat, die Funktionsweise des Programms und die hierin liegenden Probleme zu erkennen und verstehen.

3. Information und Beratung

Und das bringt mich dann zum Dritten und vielleicht wichtigsten Punkt: Information und Beratung.

Wie wir gesehen haben, ist eine der größten Gefahren, dass wir gar nicht so richtig wissen, was mit unseren Daten im Internet und bei der Nutzung von digitalen Diensten überhaupt alles passiert. Deshalb sehe ich es als eine der wichtigsten meiner Aufgaben an, Menschen für die Risiken von Datenverarbeitungsprozessen zu sensibilisieren.

Es geht uns Datenschützern nämlich – anders als es immer mal wieder gerne plump behauptet wird – nicht darum, digitale Lösungen zu verbieten oder den Menschen vorzuschreiben, wie sie mit ihren Daten umzugehen haben.

Unser Ziel ist es vielmehr eine Situation zu schaffen, in der Nutzerinnen und Nutzern alle relevanten Vor- und Nachteile aufgezeigt bekommen, um dann eigenständig eine informierte Entscheidung treffen zu können, ob die vermeintlichen Vorteile die Nachteile für sie persönlich aufwiegen können.

Das erreicht man zum einen, indem man die Anbieter verpflichtet, die notwendigen Informationen in verständlicher Art und Weise zur Verfügung zu stellen; das verlangt übrigens auch das Gesetz. Und zum anderen, indem man parallel aktiv Aufklärung über häufige Risiken und Stolpersteine betreibt und versucht, Menschen für das Thema Datenschutz zu sensibilisieren.

a) Angebote des BfDI

Als BfDI tun wir das vor allem über unsere Öffentlichkeitsarbeit. Hier bieten wir beispielsweise über unsere Website ein großes Sortiment an kostenlosen Informationsmaterialen an; sowohl zu spezifischen als auch zu ganz allgemeinen Themen.

Seit einiger Zeit legen wir dabei einen besonderen Fokus auf Kinder und Jugendliche. Beispielsweise haben wir gerade aktuell einen neuen, hybriden Flyer mit dem Thema „Datenschutz ist Kinderschutz“ herausgegeben, in dem wir Tipps zum sicheren Verhalten für Kinder und Jugendliche im Netz geben.

Zudem haben wir bereits im letzten Jahr zwei Pixi Bücher veröffentlicht, die gezielt Kinder im Kindergarten und Grundschulalter ansprechen und spielerisch und mit Spaß an das Thema Datenschutz heranführen sollen. Beides haben wir im Eingangsbereich ausgelegt, so dass sie sich nachher gerne ein Exemplar mitnehmen können.

Dass wir uns gerade mit den Pixi Büchern an die besonders jungen Kinder gewandt haben, hat übrigens auch einen Grund. Um besser zu verstehen, wie Kinder und Jugendliche das Thema Datenschutz erleben, haben wir einen Fokusgruppentest durchführen lassen.

b) Fokusgruppentest

Dabei haben wir an insgesamt sechs Schulen im Kölner Raum unterteilt in drei Gruppen (9 Jährige, 10-12 Jährige und 13-16 Jährige) jeweils Bewusstsein und Einstellung zum Datenschutz, Berührungspunkte mit ihm im Alltag, das allgemeine Interesse am Datenschutz und die Art, wie man zum Thema angesprochen werden möchte, abgefragt.

Das vielleicht wichtigste Ergebnis dabei war, dass präventive Maßnahmen bereits bei der Gruppe der 10-12 Jährigen nur noch sehr bedingte Aussichten auf Erfolg haben. Hier haben die meisten Kinder bereits Smartphones und sind somit aktiver Teil der sozialen Medien. Dies und der Umstand, dass die Kontakte mit Datenschutzfragen wie Einwilligungserklärungen, die in der Regel gerade nicht für Kinder verfasst sind, als kompliziert und nervig empfunden werden, führt dazu, dass diese Gruppe nur sehr schwer erreicht werden kann.

Bei den Grundschülern hingegen stellte sich dies genau gegenteilig dar. Hier gibt es bereits einen ausgeprägten Sinn für Gerechtigkeit und Mitgefühl verbunden mit einem großen Drang nach Eigenständigkeit und dem Wunsch, für sich selbst Entscheidungen treffen zu können. Gerade dies erweist sich als der perfekte Nährboden, um die Kinder für Themen zu sensibilisieren, die noch nicht einmal wirklicher Gegenstand ihres Alltags sind, und es ist die Chance, sich mit den „erlernten“ Fragen erneut auseinanderzusetzen, wenn man in naher Zukunft zum ersten Mal stolz das eigene Smartphone in den Händen hält.

c) Weitere Informationsquellen

Dieser Ansatz, nicht erst zu warten, bis die Kinder bereits „zu alt“ und „zu betriebsblind“ sind, sollte übrigens allgemein verfolgt werden. Medienkompetenz und datenschutzrechtliche Sensibilisierung sollte zwingend Teil der Lehrpläne, und zwar schon in den Grundschulen, sein.

Dies setzt natürlich voraus, dass auch sämtliche Erziehungsberechtigten und Lehrkräfte dabei unterstützt werden, das erforderliche Wissen zu erlangen, um den Kindern von Beginn an eine echte Unterstützung zu sein.

Hierfür aber müssen auch wir Erwachsenen
a) bereit sein, uns mit der aktuellen Technik auseinanderzusetzen und sie und ihre Tücken zu verstehen, selbst dann wenn wir sie selber nicht nutzen und vor allem
b) dort, wo wir selber soziale Netzwerke oder andere digitale Angebote nutzen und einsetzen, unseren Kindern mit gutem Beispiel voran gehen und uns mit den auch für uns mitunter lästigen und komplizierten Fragen beschäftigen.

Denn generell gilt: Nur wer Risiken selbst erkennt und richtig einschätzt, hat die Möglichkeit, anderen zu helfen, sich vor ihnen zu schützen.

In diesem Sinne danke ich Ihnen für Ihre Aufmerksamkeit und freue mich auf die Diskussion.