Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Impuls

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Regulierung: Konsequenzen von digitalen Systemimmanenzen?“

CIO-Roundtable der deutschen ICT + Medienakademie

St. Augustin

26. Oktober 2023

Es gilt das gesprochene Wort

Sehr geehrter Herr Prof. Dr. Prinz,
Sehr geehrter Herr Hoffmann,
Sehr geehrter Herr Gerlach,
Sehr geehrte Damen und Herren

I. Einleitung

ich blicke heute in die Runde und sehe viele bekannte Gesichter – es ist schön, Sie alle wiederzusehen. Über die Einladung zum und die Gelegenheit, mit Ihnen über die Frage zu diskutieren, ob Regulierung die Konsequenz aus digitalen Systemimmanenzen ist, habe ich mich sehr gefreut.

Es ist auch eine Rückkehr an alte Wirkungsstätte, schließlich war ich hier am Campus in den 90er Jahren als studentische und wissenschaftliche Hilfskraft tätig.

Das Thema bietet sich auch an, denn die Europäische Union hat im Kontext ihrer Digitalstrategie ein Gesetzespaket vorgelegt, um dem sich aus den Folgen der Digitalisierung ergebenen Regulierungsbedarf gerecht zu werden. Insofern könnte man also die eingangs gestellte Frage schon an dieser Stelle mit „ja“ beantworten. Die rasante Entwicklung im Digitalbereich hat dazu geführt, dass die aktuellen Gesetze den sich an sie ergebenden Anforderungen nicht immer hinreichend gerecht werden können.

Deshalb lohnt es sich auch, einen kurzen Blick auf die europäischen Digitalrechtsakte zu werfen, wobei ich als BfDI – vermutlich wenig verwunderlich – natürlich vor allem auf datenschutzrechtliche Aspekte eingehen möchte.

II. DMA / DSA

Als erstes gibt es da den Digital Markets Act und den Digital Services Act. Sie gehören zu den ersten Verordnungen der Europäischen Digitalstrategie, die 2022 verabschiedet wurden und bereits in Kraft getreten sind. Ihre volle Wirksamkeit werden sie ab Anfang 2024 entfalten. Diese Rechtsakte zielen zwar im Kern nicht auf das Datenschutzrecht, haben jedoch viele datenschutzrechtliche Bezüge.

Nach dem Digital Markets Act, kurz: DMA, werden bestimmte Praktiken großer Digitalunternehmen, die als Gatekeeper – oder auf Deutsch: „Torwächter“ – eingestuft werden, verboten. Die EU-Kommission kann Marktuntersuchungen durchführen und Verstöße gegen die Verhaltenspflichten des DMA z.B. durch Soziale Netzwerke oder Suchmaschinen sanktionieren.

Der Fokus der Verordnung liegt beim Wettbewerbsrecht und soll die Marktmacht großer Digitalkonzerne beschränken.

Dabei nimmt der DMA allerdings an vielen Stellen Bezug auf Regelungsinhalte, die bereits in der DSGVO angelegt sind, wie z.B. Interoperabilität, Profiling und insbesondere die Anforderungen an eine wirksame Einwilligung von Nutzerinnen und Nutzern.

Der Digital Services Act, kurz: DSA, führt Sorgfaltspflichten für große Vermittlungsdienste wie Online-Plattformen, Online-Marktplätze und Suchmaschinen ein. Die Pflichten umfassen das Löschen von illegalen Inhalten sowie Transparenz für Verbraucher im Hinblick auf Online-Kauf, Werbung und Empfehlungssysteme. Ziel der Verordnung ist es, europaweit ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld zu schaffen.

Für große Plattformen mit mehr als 45 Mio. Nutzenden pro Monat gelten besondere Anforderungen, deren Umsetzung von der EU-Kommission beaufsichtigt wird.

Auch im DSA bestehen Bezüge zum Datenschutzrecht. So werden bei der Verarbeitung sensibler Daten oder bei Daten Minderjähriger „dark patterns“ (besser: deceptive design patterns) und die Anzeige von Werbung verboten, die auf Profilbildung beruht.

III. DGA

Weiterer Bestandteil des EU-weiten Regelwerks für den digitalen Raum ist der Entwurf des Data Governance Act, kurz DGA. Auch dieser ist bereits in Kraft getreten und gilt seit September.

Mit dem DGA sollen Voraussetzungen für die Weitergabe von Daten durch öffentliche Stellen zur allgemeinen Nutzung geschaffen werden. Praktisch will man mit dem DGA eine Möglichkeit zur Einrichtung sogenannter Vermittlungsdienste schaffen, die als neutrale Vermittler Datenanbietende und Datennutzende zusammenbringen.

Dies kann zum Beispiel im Bereich der Forschung einen großen Mehrwert bieten. Auch die Schaffung von sogenannten datenaltruistischen Organisationen soll den Mitgliedsstaaten ermöglicht werden.

Wichtig ist dabei, dass durch den DGA keine eigene Rechtsgrundlage für eine Datenweitergabe geschaffen wird. Auch hierfür bleiben weiterhin die Regelungen der DSGVO maßgeblich und über diesen beständigen datenschutzrechtlichen Anker bin ich froh.

IV. DA

Gleiches sollte auch für den Data Act gelten, zu dem zurzeit noch die Trilog-Verhandlungen laufen. Hier geht es um Daten, die von vernetzten Geräten erzeugt werden, zum Beispiel durch virtuelle Sprachassistenten oder smarte Haushaltsgeräte.

Ziel der Kommission ist es, zu regeln, wer Zugriff auf diese Daten hat und wer sie wie nutzen darf. So sollen Nutzende Zugang zu den vom Hersteller gesammelten eigenen Daten erhalten können, unfaire Vertragsklauseln sollen aus standardisierten Lizenzverträgen verschwinden und unter bestimmten Bedingungen sollen öffentliche Stellen ein Recht auf Datenzugang und Datennutzung erhalten.

Was ich nun verstärkt in die Trilog-Verhandlungen einbringen möchte, können Sie sicher schon ahnen: die DSGVO muss auch durch den Data Act unberührt bleiben.

Soweit bei der Anwendung des Data Acts personenbezogene Daten verarbeitet werden, müssen die Regelungen der DSGVO gelten. Insbesondere muss sicherstellt sein, dass das Teilen personenbezogener Daten in Anwendung des Data Acts jederzeit mit den einschlägigen Datenschutzvorschriften vereinbar ist.

Der Data Act darf zudem kein neues Recht für Dateninhaber schaffen, die durch Nutzung eines Geräts erhaltenen Daten zu verwenden. Der Data Act kann keine „Rechtsgrundlage“ oder gar „rechtliche Verpflichtung“ im Sinne der DSGVO schaffen. Auch hier muss die DSGVO der maßgebliche Anker für den Datenschutz bleiben. Also die sechs möglichen Rechtsgrundlagen für eine Verarbeitung personenbezogener Daten.

V. KI- Verordnung

Wie wichtig Künstliche Intelligenz und algorithmenbasierte Anwendungen bereits aktuell sind, sollte spätestens seit dem Hype um Large Language Modelle wie Chat-GPT auch Nicht-Fachleuten bewusst sein. Dass hierbei mitunter auch sensible personenbezogene Daten verarbeitet werden, ist unstreitig. Problematisch ist jedoch, dass die genauen Prozesse bei vielen Anwendungen, die wir landläufig unter KI zusammenfassen, oft gar nicht wirklich bekannt sind. Nicht zuletzt deshalb ist der im Frühjahr 2021 von der Europäische vorgelegte Entwurf für eine KI-Verordnung aus datenschutzrechtlicher Sicht das vielleicht wichtigste Gesetz der EU-Digitalrechtsakte.

Die KI-Verordnung verfolgt einen risikobasierten Ansatz. KI-Systeme, die kein Risiko für Gesundheit, Sicherheit oder Grundrechte darstellen, werden von der Verordnung nicht berührt, können frei und rechtssicher im Markt eingeführt werden. KI-Systeme, deren Verwendung mit einem zumindest gewissen Risiko einhergehen, sollen jedoch reguliert werden. Je nach Einstufung werden unterschiedliche Sorgfaltspflichten, Zulassungsvoraussetzungen und Kontrollen erforderlich.

Mir ist dabei zunächst wichtig, dass am Ende der aktuell noch stattfindenden Verhandlungen der Verordnung einige Schlüsselregelungen stehen, die ich als essentiell betrachte, um eine grundrechtskonforme Nutzung von KI zu ermöglichen.

Eine der wichtigsten Voraussetzungen ist in diesem Zusammenhang eine hinreichende Transparenz. Betroffene müssen erkennen können, dass ihre Daten von einer künstlichen Intelligenz verarbeitet werden. Sie müssen Informationen über das KI-System erhalten, da nur so überhaupt die Möglichkeit entsteht z.B. algorithmische Diskriminierung erkennen zu können.

In einem zweiten Schritt muss gewährleistet sein, dass sich betroffene Personen gegen Diskriminierung durch KI-Systeme zu verteidigen können. Die KI-Verordnung sollte also Beschwerdemechanismen vorsehen. Wer durch solche Systeme in seinen Grundrechten verletzt wurde, muss die Möglichkeit haben rechtliche Schritte einzuleiten.

Und das bringt uns dann auch zu einem weiteren zu regulierenden Thema: klare Verantwortlichkeiten. Um die grundrechtskonforme Entwicklung und Anwendung von KI-Systemen gewährleisten zu können, ist es entscheidend, dass feststeht, wer für die in ihnen ablaufenden Datenverarbeitungen verantwortlich ist. Nur weil KI-Prozesse mitunter in einer Art Blackbox abgewickelt werden, darf das nicht dazu führen, dass hier ein Verantwortungsvakuum entsteht. Wenn zum Beispiel der Einsatz eines KI-System, das – auch unbeabsichtigt – Trainingsdaten falsch interpretiert, zu Diskriminierung in einem Bewerbungsprozess führt, muss klar geregelt sein, wer hierfür verantwortlich ist.

Ich bin der Meinung, dass KI-Systeme nur dann am europäischen Markt wettbewerbsfähig sein können, wenn die Menschen darauf vertrauen können, dass sie sicher sind und ihre Grundrechte beachtet werden. Ich werde mich daher auch hier konsequent dafür einsetzen, dass die Grundsätze der DSGVO nicht unterlaufen werden.

VI. DSGVO

Meine Damen und Herren, sicher ist Ihnen aufgefallen, dass ich bei jedem der bisher angesprochenen Rechtsakte immer auch noch ein weiteres Gesetz erwähnt habe: die DSGVO.

Jetzt mag man sagen: als Datenschützer ist das nicht wirklich verwunderlich. Aber darüber hinaus zeigt es einen wichtigen Umstand.

Egal wieviel sinnvolle neue Regulierung die europäischen Digitalrechtsakte mit sich bringen, sie werden weder alleine noch

zusammen eine umfassende datenschutzrechtliche Regulierung unseres digitalen Alltags ermöglichen können. Überall dort, wo Sachverhalte datenschutzrechtliche Fragen aufwerfen, bedarf es daher zwingend der Anwendbarkeit der DSGVO.

Sie ist bereits nach 5 Jahren unser fester Anker im europäischen Datenschutzrecht und hat sich darüber hinaus sogar zu einer Art weltweiten Goldstandard für Datenschutzregulierung entwickelt.

Sie bietet Regelungen zum Schutz der informationellen Selbstbestimmung im digitalen Zeitalter und damit eine Grundlage, auf der alle neuen Digitalrechtsakte aufsetzen müssen, wenn es um die Gewährleistung des Grundrechts auf Datenschutz geht.

Dementsprechend darf die DSGVO auch keinesfalls durch die neuen Rechtsakte ausgeschlossen oder auch nur eingeschränkt werden. In Sachen Datenschutz ist und bleibt sie das essentielle Gesetz zur Regulierung der Digitalisierung.

VII. Schlussbemerkung

Am Ende greife ich nochmals die bereits eingangs beantwortete Frage auf und stelle erneut klar, dass die digitale Entwicklung weitergehende Regulierung erforderlich macht. Die gute Nachricht hierbei ist, wir haben dies erkannt und mit den europäischen Digitalrechtsakten einen guten Ansatz gefunden, um dieser Herausforderung zu begegnen.

Zudem fangen wir ja nicht bei Null an, zumindest nicht in datenschutzrechtlicher Hinsicht. Die DSGVO bietet hier in allen Bereichen, sogar in Bezug auf neue Technologien, Orientierung und Halt.

Als Datenschutzbeauftragter werde ich mich dafür einsetzen, dass wir diese Möglichkeiten auch weiterhin nutzen, um auch künftig dafür zu sorgen, dass Digitalisierung und Grundrechteschutzes Hand in Hand gehen.

Ich danke Ihnen für Ihre Aufmerksamkeit.