Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„EU-Digitalstrategie und die dazugehörigen Rechtsakte von DGA, DMA, DSA und AIA – Auswirkungen für den Datenschutz“

Europäische Akademie für Informationsfreiheit und Datenschutz
(EAID e.V.)

27.01.2022

Online

Es gilt das gesprochene Wort

Lieber Peter Schaar und Team des EAID,
liebe Frau Geese und Frau Nikolay,
lieber Herr Zerdick,
lieber Klaus,
sehr geehrte Damen und Herren,

ich bedanke mich ganz herzlich für die freundliche Einladung und die Gelegenheit, an diesem Austausch zur EU-Datenstrategie und den zugehörigen Rechtsakten DGA, DSA, DMA und AIA teilnehmen zu können.

EDPS und EDSA haben jeweils einzeln und in einigen gemeinsamen Papieren unsere fachlichen Kritikpunkte zu den genannten Vorlagen dargelegt; zuletzt in einem rechtsaktübergreifenden Statement vom November letzten Jahres.

Dabei handelt es sich zum Teil um recht kleinteilige fachliche Erwägungen. Erlauben Sie mir deshalb, mich in meinem heutigen Beitrag auf einige allgemeinere Anmerkungen zu den Auswirkungen des Digitalpakets zu konzentrieren.

1. Europäischer Regelungsbedarf

In weitgehend unregulierten Räumen übt einfach der Stärkere seine Macht aus. Um den Berliner Juraprofessor Möllers mit etwas Drastischem zu digitalen Räumen zu zitieren: „Es gibt kein weltweites Kartellrecht, also haben wir Warlords: Das sind die Großkonzerne.“

Hier möchten wir Datenschützer leicht gekränkt ergänzen: aber es gibt doch schon lange andere Vorschriften für das Internet, auch und gerade das Datenschutzrecht. Das mag zutreffen, nur dass auch dieses Recht erst kürzlich mit der DSGVO überhaupt europäisch „scharf geschaltet wurde“. Und nach wie vor aus diversen Gründen – vor allem im grenzüberschreitenden Kontext – noch nicht zufriedenstellend vollzogen wird.

Daher begrüßen wir auch die vehemente Fortsetzung eines breiten EU-Regelungsanspruches in der Digitalisierung. Ohne entsprechende gesetzliche Regulierung sind neben wettbewerblichen Fragen vor allem die Grundrechte nicht zu gewährleisten. Der Datenschutz war mit der DSGVO ja insoweit Avantgarde.

Gerade mit Blick auf die Gewährleistung der Datenschutzgrundrechte erscheint der jetzt erhobene Anspruch von mehr „digitaler Souveränität“, verstanden als demokratische Autonomie und individuelle Selbstbestimmung, schlüssig. Insoweit gibt es – neben dem von China und den USA – Bedarf für einen die Grundrechte der Bürgerinnen und Bürger betonenden dritten Weg in der Datenpolitik.

2. Der „Drei-Säulen-Ansatz“

Es ist lange überfällig, dass die EU auf gleich mehreren Feldern regulierend eingreift: um grundlegende Spielregeln zu sichern und die viel und lange diskutierten negativen Folgen einer von Oligopolisten geprägten Plattformökonomie für unsere Gesellschaften einerseits

einzuhegen und andererseits Impulse für einen europäischen Ansatz zu liefern.

Dabei lassen sich für mich inzwischen drei Säulen unterscheiden:
zum einen sind da die auf Einhegung bestehender Plattformen von Big Tech/GAFAM (oder jetzt AMAMA) ausgerichteten und einen breiten Regelungsansatz verfolgenden Digital Services Act (DSA) und Digital Markets Act (DMA) Sie stehen (noch) klar im Mittelpunkt der Diskussionen. Einige Regelungsziele der Compliance-Pflichten wie etwa die systemische Folgenabschätzung, Transparenzpflichten und auch die Aktivierung des Wettbewerbsrechts durch den DMA, bringen auch für den Datenschutz Fortschritte und belegen für mich die zunehmende Ausdifferenzierung des Privatheitsschutzes.

Zum anderen sind da der Data Governance Act, der mehrfach verschobene, jetzt für kommenden Monat angekündigte Data Act und die sukzessive geplanten Regeln für sektorspezifische Datenräume. Mit dieser Säule entsteht eine Art Infrastrukturgewährleistungsrecht, mit dem ein rechtssicherer Rahmen für ein alternatives, ein mehr europäisches Modell der Plattformwirtschaft, geschaffen werden soll.

Und schließlich gibt es den Entwurf für eine KI-Verordnung und inzwischen auch einen Entwurf für eine Verordnung für mehr Transparenz beim politischen Microtargeting. Beides sind Gesetzesakte, bei denen nicht ausschließlich, aber besonders auch bereichsspezifisch, Datenschutzgesetzgebung stattfindet. Die KI-Verordnung ist im Gegensatz zur DSGVO technikspezifisch angelegt.

Und im Gegensatz zur Grundverordnung regelt die Microtargeting-VO eine Profiling-Problematik bereichsspezifisch.

Mit diesem Paket treten wir also in eine auch für uns Datenschützer durchaus neue Gesetzgebungsphase ein. Die Phase gesetzlicher Umsetzung der DSGVO ist überwiegend abgeschlossen. Auch eine erste vorsichtige DSGVO-Reformdebatte ist mit der ersten Evaluation durch die Kommission beendet.

Sichtbar werden jetzt die Umrisse eines übergreifenden EU-Daten-Informationsrechts, innerhalb dessen die Datenschutzgrundverordnung nur noch einen, wenn auch weiterhin wesentlichen Grundbaustein unter vielen anderen Bausteinen, darstellt.

3. Auswirkungen auf den Datenschutz

Die Folgen für den Datenschutz sind durchaus gravierend:
Zum einen verändert sich der Kontext des Datenschutzdiskurses grundlegend. Im Vordergrund stehen jetzt Fragen des Datenzugangs, der Ermöglichung des KI-Einsatzes, auch eine sog. „Kultur des Datenteilens“ wird beschworen. Das ist ein bedeutender Narrativwechsel. Wir werden uns als Datenschützer dazu klug verhalten müssen, um durchzudringen.

Für den Bereich der nicht-personenbezogenen Daten mag dieses Narrativ auf den ersten Blick problemlos erscheinen. Doch auch hier werden schon dringend Antworten gebraucht. Anonyme Datenbestände sind veränderlich, ihre laufende Prüfung geboten, Re-Personalisierungen müssen ausgeschlossen werden.

Verfahren der Anonymisierung (und Nach-Anonymisierung) brauchen weiter Forschung und die Aufsichtsbehörden müssen hier fachlich mitkommen können.

Bewegen wir uns aber im Anwendungsbereich des Datenschutzes, sind die Spannungsfelder offensichtlich. Für die einen mag es darum gehen, Daten und die mit ihnen erschließbaren Informationen aus den sogenannten Datensilos zu befreien. Für Datenschützer geht es hingegen um Datenbestände, die erst durch die Wahrung des Gebots der Zweckbindung im Sinne der Betroffenen steuerbar und kontrollierbar werden. Das Datenteilen oder auch nur die Gewährung der Datennutzung bedürfen stets der eingehenden rechtlichen Ausgestaltung zur Absicherung der Rechte der Betroffenen.

Erwartbar wird der Druck durch verantwortliche Stellen steigen, auch bloß pseudonymisierte Datenbestände privilegiert zu sehen oder mit dem Konzept des broad consent Verarbeitungserweiterungen zu erzielen.

a. Datennutzung und Datenschutz als Herausforderung

Das Regelungspaket steht ganz im Zeichen der Mobilisierung der Daten. Quantitativ wie qualitativ werden wir als Aufsichtsbehörden ein gänzlich neues Spielfeld der kommerziellen Massendatenverarbeitung zu bewältigen haben.

Und Grundlage der Regulierung sind Leittechnologien und Anwendungen von Big Data, vom Internet of Things, Cloud-Technologien und den darauf laufenden KI-Anwendungen.

Hier folgt die Kommission den globalen IT-Trends. Auch die KI- und Datenstrategie der EU sind hier letztlich eng miteinander verknüpft. Zu diesen Zusammenhängen der technischen Grundlagen hätte man in Brüssel meines Erachtens deutlich transparenter kommunizieren können. Denn sie verdeutlichen in der Zusammenschau erst die Dimension auch der damit verbundenen komplexen datenschutz-rechtlichen Herausforderungen.

Im Mittelpunkt der Regulierung steht, da beißt die Maus keinen Faden ab, eine primär wirtschaftspolitische Zielsetzung. Es geht um eine EU-Datenwirtschaft, die bis 2025 mit 829 Milliarden Euro oder 5,8 Prozent des Bruttoinlandsprodukts angesetzt wird.

Die Bürgerinnen und Bürger und die sie betreffenden personenbezogenen Informationen und Daten sollen der Rohstoff für das so geplante Wirtschaftswachstum sein.

Der Rückenwind für eine solche Datenstrategie kommt aber auch von anderer Seite, etwa unter Gemeinwohlgesichtspunkten.
Denn große Hoffnungen werden in die digitale, die datenmäßige Bewältigung der existenziellen Krisen unserer Zeit, der Klimakrise, wie auch bei drängenden Fragen der Bildung, der Forschung und der aktuellen Gesundheitskrise als Pandemie gesetzt.

Mit Daten soll das Wissen generiert werden, das der Menschheit zum Überleben oder besserem Leben verhelfen soll. Die Unterstützung der Gemeingüter oder die Stärkung öffentlicher Einrichtungen, hier liegt für mich ein weitreichenderes Potential einer Datenstrategie, die mehr ist als reine Industriestrategie.

Für den Datenschutz gilt es hier dann, hinsichtlich der Interessen und Zielsetzungen sorgfältig zu differenzieren. Forschungszwecke etwa erfahren ja schon in der DSGVO selbst eine deutliche Privilegierung.

b. Gute Ansätze

Um das zunächst deutlich zu sagen: ich begrüße es sehr, dass in dieser Gesetzgebungsphase die EU-Institutionen bis jetzt datenschutzpolitisch durchaus Flagge zeigen und

1. in der Strategie selbst wie auch in den bisherigen Verhandlungen um die vorliegenden Entwürfe ihr Bekenntnis zur DSGVO und zu dem damit erreichten Schutzniveau weitgehend durchhalten,

2. mit der Plattformregulierung durch DSA und DMA zu mehr Transparenz bei Algorithmen (Stichwort Forschungsdatenzugang), zu roten Linien beim Verhaltenstracking und zu Einschränkungen bei Dark Patterns kommen (sollte sich das EP beim Digital Services Act mit seinen weitergehenden Forderungen durchsetzen, könnte man tatsächlich bei dieser alle Plattformen betreffenden horizontalen Regelung von einer Art digitalem Grundgesetz sprechen).

3. beim DGA die angedachten Instrumente der Datenökonomie wie etwa die Datentreuhand mit Augenmaß aufgegriffen und für den erwarteten Data Act etwa die Frage der Interoperabilität als erweiterte Datenportabilität auch der Nutzerinnen und Nutzer angegangen werden könnte. Ein Recht auf leichten Cloud-Wechsel würde den Wettbewerb schaffen, den es auch um das beste datenschutzrechtliche Angebot braucht. Hier offenbar mitgedachte europäische Projekte wie Gaia-X, die

mit dem Bekenntnis zu Datenschutz, Datensicherheit und offenen Formaten auch von diesen Regeln erfasst werden, könnten unterm Strich eine Verbesserung auch für den Datenschutz bedeuten.

4. Schließlich begrüße ich den Entwurf der KI-Verordnung als eine Weiterentwicklung für den erwarteten bereichsspezifischen Datenschutz. Nichts anderes scheint mir auch der Entwurf für eine Verordnung über die Transparenz und das Targeting politischer Werbung zu sein, der im Rahmen eines Gesamtpakets zum Europäischen Aktionsplan für Demokratie kürzlich veröffentlicht wurde, der ja explizit die DSGVO-Vorschriften ergänzt. Im Einzelnen mögen hier noch einige Fragen zu klären sein, aber die problemorientierte Ausdifferenzierung des Datenschutzes mit entsprechend relevanten, auch überindividuellen Schutzgütern wie eben dem Erhalt unserer Demokratie, halte ich für folgerichtig.

c. Weiterer Reglungsbedarf

Doch wo so viel Licht ist, gibt es natürlich auch Schatten. Meine Kritikpunkte lassen sich mit der Forderung nach einer noch gezielteren Weiterentwicklung des Datenschutzes zusammenfassen. Mit dem vielgehörten Versprechen „Die DSGVO bleibt unberührt“ kommt der Datenschutz im Zuge dieses Regulierungspaketes letztlich nicht hin, wenn er effektiv bleiben soll.

Lassen Sie mich deshalb ein paar Punkte nennen, die im Hinblick auf die Folgen für den Datenschutz wichtig werden.

Durch das jetzt vorliegende Gesetzgebungspaket darf der zu lange liegengebliebene Abschluss des ePrivacy-VO-Prozesses nicht untergepflügt werden. Wir brauchen diese höhere Schutzstandards für die Online-Kommunikation festlegende Regelung. Frankreich will hier offenbar weiterverhandeln, aber Priorität hat das Thema nicht. Vielleicht kann Frau Nicolay uns hierzu etwas Neues berichten.

Das Gesetzespaket zielt auf die Mobilisierung von Big Data und KI. Genau für die damit verbundenen vielfältigen Datenschutzfragen, besonders des Profiling und der automatisierten Entscheidungsfindung, ist die DSGVO nicht hinreichend gerüstet. Die Mängel etwa des Artikel 22 DSGVO wurden früh erkannt und von uns stets moniert, aber nicht behoben. Der Entwurf der KI-Verordnung allein gibt hierauf (noch) keine ausreichenden Antworten.

Ausgerechnet das mit den gravierendsten Grundrechtseingriffen verbundene Überwachungsmodell des Pervasive Tracking durch Plattformen und Gatekeeper erhält im DSA und auch im VO-Entwurf zum politischen Microtargeting keine ausreichende Einschränkung.

Wir vertreten mit den Kollegen vom EDPS die Forderung nach einem Ende des umfassenden Verhaltensprofiling zu Werbezwecken. Es ist der Kern fragwürdiger Geschäftsmodelle. Für evident mit dem Grundrecht auf Datenschutz nicht vereinbare Verarbeitungsformen braucht es klare rote Linien im Datenschutz. So haben wir auch in Bezug auf die KI-Verordnung eine Reihe von hochriskanten KI-Anwendungen wie die von Privaten durchgeführte biometrische Erfassung in öffentlichen Räumen benannt, die wir ebenso für unzulässig halten.

Immerhin zeigen die vorliegenden Gesetzesentwürfe den Versuch einer mehr risikoabhängigen Regulierung beim Thema Werbung. Der Fokus auf den Schutz von Kindern wirft allerdings die Frage nach der datenschutzkonformen Umsetzbarkeit durch verantwortliche Stellen auf, während der etwa vom EP im Rahmen des DSA geforderte Ausschluss der Verwertung besonders geschützter Daten bereits nach geltendem Recht die engen Voraussetzungen des Artikel 9 DSGVO zu beachten hätte.

Damit hängt eng zusammen die Frage der Absicherung wirksamer Einwilligungen. Zwar ist es völlig richtig, insgesamt weiter die informationelle Selbstbestimmung der Nutzerinnen und Nutzer zu betonen. Doch die dafür auf Online-Plattformen notwendigen echten Entscheidungsspielräume müssen tatsächlich unter großem Aufwand erst geschaffen werden. Die Regelung der wirklich uferlosen Möglichkeiten von Dark Patterns wird umso wichtiger, wenn und soweit die Einwilligung im Mittelpunkt der Rechtfertigung von Daten-verarbeitungen bleibt.

Gerade bei der Regulierung eines eigenen europäischen Datenraums als Alternative zu den kommerziellen Friss- oder Stirb-Angeboten der Großen gilt es bei aller Dringlichkeit, Sorgfalt walten zu lassen.

Bei DGA, DA und den geplanten Datenräumen müssen wir im Blick behalten, dass es sich bei den Buzzwords der Datenökonomie datenschutzrechtlich zumindest um hybride und ambivalente Regelungsinstrumente handelt.

Datentreuhänder, Interoperabilität, Datenaltruismus, Reallabore/Sandboxes oder ein Open Data für personenbezogene Daten führen in für den Datenschutz ganz eigene Gewinn- und Verlustrechnungen.

Erst ihre konkrete Ausgestaltung erlaubt uns die Beurteilung, ob sie am Ende ganz überwiegend nur datenwirtschaftliche Funktionen erfüllen oder auch zur Förderung der Selbstentfaltung und einer echten Selbstbestimmung, dem Empowerment von Bürgern taugen können.

Jedenfalls können wir uns mit einem Datenschutz als bloßem Nudging, ich denke da an bestimmte Vorstellungen von Datenschutzmanagement-Systemen wie PIMS, nicht zufrieden geben. Was es vielmehr braucht, sind echte Reflexionsräume für die Ausübung der Rechte der Bürger.

Und beim Thema Interoperabilität zum Beispiel gilt es zu bedenken, dass auch Einzelne, die Daten durchaus selbstbestimmt weitergeben, immer zugleich auch Informationsinteressen Dritter berühren können, die von diesen Daten mitbetroffen sind.

Für den Data Governance Act habe ich bei meiner Beteiligung an den Stellungnahmen stets eines betont: die wenigen unpräzisen Schutzvorgaben reichen nicht aus, um die spezifischen Risiken für betroffene Personen durch die Verwendung ihrer Daten für KI-Anwendungen und Big-Data-Auswertungen einzugrenzen und die spezifischen Risiken eines Markts für personenbezogene Daten zu bekämpfen. Spätestens die geplanten Regelungen zu den geplanten

neuen Datenräumen müssten hier mehr bereichsspezifischen Schutz bringen.

Eine andere und für das Vertrauen in den Datenschutz ganz entscheidende Ebene betrifft die Governance der unterschiedlichen Gesetzesregelungen. So will man gerade von der bekannten Schwäche der DSGVO, insbesondere der mangelhaften Ausgestaltung des One-Stop-Shop-Verfahrens, gelernt haben.

Für DSA und DMA werden deshalb weitgehend die Zuständigkeiten gewechselt: für BigTech wird die EU-Kommission selbst die Zuständigkeit übernehmen. Im Falle des DSA handelt es sich dabei um die Very Large Platforms, die mit den Gatekeepern der wettbewerbsrechtlichen Regelung weitgehend deckungsgleich sein dürften.

Umso wichtiger ist dann allerdings zumindest die Koordination und Zusammenarbeit mit den unabhängigen, ich wiederhole unabhängigen, Datenschutzbehörden bei fachlich überschneidenden Zuständigkeiten, die wir nach den gegenwärtigen Entwürfen noch nicht hinreichend gesetzlich abgesichert sehen. In der Konsequenz könnte die Wahrnehmung entstehen, dass dieses Paket auch eine gewisse Marginalisierung des Datenschutzes und eine Unterordnung unter politische Zielsetzungen nach sich zieht.

Für den Bereich des Data-Governance-Act etwa haben die Datenschutzbehörden ausdrücklich ihre Zuständigkeit für die dort genannten Aufgaben der Aufsicht beansprucht, aber nicht erhalten.

In der Folge werden wir hier – wie auch im Falle der Digital Service Coordinators des DSA – natürlich zusätzliche Aufwände haben, uns mit den überlappend zuständigen Stellen zu koordinieren, ein Prozess mit mutmaßlichen Reibungsverlusten.

4. Fazit

Insgesamt versucht die EU mit der vorliegenden Strategie wohl die Fortsetzung des sog. Brussels-Effect, also die ihr gerade mit der DSGVO zugeschriebenen Rolle als globaler Taktgeber in Sachen Digitalgesetzgebung.

Im Falle der DSGVO, da kann es für mich keinen Zweifel geben, haben auch der Datenschutz und damit die Rechte der Bürgerinnen und Bürger wesentlich profitiert.

Für das jetzt vorliegende, noch in der Verhandlung befindliche Entwurfspaket ist eine Antwort womöglich noch verfrüht. Mir persönlich scheint aber unter dem Strich: ein guter, sehr ambitionierter Anfang wurde gemacht. Weitere Schritte werden folgen müssen.

Ich danke Ihnen für Ihre Aufmerksamkeit.