ohne Starke Verbraucher keine Starke Wirtschaft

verbraucherzentrale Bundesverband

WETTBEWERB UND DATENSCHUTZ: WIE KASTOR UND POLLUX*

Synergien zwischen Wettbewerb und Datenschutz sowie Lösungsansätze für eine integrative und kooperative Betrachtung beider Politikfelder

22. November 2021

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. EINLEITUNG

Wie sollte der problematischen Marktmacht der großen Digitalkonzerne – gemeint sind hier insbesondere Google, Facebook, Amazon, Apple und Microsoft – begegnet werden? Um diese Frage dreht sich eine der großen aktuellen politischen Debatten sowohl auf nationaler, als auch auf europäischer und transnationaler Ebene. Dabei wird immer deutlicher, wie eng das Problem der Marktmacht dieser Digitalkonzerne mit Datenschutzfragen verknüpft ist. Häufig wird daher die Frage aufgeworfen, ob Wettbewerb und Datenschutz grundsätzlich in Konflikt stehen, und ob daher zur Förderung des Wettbewerbs das Datenschutzniveau abgesenkt werden sollte. Ein aktuelles Gutachten[1] des Verbraucherzentrale Bundesverbands (vzbv) legt einen Gegenentwurf zu diesem oft postulierten Konflikt vor, indem es in diesem Zusammenhang auf zwei gleichzeitig auftretende Marktversagen hinweist und Lösungsansätze unterbreitet, welche (regulatorische) Schritte erforderlich sind, um Datenschutz und Wettbewerb sinnvoll zusammenwirken zu lassen, um den Schutz personenbezogener Daten und die Privatsphäre zu gewährleisten, einen fairen Wettbewerb zu gestalten sowie die Verbraucherwohlfahrt zu steigern.

II. AUSGANGSLAGE

1. ZWEIFACHES MARKTVERSAGEN

1.1 Marktversagen 1: Ungelöstes Wettbewerbsproblem

Auf der einen Seite steht ein ungelöstes Wettbewerbsproblem, das die Marktmacht der Digitalkonzerne festigt. Dieses entsteht insbesondere, indem die Digitalkonzerne Skalen-, Netzwerk- und Lock-in-Effekte ausnutzen, über einen besseren Zugang zu gewaltigen Datenmengen verfügen und ihre Marktmacht durch die Kopplung oder anderweitigen Bevorzugung ihrer eigenen Dienste auf benachbarte Märkte ausdehnen.[2] Das traditionelle Wettbewerbsrecht hat sich nicht als effektiv erwiesen, um diese Probleme zu lösen. Daher hat die Europäische Kommission mit dem Digital Markets Act[3] (DMA) einen Verordnungsvorschlag vorgelegt, der mit seinem ex-ante Regulierungscharakter und per-se Regeln für so genannte Gatekeeper[4] diese Probleme ergänzend zum Wettbewerbsrecht lösen soll.

---

* Die Zwillinge Kastor und Pollux, der eine ein Sterblicher, der andere ein Sohn des Zeus, sind Sinnbild für zwei auf ewig unzertrennliche Menschen in der griechischen Mythologie: Wikipedia: Dioskuren, https://de.wikipedia.org/wiki/Dioskuren [Zugriff: 18.11.2021]

[1] Kerber, Wolfgang; Specht-Riemenschneider, Louisa: Synergies between data protection law and competition law. Expert report commissioned by vzbv (2021), URL: https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf [Zugriff: 22.11.2021].

[2] Vgl. ebd., S. 17ff.

[3] Europäische Kommission: Vorschlag für **eine** Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte). COM/2020/842 final.

[4] Nach Artikel 2 sowie Artikel 3 DMA sind Gatekeeper Betreiber sogenannter zentraler Plattformdienste, wie etwa Betriebssysteme, Online-Vermittlungsdienste, Messenger oder Suchmaschinen, wobei diese Dienste erhebliche Auswirkungen auf den europäischen Binnenmarkt haben müssen und gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dienen. Diese Position müssen sie dauerhafte innehaben oder absehbar in naher Zukunft erlangen.

1.2 Marktversagen 2: Informations- und Rationalitätsprobleme

Auf der anderen Seite stehen Informations- und Rationalitätsprobleme von Verbraucher:innen, die ihre Rechte auf Privatsphäre und den Schutz personenbezogener Daten gefährden.[5] Denn insbesondere durch intransparente Datenschutzbestimmungen, aber auch durch eine manipulative Gestaltung der Angebote („dark patterns“), sind sie kaum in der Lage, freiwillige und informierte Entscheidungen über die Verarbeitung ihrer personenbezogenen Daten zu treffen. Hinzu kommt, dass auf vielen digitalen Märkten die Bereitstellung personenbezogener Daten durch Verbraucher:innen als eine Art Gegenleistung verwendet wird, um Dienstleistungen in Anspruch nehmen zu können. Dadurch werden aber auch die Entscheidungen der Verbraucher:innen zunehmend komplexer. Möchten Verbraucher:innen beispielsweise verschiedene Dienste vergleichen, würden sie nicht nur Informationen darüber benötigen, welche Daten erhoben und für welche Zwecke sie verarbeitet werden, sondern müssten auch den Wert dieser Daten sowie die „Kosten“ der Bereitstellung dieser Daten im Hinblick auf die damit verbundenen Risiken berücksichtigen.[6]

1.3 Enge Verbindung der beiden Marktversagen

Durch die Schlüsselrolle personenbezogener Daten auf vielen digitalen Märkten und in den Geschäftsmodellen der Digitalkonzerne sind beide Marktversagen eng miteinander verwoben:

Beispielsweise kann sich einerseits die große Marktmacht der Digitalkonzerne negativ auf den Datenschutz auswirken. Durch das ungelöste Wettbewerbsproblem führt kaum ein Weg an den Diensten der Digitalkonzerne vorbei, wenn Verbraucher:innen am beruflichen und sozialen Gesellschaftsleben oder an der politischen Willensbildung teilhaben möchten. Hierdurch und darüber hinaus haben diese Unternehmen vielfältige Möglichkeiten, personenbezogene Daten über verschiedene Dienste hinweg zu erheben und über den Einsatz von Tracking-Technologien auf Drittanbieter-Webseiten im gesamten Internet zu sammeln. Dadurch verfügen Digitalkonzerne über die Möglichkeit, große Mengen personenbezogener Daten von ihren Nutzer:innen zu verarbeiten.[7]

Andererseits kann der überlegene Zugang zu personenbezogenen Daten zu einer weiteren Stärkung der wirtschaftlichen Macht der Digitalkonzerne führen, indem Marktzutrittsschranken erhöht und Konkurrenten ausgeschlossen werden. Gleichzeitig können Digitalkonzerne die große Informationsasymmetrie zwischen ihnen und den Verbraucher:innen auf vielfältige Weise zur Informations- und Verhaltensmanipulation nutzen.[8]

2. GEGENSEITIGE AUSWIRKUNGEN DER POLITIKFELDER „WETTBEWERB“ UND „DATENSCHUTZ“

Bisher wurden die Politikfelder „Wettbewerb“ und „Datenschutz“ zumeist strikt getrennt voneinander betrachtet. Zunehmend setzt sich jedoch die Einsicht durch, dass es zwischen diesen beiden Domänen vielfältige Interdependenzen gibt und dass daher eine

---

[5] Vgl. Kerber, Wolfgang; Specht-Riemenschneider, Louisa (2021) (wie Anm. 1), S. 18ff.

[6] Vgl. ebd., S. 29f.

[7] Vgl. ebd., S. 19.

[8] Vgl. ebd., S. 20. Sowie Martini, Mario u. a.: Dark Patterns 01 (2021), in: ZfDR - Zeitschrift für Digitalisierung und Recht, H. 1, URL: https://rsw.beck.de/docs/librariesprovider132/default-document-library/zfdr_heft_2021-01.pdf [Zugriff: 04.05.2021].

strikte Trennung nicht mehr zeitgemäß ist. So hat auf der einen Seite das Wettbewerbsrecht weitreichende Auswirkungen auf den Datenschutz, auf der anderen Seite kann sich auch das Datenschutzrecht auf den Wettbewerb auswirken. Diese Wechselwirkungen bieten die Chance für Synergien, können aber auch zu Konflikten führen.

2.1 Mögliche Auswirkungen des Wettbewerbsrechts auf den Datenschutz

Digitalkonzerne setzen beispielsweise ihre Markmacht dafür ein, den Nutzer:innen eine Einwilligung für das Zusammenführen von Daten der Nutzer:innen aus ihren verschiedenen Diensten und weiteren Quellen abzuringen. Darüber hinaus können wettbewerbsschädliche Praktiken wie Kopplung und Bündelung oder die Selbstbevorzugung eigener Dienste den Datenzugang der Digitalkonzerne weiter erhöhen. Dieser überlegene Zugang zu personenbezogenen Daten führt zu einer weiteren Stärkung der wirtschaftlichen Macht von Gatekeepern, indem Marktzutrittsschranken erhöht und Konkurrenten ausgeschlossen werden.[9] Wenn jedoch das Wettbewerbsrecht dieses Problem adäquat adressiert, kann es gleichzeitig positive Auswirkungen auf den Datenschutz haben und somit das Datenschutzrecht bei der Gewährleistung eines hohen Datenschutzniveaus unterstützen.

Das Wettbewerbsrecht kann jedoch auch in Konflikt mit dem Datenschutzrecht treten, beispielsweise, wenn Regelungen über den Datenzugang und die gemeinsame Nutzung von Daten, die dem Abbau von Marktzutrittsschranken dienen sollen, auch personenbezogen Daten erfassen. Auf der einen Seite könnte ein solcher Datenaustausch den Datenschutz beeinträchtigen, auf der anderen Seite setzt das Datenschutzrecht dem Umfang eines solchen Datenaustauschs enge Grenzen, was die Wirksamkeit dieses wettbewerbsrechtlichen Instruments beeinträchtigen kann. Dieses Problem könnte jedoch durch den Einsatz von fortgeschrittenen Anonymisierungstechniken sowie einer verbesserten Zusammenarbeit zwischen Wettbewerbs- und Datenschutzbehörden abgefedert werden.[10]

2.2 Mögliche Auswirkungen des Datenschutzrechts auf den Wettbewerb

Oftmals wird die Frage aufgeworfen, inwieweit das derzeitige Datenschutzrecht (also insbesondere die Datenschutz-Grundverordnung[11] (DSGVO)) negative Auswirkungen auf den Wettbewerb hat und die Digitalkonzerne begünstigen könnte, da diese leichter eine Einwilligung zur Datenverarbeitung erhalten könnten als andere (kleinere) Unternehmen.

Zwar mag die Annahme richtig sein, dass die Digitalkonzerne oft leichter eine Einwilligung für die Verarbeitung personenbezogener Daten erhalten (dahingestellt sei hier, ob eine solche Einwilligung den Anforderungen der DSGVO entspricht). Die Hauptgründe für diesen Wettbewerbsvorteil liegen jedoch – wie oben gezeigt – in der enormen Marktmacht der Digitalkonzerne. Denn da Verbraucher:innen es kaum vermeiden können, die Dienste der Digitalkonzerne zu nutzen, fällt es den Digitalkonzernen leicht, eine sehr weitreichende Zustimmung zur Verarbeitung personenbezogener Daten zu

[9] Vgl. ebd., S. 40f.

[10] Vgl. ebd., S. 46.

[11] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

erhalten. Gleichzeitig sind Verbraucher:innen oft nicht in der Lage, freiwillige und informierte Entscheidungen zur Verarbeitung ihrer personenbezogenen Daten zu treffen.[12]

Auf der Seite des Datenschutzrechts liegt das Problem vielmehr in der der mangelnden Durchsetzung der DSGVO. Dies spielt den Digitalkonzernen in die Hände, die Grenzen des Datenschutzrechts auszutesten und mögliche Lücken ausnutzen. Aufgrund ihrer enormen finanziellen Ressourcen können sie das Risiko von Rechtsstreitigkeiten sowie möglicher Geldstrafen deutlich leichter tragen, als andere Unternehmen.[13]

III. LÖSUNGSANSÄTZE

1. INTEGRATIVE BETRACHTUNG VON WETTBEWERBS- UND DATENSCHUTZRECHT

Die bisherigen Überlegungen zeigen, dass Wettbewerb und Datenschutz nicht grundsätzlich in Konflikt stehen, sondern sich vielmehr ungelöste Probleme in beiden Politikfeldern gegenseitig verstärken. Wenn also das Problem der Marktmacht gelöst und gleichzeitig die DSGVO ordnungsgemäß durchgesetzt würde, könnte man davon ausgehen, dass die meisten dieser ungerechtfertigten Wettbewerbsvorteile der Digitalkonzerne entfallen würden. Eine Absenkung des Datenschutzniveaus hingegen, beispielsweise durch eine weitere Auslegung der Rechtsgrundlage der Interessenabwägung oder erleichterte Möglichkeiten einer Datenverarbeitung zu anderen Zwecken, als zu denen die Daten ursprünglich erhoben wurden, wäre keine angemessene politische Antwort. Denn es wäre absehbar, dass die Digitalkonzerne deutlich besser in der Lage wären als andere Unternehmen, diese neuen Möglichkeiten der Datenverarbeitung auszunutzen – was die Marktmacht der Digitalkonzerne weiter festigen würde.[14]

Da, wie gezeigt, die verschiedenen Politikfelder eng miteinander verwoben sind, sollte statt der bisherigen strikten Trennung künftig vielmehr eine integrative und kooperative Betrachtung erfolgen. Dies bedeutet, dass das Wettbewerbsrecht auch den Datenschutz und das Datenschutzrecht auch Wettbewerbsfragen im Blick haben sollte, um gezielt Synergien zu nutzen und mögliche Konflikte zu entschärfen. Gleichzeitig sollte eine stärkere Kooperation der jeweiligen Aufsichtsbehörden erfolgen. Auf diese Weise würde sich die Chance erhöhen, die Ziele beider Politikbereiche, nämlich Wettbewerb und Datenschutz, besser zu erreichen.[15]

2. LÖSUNGSANSÄTZE IM DIGITAL MARKETS ACT

2.1 Weites Verständnis des Fairness-Prinzips im DMA

Die begriffliche Offenheit der Ziele des DMA „Anfechtbarkeit“ und „Fairness“ hat zu der Debatte geführt, ob der DMA nur eine andere (ex-ante-regulierende Form) der Wettbewerbspolitik ist, oder ob er bezogen auf den Begriff der Fairness auch weitere politische

[12] Vgl. Kerber, Wolfgang; Specht-Riemenschneider, Louisa (2021) (wie Anm. 1), S. 40f.

[13] Vgl. ebd., S. 37ff.

[14] Vgl. ebd., S. 41.

[15] Vgl. ebd., S. 52f.

Ziele verfolgen kann, wie zum Beispiel datenschutz- und verbraucherpolitische Ziele. Der DMA erkennt an, dass „das Verhalten von Gatekeepern zu schwerwiegenden Ungleichgewichten bei der Verhandlungsmacht und folglich zu unlauteren Praktiken und Bedingungen[16] für gewerbliche Nutzer und Endnutzer“ führt.[17] Gleichzeitig zielen die Verpflichtungen des DMA für Gatekeeper[18] primär darauf ab, gewerbliche Nutzer von unlauterem Verhalten zu schützen. Der Schutz der Verbraucher:innen soll daraus lediglich mittelbar, über verbesserte Wettbewerbsbedingungen erfolgen. Diese Inkonsistenz und Unklarheit des DMA hinsichtlich des Schutzes der Endnutzer:innen sollte aufgelöst werden:

> Der DMA sollte als Regulierung der Digitalkonzerne interpretiert werden, die neben dem Wettbewerb auch datenschutz- und verbraucherpolitische Ziele berücksichtigen sollte.[19]

> Da Verbraucher:innen mindestens in ähnlichem Maße wie gewerbliche Nutzer:innen von den Gatekeepern abhängig sind, sollten sie in gleichem Maße wie diese vor unlauteren Praktiken der Gatekeeper geschützt werden.[20] So sollte etwa bei der Aktualisierung der Verpflichtungen für Gatekeeper nach Artikel 10 DMA die Europäische Kommission nicht nur die unlautere Behandlung gewerblicher Nutzer:innen, sondern auch „unfaire“ Behandlung von Endnutzer:innen durch Gatekeeper berücksichtigen.

2.2 Untersagung der Zusammenführung von Daten

Gatekeeper können durch ihre Marktmacht leichter weitreichende Einwilligungen generieren, gleichzeitig sind Verbraucher:innen oft nicht in der Lage, freiwillige und informierte Entscheidungen zur Verarbeitung ihrer personenbezogenen Daten zu treffen. Vor diesem Hintergrund muss in Frage gestellt werden, ob der Vorschlag der EU-Kommission (Artikel 5(a) DMA), dass Gatekeeper personenbezogene Daten nur mit Einwilligung der Nutzer:innen aus ihren verschiedenen Diensten oder aus Diensten Dritter zusammenzuführen dürfen, überhaupt eine geeignete Maßnahme wäre, um die Wettbewerbsprobleme zu lösen, die durch die Kombination von Daten aus verschiedenen Quellen entstehen. Denn diese Abhilfemaßnahme würde sich nur dann positiv auf den Wettbewerb auswirken, wenn eine große Zahl von Nutzer:innen diese Zustimmung verweigert. Davon kann jedoch aufgrund der genannten Probleme nicht ausgegangen werden.

---

[16] „unfair practices and conditions“ im englischen Regelungsvorschlag der Kommission.

[17] Vgl. Europäische Kommission (wie Anm. 3), Recital (4).

[18] Vgl. ebd. Artikel 5 und Artikel 6. Auch bei der Aktualisierung der Verpflichtungen der Gatekeeper nach Artikel 10 DMA sollen unlautere Praktiken der Gatekeeper gegenüber Endnutzer:innen nicht berücksichtigt werden. Auch hier wird lediglich auf unlauteres Verhalten der Gatekeeper gegenüber gewerblichen Nutzern abgestellt.

[19] Vgl. Kerber, Wolfgang; Specht-Riemenschneider, Louisa (2021) (wie Anm. 1), S. 65ff.

[20] Vgl. auch Digital Regulation Project: Fairness and Contestability in the Digital Markets Act, Policy Discussion Paper No.3, S. 7 (2021). URL: https://tobin.yale.edu/sites/default/files/Digital%20Regulation%20Project%20Papers/Digital%20Regulation%20Project%20-%20Fairness%20and%20Contestability%20-%20Discussion%20Paper%20No%203.pdf [Zugriff 09.11.2021]; BEUC: Digital Markets Act proposal. Position Paper (2021). URL: https://www.beuc.eu/publications/beuc-x-2021-030_digital_markets_act_proposal.pdf [Zugriff 09.11.2021].

> Es ist sowohl aus der Perspektive des Wettbewerbs, als auch aus der Perspektive des Datenschutzes empfehlenswert, Gatekeepern über Artikel 5(a) DMA zu untersagen, Daten über ihre verschiedenen Dienste sowie über die Dienste anderer Anbieter (etwa Datenbroker) hinweg zu verknüpfen.[21]

2.3 Untersagung von „dark patterns“

Wie beschrieben, sind Verbraucher:innen unter anderem durch eine manipulative Gestaltung der Dienste von Digitalkonzernen mit Hilfe von „dark patterns“ nur schwer in der Lage, freiwillige und informierte Entscheidungen über die Verarbeitung ihrer personenbezogenen Daten zu treffen. Jedoch wird dieses Marktversagen bisher im DMA nicht ausreichend adressiert.

> Artikel 11 DMA sollte Gatekeepern explizit die Verwendung von „dark patterns“ untersagen, also die Nutzung einseitig gestalteter Benutzeroberflächen und Auswahlmenüs, die die Interessen von Gatekeepern begünstigen – zum Nachteil der Nutzer:innen.[22]

3. LÖSUNGSANSÄTZE IM DATENSCHUTZRECHT

3.1 Asymmetrische Regulierung im Datenschutzrecht

Darüber hinaus sollte künftig auch ein stärkerer Fokus auf die Möglichkeiten einer asymmetrischen Regulierung auch im Datenschutzrecht gelegt werden. Denn die Kombination aus der enormen Marktmacht der Digitalkonzerne mit der großen Informationsasymmetrie zwischen ihnen und den Verbraucher:innen führt auch zu weitaus höheren Risiken für das Recht auf Privatsphäre und das Recht auf den Schutz personenbezogener Daten, was strengere Datenschutzregelungen für diese Konzerne rechtfertigen kann.

Eine solche asymmetrische Regulierung ist auch grundsätzlich in der DSGVO angelegt. Denn obgleich die DSGVO primär eine horizontale Regelung darstellt, die gleichermaßen für alle Unternehmen gilt, liegt einigen ihrer Bestimmungen ein risikobasierter Ansatz zugrunde. Dies bedeutet, dass die DSGVO zwar einen Minimalstandard definiert, im Falle eines erhöhten Risikos der Datenverarbeitung aber strengere Vorgaben gelten (so müssen beispielsweise technische und organisatorische Maßnahmen, ein dem Risiko angemessenes Schutzniveau gewährleisten). Dieser risikobasierte Ansatz sollte mit Blick auf die Digitalkonzerne durch eine entsprechende Auslegung der DSGVO beziehungsweise durch entsprechende Leitlinien der europäischen Datenschutzbeauftragten weiter ausgebaut werden.[23]

So besagt beispielsweise Erwägungsgrund 43 der DSGVO, dass bei der Beurteilung, ob eine Einwilligung freiwillig erfolgt, berücksichtigt werden sollte, ob zwischen der be-

---

[21] Vgl. Kerber, Wolfgang; Specht-Riemenschneider, Louisa (2021) (wie Anm. 1), S. 69ff.

[22] Vgl. ebd., S. 89f. Ebenso: Verbraucherzentrale Bundesverband: Wahlfreiheit von Verbrauchern und effektiven Wettbewerb in digitalen Märkten sicherstellen. Positionspapier des vzbv zum Vorschlag der Europäischen Kommission für eine Verordnung über wettbewerbsfähige und faire digitale Märkte (Digital Markets Act), S. 16f (2021). URL: https://www.vzbv.de/publikationen/wahlfreiheit-fuer-nutzer-digitalen-maerkten-sicherstellen [Zugriff: 09.11.2021].

[23] Vgl. ebd., S. 98ff.

troffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht. Angesichts ihrer enormen Marktmacht, die bis zu einer quasi-Monopolstellung reicht, sollte in Bezug auf die Digitalkonzerne ein solches Ungleichgewicht angenommen werden.

> Dementsprechend muss bei Digitalkonzernen angenommen werden, dass eine Einwilligung nicht freiwillig erfolgen kann – soweit das Ungleichgewicht nicht abgefedert wird, beispielsweise indem eine alternative, kostenpflichtige Option zur Nutzung des Dienstes angeboten wird.[24]

Auch bei einer Interessenabwägung nach Artikel 6 Absatz 1 lit. f DSGVO könnten die Risiken in Betracht gezogen werden, die durch die beiden Marktversagen entstehen.

> Demnach sollten die schutzwürdigen Interessen der betroffenen Person stärker gewichtet werden, wenn es sich bei der datenverarbeitenden Stelle um einen marktmächtigen Digitalkonzern handelt, als wenn ein anderes Unternehmen die Daten verarbeiten möchte.[25]

> Darüber hinaus könnte es gerechtfertigt sein, besonders risikoträchtige Datenverarbeitungen durch Digitalkonzerne zu untersagen, wenn das Risiko für die betroffene Person die Interessen an der Datenverarbeitung eindeutig überwiegt und das Konzept der Einwilligung aufgrund der beiden Marktversagen nicht funktioniert.[26]

3.2 Verbesserte Rechtsdurchsetzung

Das Durchsetzungsdefizit einzelner Datenschutzbehörden kann auf der einen Seite auf fehlende Ressourcen zurückgeführt werden, es hat aber auf der anderen Seite auch noch weitere Gründe, wie insbesondere die Auswirkungen des „one-stop-shop-Prinzips“ und die daraus resultierende komplexe Zuständigkeitsstruktur. Dieses besagt, dass für die Durchsetzung der DSGVO grundsätzlich die jeweilige Aufsichtsbehörde am Ort der Hauptniederlassung eines für die Datenverarbeitung verantwortlichen Unternehmens federführend ist. Dieses „one-stop-shop-Prinzip“ mag zwar mehr Rechtssicherheit für die jeweiligen Unternehmen bringen, es resultiert aber gleichzeitig in einer uneinheitlichen Rechtsdurchsetzung in den verschiedenen Mitgliedstaaten. Handelt eine Aufsichtsbehörde bei Fragen, die eine grenzüberschreitende Datenverarbeitung betreffen, nicht angemessen, kommt ein kompliziertes Kohärenzverfahren zum Tragen, in dessen Rahmen die anderen betroffenen Aufsichtsbehörden beziehungsweise der Europäische Datenschutzausschuss intervenieren können. In Folge können sich entsprechende Durchsetzungsverfahren über viele Jahre hinweg ziehen.

> Abhilfe könnte eine finanziell angemessen ausgestattete Europäische Datenschutzbehörde bieten, an die der Europäische Datenschutzausschuss große, grenzüberschreitende Fälle übertragen könnte. So ließe sich verhindern, dass die Digitalkonzerne Standortvorteile mit Blick auf die unterschiedlichen Rechtsdurchsetzungspraktiken ausnutzen, gleichzeitig ließen sich die besonders risikobehafteten Datenverarbeitungen dieser Unternehmen sorgfältiger kontrollieren.[27]

---

[24] Vgl. ebd., S. 100ff.

[25] Vgl. ebd., S 102.

[26] Vgl. ebd., S. 102.

[27] Vgl. ebd., S. 103ff.