Gewährleistung effektiven Grundrechtsschutzes auf Grundlage des Kommissionsentwurfs für eine KI-Verordnung?

Zu den Unzulänglichkeiten des Regulierungskonzepts angesichts besonderer Herausforderungen der Aufsicht über datenverarbeitende Systeme

Mona Winau*

Eine effektive behördliche Aufsicht und Rechtsdurchsetzung sind besonders in von Vollzugsdefiziten geprägten Bereichen, wie bei der Regulierung datenverarbeitender Systeme, zentrale Elemente zur Gewährleistung eines effektiven Grundrechtsschutzes. Mit einem harmonisierten Rechtsrahmen verfolgt die EU-Kommission das Ziel grundrechtliche Werte im Zusammenhang mit sog. Künstlicher Intelligenz zu schützen. Ob das gewählte Regulierungskonzept geeignet ist dieses Ziel zu erreichen, begegnet Zweifeln.

I. Einleitung

Der von der EU-Kommission im April 2021 vorgelegte Entwurf einer europäischen Verordnung zur Regulierung Künstlicher Intelligenz (KI-VO-E)[1] soll einen einheitlichen Rechtsrahmen schaffen, der Innovation und Marktentwicklung im KI-Bereich unterstützt und zugleich ein hohes Schutzniveau für kollektive sowie individuelle Rechte und Rechtsgüter garantiert. Mit einem menschenzentrierten Regulierungsrahmen, der die Einhaltung von Grundrechten sichert, soll Vertrauen in Systeme der Künstlichen Intelligenz (vgl. Art. 3 Nr. 1) geschaffen werden. Die Gewährleistung des Grundrechtsschutzes und die Stärkung der dazu erforderlichen Rechtsdurchsetzungsinstrumente sind ausdrücklich formulierte Ziele des Kommissionsentwurfs.[2]

* Karlsruher Institut für Technologie, Institut für Informationssicherheit und Verlässlichkeit (KASTEL); mona.winau@kit.edu. Die vorliegende Arbeit wurde am Institut für Informationssicherheit und Verlässlichkeit (KASTEL), unterstützt vom Bundesministerium für Bildung und Forschung, entwickelt.

1 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union v. 21.04.2021, COM (2021) 206 final.

2 COM (2021) 206 final (s. Fn. 1), Begründung, 1.1; näher zum Grundrechtsschutz 3.5; EG 1 S. 2.

Für einen effektiven Grundrechtsschutz bedarf es einer funktionsfähigen behördlichen Aufsicht. Für das Datenschutzrecht hat der EuGH dies in Anknüpfung an Art. 16 Abs. 2 Satz 2 AEUV und Art. 8 Abs. 3 GrCh wiederholt betont.[3] Übertragen lässt sich dies auch auf die KI-Regulierung, denn die besondere Bedeutung der behördlichen Aufsicht folgt unter anderem aus spezifischen Schwierigkeiten des Vollzugs, die sich aus den Eigenarten des Regelungsgegenstands »Datenverarbeitung« ergeben.[4] Gerade in Bezug auf die Datenverarbeitung überschneiden sich die Regelungsgegenstände des Datenschutz- und des KI-Rechts. Während das Datenschutzrecht einen rechtlichen Rahmen für die Verarbeitung personenbezogener Daten schafft (Art. 2 Abs. 1 DSGVO), sollen durch die KI-Verordnung produktsicherheitsrechtliche Vorgaben für Systeme Künstlicher Intelligenz,[5] die personenbezogene und/oder nicht-personenbezogene Daten verarbeiten, geschaffen werden (Art. 1, Art. 3 Nr. 1 KI-VO-E). Die Ziele des europäischen Datenschutz- und KI-Rechts überschneiden sich, soweit es um den Schutz vor unverhältnismäßigen Grundrechtsbeeinträchtigungen geht, die mit Datenverarbeitungsvorgängen im Zusammenhang stehen. Die besonderen Vollzugsdefizite folgen aus Informations- und Machtasymmetrien, die zu einer wesentlichen Schwächung der Position Betroffener führen.[6]

Ein strukturelles Ungleichgewicht zuungunsten der Betroffenen besteht im Verbraucherrecht grundsätzlich, weil die Einblicke des Verbrauchers in unternehmerische Betriebsabläufe begrenzt sind, Verbraucher regelmäßig über weniger Ressourcen verfügen und nicht in gleicher Weise Zugang zu juristischem Wissen und Prozesserfahrung haben.[7] Im Zusammenhang mit Datenverarbeitungsprozessen sind die Ungleichgewichte besonders ausgeprägt, denn Datenverarbeitungen sind als solche nicht spürbar. Auch wenn durch sie verursachte negative Konsequenzen durchaus spürbar werden können, ist die dahinter stehende Datenschutzrechtsverletzung, wenn überhaupt, regelmäßig nur schwer erfass- und beweisbar.[8] Bei hoch komplexen automatisierten Verarbeitungsvorgängen, wie sie gerade Systemen der Künstlichen Intelligenz zugrundeliegen können, sind die Schwierigkeiten der Erkennbarkeit und Beweisbarkeit von Grundrechtsbeeinträchtigungen besonders ausgeprägt.[9] Sowohl für das Datenschutzrecht als auch für das KI-Recht ist daher zu befürchten, dass sich Betroffene, die eine Verletzung ihrer Rechte annehmen, auf Grundlage einer rationalen Betrachtung nach dem Kosten-Nutzen-Prinzip dennoch gegen eine aufwändige und kostenintensive Prozessführung bei ungewissen Erfolgsaussichten entscheiden werden.[10] Zum einen kann den Schwächen des Individualrechtsschutzes mit einer Stärkung privater Rechtsdurchsetzungsmöglichkeiten, etwa der Ergänzung um kollektive oder administrative Rechtsschutzelemente,[11] der Verschärfung von Informations- oder Auskunftspflichten der Anwender von KI-Systemen[12] und der Anpassung des Beweisrechts[13] begegnet werden. Zum anderen braucht es eine wirkmächtige staatliche Rechtsaufsicht und -durchsetzung.

Gegenstand der folgenden Betrachtung ist das Regulierungskonzept nach dem Kommissionsentwurf, das die Einhaltung und Durchsetzung des KI-Rechts sicherstellen soll. Auf einen Überblick zum Regulierungskonzept, insbesondere zu den Aufsichtsstrukturen (II.), folgt eine Analyse und kritische Betrachtung der Eignung zur Gewährleistung des angestrebten Grundrechtsschutzes (III.). Dabei wird zunächst das Erfordernis einer wirkmächtigen behördlichen Aufsicht vor dem Hintergrund selbstregulativer Elemente im Regulierungskonzept dargestellt (1.). Im Fokus steht das Problem einer zu befürchtenden unzureichenden Ressourcenausstattung der Aufsichtsbehörden (2.). Aufgezeigt werden auch Schwächen, die der gewählte rein produktsicherheitsrechtliche Ansatz unter Verzicht auf subjektive Rechte mit sich bringt (3.).

II. Regulierungs- und Vollzugskonzept im KI-VO-E

1. Risikobasiertes Produktsicherheitsrecht

Ziel des Kommissionsentwurfs zur KI-Regulierung soll zwar unter anderem der Schutz von Grundrechten sein, der konzeptionelle Ansatz beschränkt sich allerdings auf produktsicherheitsrechtliche Vorgaben, ohne dass subjektive Rechte für betroffene Personen vorgesehen sind. Rechte betroffener Personen im Zusammenhang mit dem Betrieb von KI-Systemen sind folglich auf solche aus bereichsspezifischen Gesetzen, wie etwa dem Antidiskriminierungsrecht oder dem Datenschutzrecht, beschränkt.

Das Regulierungskonzept ist risikobasiert. Nach Art. 5 sind bestimmte, als besonders risikoreich eingestufte KI-Systeme – z.B. Systeme zur unterschwelligen Verhaltensbeeinflussung, die das Risiko eines physischen oder psychsichen Schadens für Betroffene bergen können (Abs. 1 Buchst. a) – absolut bzw. grundsätzlich verboten. Für das Inverkehrbringen und die Inbetriebnahme von Hoch-Risiko-KI-Systemen nach Art. 6 formuliert der Entwurf eine Reihe an materiellen und prozeduralen Anforderungen, die etwa das Risiko-Management

3 Zur primären Funktion der Datenschutzaufsicht als Grundrechtshüter, EuGH 09.03.2010, C-518/07 – Kommission/Deutschland, Rn. 21 ff., insb. 23; EuGH 16.10.2016, C-614/10 – Kommission/Österreich, Rn. 36; EuGH 08.04.2014 – Kommission/Ungarn, Rn. 47 f.

4 Kröger/Pilniok/*Spiecker gen. Döhmann*, Unabhängiges Verwalten in der Europäischen Union, 2016, S. 97, 105.

5 Zur Begriffsdefinition nach Art. 3 Nr. 1 KI-VO-E i.V.m. Anhang I und der Kritik an deren Breite *Straub* ZdiW 2022, 71, 71 f.

6 Vgl. Kröger/Pilniok/*Spiecker gen. Döhmann* (s. Fn. 4), S. 97, 104 ff.; *Lancieri* Maine Law Review 74 (2022), 15, 29 ff.

7 Sachverständigenrat für Verbraucherfragen (SVRV), Verbrauchergerechtes Scoring, 2018, S. 40 m.w.N., https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Verbrauchergerechtes_Scoring.pdf [15.11.2022].

8 Kröger/Pilniok/*Spiecker gen. Döhmann* (s. Fn. 4), S. 97, 105 f.; *Golla* JIPITEC 2017, 70, 72 Rn. 9; *Busch*, Algorithmic Accountability, 2018, S. 50, https://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Algorithmic%20Accountability.pdf [15.11.2022].

9 Vgl. zur Komplexität sog. statistischer Diskriminierungen *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen, 2019, S. 28 ff., https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/publikationen/Expertisen/studie_diskriminierungsrisiken_durch_verwendung_von_algorithmen.pdf [15.11.2022].

10 Vgl. *Busch* (s. Fn. 8), S. 52; *Golla* JIPITEC 2017, 70, 71 f. Rn. 7 ff.; *Lancieri* Maine Law Review 74 (2022), 15, 41; Kröger/Pilniok/*Spiecker gen. Döhmann* (s. Fn. 4), S. 97, 106; *Podszun/Busch/Hennig-Bodewig*, Behördliche Durchsetzung des Verbraucherrechts?, 2018, S. 174.

11 Vgl. *Martini* JZ 2017, 1017, 1024; *Orwat* (s. Fn. 9), S. 108; Sachverständigenrat für Verbraucherfragen (SVRV) (s. Fn. 7), S. 40.

12 Vgl. *Orwat* (s. Fn. 9), S. 109; Sachverständigenrat für Verbraucherfragen (SVRV) (s. Fn. 7), S. 40. Teilweise sieht bereits die KI-Verordnung strengere Informationspflichten auch für die Anwender von KI-Systemen vor. So statuiert Art. 52 etwa Transparenzpflichten für bestimmte KI-Systeme und soll mit Art. 60 eine EU-Datenbank für eigenständige Hochrisiko-Systeme eingerichtet werden. Zudem sind weitgehende Zugriffsrechte der Aufsichtsbehörden vorgesehen (Art. 64).

13 *Martini* JZ 2017, 1017, 1023 f. Vgl. zu gegenwärtigen Reformvorhaben im Produktsicherheitsrecht die Vorschläge der EU-Kommission für eine überarbeitete Produkthaftungs-Richtlinie [COM (2022) 495 final] und eine KI-Haftungs-Richtlinie [COM (2022) 496 final].

(Art. 9), die Datenauswahl und -verwaltung (Art. 10) sowie die Dokumentation (Art. 11, 12), Transparenz (Art. 13), Kontrollierbarkeit (Art. 14) und Sicherheit (Art. 15) betreffen. Für KI-Systeme unterhalb der Schwelle eines hohen Risikos sind im Entwurf keine verbindlichen Vorgaben vorgesehen, allerdings soll eine freiwillige Bindung an die Vorgaben für Hoch-Risiko-Systeme unterstützt werden. Dazu fördern und erleichtern die Kommission und die Mitgliedstaaten die Aufstellung von Verhaltenskodizes durch die Anbieter von KI-Systemen oder deren Interessenvertretungen (Art. 69).[14]

2. Präventive (Selbst-)Regulierung: Das Konformitätsbewertungsverfahren

Die Konformität der Hoch-Risiko-Systeme (vgl. Art. 6) mit den Verordnungsregelungen soll durch ein grundsätzlich internes, vom Hersteller selbst durchzuführendes Konformitätsbewertungsverfahren gem. Art. 19 Abs. 1, Art. 43 Abs. 1 (a) i.V.m. Anhang VI vor dem Inverkehrbringen eines KI-Systems sichergestellt werden. Eine Ausnahme besteht ausschließlich für biometrische Fernidentifizierungssysteme nach Anhang III Nr. 5.[15] Für sie muss ein externes Konformitätsbewertungsverfahren durch eine notifizierte Stelle durchgeführt werden (Art. 43 Abs. 2 Satz 2). Die Benennung notifizierter Stellen und die Aufsicht über sie obliegt Notifizierungsbehörden, die in den Mitgliedstaaten einzurichten sind (Art. 30). Ihre Einrichtung und Organisation muss sicherstellen, dass Interessenkonflikte mit Konformitätsbewertungsstellen vermieden werden und diese ihre Aufgaben objektiv und unparteilich wahrnehmen (Art. 30 Abs. 3).

3. Aufsicht und Rechtsdurchsetzung im Rahmen der Marktüberwachung

Nach dem Inverkehrbringen der Systeme erfolgt eine behördliche Aufsicht über ihre Konformität durch spezielle Marktüberwachungsbehörden in den Mitgliedstaaten. Ihre organisatorische Struktur muss die Objektivität und Unparteilichkeit ihrer Aufgabenwahrnehmung sicherstellen (Art. 59 Abs. 1). Die Aufgaben der Marktüberwachung sowie der Notifizierung sollen grundätzlich durch eine ausgewählte Behörde unter den zuständigen nationalen Behörden eines Mitgliedstaats wahrgenommen werden, wenn nicht organisatorische und administrative Gründe des jeweiligen Mitgliedstaats die Benennung von mehr als einer Behörde erfordern (Art. 59 Abs. 2). Die ausgewählte Behörde fungiert zudem als Ansprechpartner für die Mitgliedstaaten und die Kommission. Sie entsendet außerdem einen Vertreter in den Europäischen Ausschuss (Art. 3 Nr. 42).[16]

Gem. Art. 63 Abs. 1 KI-VO-E gilt die EU-Marktüberwachungsverordnung (VO (EU) 2019/1020), soweit der Verordnungsentwurf keine spezielleren Regelungen trifft.[17] Die Kompetenz anderer Behörden, die für den Grundrechtsschutz im Zusammenhang mit der Anwendung von KI-Systemen zuständig sind, bleibt unberührt. Solche anderen Behörden sind etwa die Datenschutzaufsichtsbehörden und die Antidiskriminierungsstelle des Bundes.[18] Deren Zuständigkeit bleibt allerdings auf die Überprüfung der Einhaltung des Datenschutzrechts (vgl. Art. 54 Abs. 1 DSGVO) beziehungsweise auf die Aufgaben nach § 27 AGG zur Förderung der Gleichstellung beschränkt. Sie werden durch den Verordnungsentwurf zudem mit Zugriffsrechten auf die obligatorisch anzufertigenden Dokumentationen zum KI-System ausgestattet, soweit sie zur Erfüllung ihrer Aufgaben notwendig sind (Art. 64 Abs. 3). Genügt der Zugriff auf die Dokumentationen für die Feststellung eines Unionsrechtsverstoßes nicht, können die anderen zuständigen Behörden nach Art. 64 Abs. 5 einen »begründeten Antrag« bei der Marktüberwachungsbehörde stellen, damit diese das jeweilige KI-System überprüft. Die von der Marktüberwachungsbehörde durchgeführte Überprüfung hat unter enger Einbeziehung der antragstellenden Behörde zu erfolgen (S. 2). Zur Wahrnehmung ihrer Aufgaben können die Marktüberwachungsbehörden Einsicht in sämtliche Trainings-, Validierungs- und Testdatensätze und, wenn zur Bewertung der Konformität eines Hoch-Risiko-Systems mit den Anforderungen der Verordnung notwendig, sogar Zugriff auf den Quellcode des Systems verlangen (Art. 64 Abs. 1, 2).

Das Marktüberwachungskonzept schließt ebenfalls selbstregulative Elemente ein. Hersteller von Hoch-Risiko-KI-Systemen müssen ein System zur Produktüberwachung nach dem Inverkehrbringen einrichten (Art. 61) und den zuständigen Marktüberwachungsbehörden von Verstößen gegen grundrechtsschützendes Unionsrechts berichten (Art. 62 Abs. 1).

Für KI-Systeme mit einem Risiko auf nationaler Ebene[19] gelten spezielle behördliche Überprüfungs-, Unterrichtungs- und Abhilfepflichten (Art. 65).[20] Subsidiär gelten die allgemeinen Aufgaben- und Befugniszuweisungen aus Art. 11 Marktüberwachungsverordnung bzw. § 7 Abs. 1 Satz 1 Marktüberwachungsgesetz (MüG) i.V.m. Art. 14 Abs. 4 und 5 EU-Marktüberwachungsverordnung (MÜ-VO). Darunter fallen etwa die Befugnisse zu unangekündigten Inspektionen (Abs. 4 Buchst. d) und zum Verhängen von Sanktionen (Abs. 4 Buchst. i). Bei Feststellung der Nichtkonformität eines Systems sind geeignete Abhilfemaßnahmen anzuordnen und, wenn erforderlich, auch Korrekturmaßnahmen, einschließlich des Verbots respektive der Einschränkung des Inverkehrbringens eines Produktes und dessen Rückruf, zu ergreifen (Art. 65 Abs. 2 und 5 KI-VO-E, § 8 Abs. 2 Satz 1 MüG i.V.m. Art. 16 Abs. 2 und 5 MÜ-VO).[21]

Zusätzlich zur grenzüberschreitenden Amtshilfe (Kapitel VI) sowie dem Koordinations- und Kooperationsnetzwerk (Kapitel VIII) der Marktüberwachungsverordnung soll eine unionsweite Datenbank für KI-Systeme als Informationsbasis für die Behörden (Art. 60) eingerichtet und die Vernetzung der mitgliedstaatlichen Behörden über den Europäischen Ausschuss für Künstliche Intelligenz (Art. 56) institutionalisiert

14 Vgl. zu den Risikokategorien *Ebert/Spiecker gen. Döhmann* NVwZ 2021, 1188, 1189 f.; *Orssich* EuZW 2022, 254, 255 ff.; *Straub* ZdiW 2022, 71, 71 ff.; *Bleckat* ZdiW 2021, 293, 294 f.

15 Der Anwendungsbereich des externen Konformitätsbewertungsverfahrens ist bewusst wegen der umfassenderen Erfahrung von Zertifizierern im Bereich der Produktsicherheit auf biometrische Fernidentifizierungssysteme beschränkt und kann vorläufig sein, EG 64; vgl. auch *Roth-Isigkeit* ZRP 2022, 187, 188 f.

16 Näher zu den Funktionen der nationalen Aufsichtsbehörden, Notifizierungs- und Marktüberwachungsbehörden und zu Möglichkeiten der Behördenorganisation in Deutschland *Roth-Isigkeit* ZRP 2022, 187, 187 f.

17 Vgl. EG 79; *Geiß/Felz* NJW 2019, 2961, 2962; *Roos/Weitz* MMR 2021, 844, 846.

18 Vgl. dazu EG 79 S. 2.

19 Systeme, mit denen ein Risiko für unionsrechtliche geschützte öffentliche Interessen wie etwa Gesundheit oder Arbeitssicherheit verbunden ist, das über das hinausgeht, was in Anbetracht der Zweckbestimmung normalerweise vernünftig und vertretbar wäre (Art. 65 Abs. 1 KI-VO-E i.V.m. Art. 3 Nr. 19 MÜ-VO).

20 Näher dazu *Roth-Isigkeit* ZRP 2022, 187, 190.

21 Ausführlicher zur Marktüberwachung *Roth-Isigkeit* ZRP 2022, 187, 189 f.

werden. Der Ausschuss ist aus den Vertretern der Marktaufsichtsbehörden jedes Mitgliedsstaats und dem Europäischen Datenschutzbeauftragten zusammengesetzt (Art. 57). Er soll die Kommission insbesondere bei der Gewährleistung einer effektiven Zusammenarbeit der nationalen Aufsichtsbehörden, den Binnenmarkt betreffenden, aktuellen Angelegenheiten sowie der einheitlichen Anwendung der Verordnung beraten und unterstützen (Art. 56 Abs. 2).

III. Effektiver Grundrechtsschutz durch den KI-VO-E

Die Schaffung eines besonderen Rechtsrahmens für KI-Systeme und die Absicherung der Einhaltung dieser Regelungen durch das präventive Konformitätsbewertungsverfahren sowie eine kontinuierliche Überwachung nach dem Inverkehrbringen durch die Marktüberwachungsbehörden bilden die notwendige Grundlage für einen effektiven Grundrechtsschutz. Auch um den umfangreich vorgesehenen selbstregulativen Elementen größtmögliche Wirksamkeit zu verleihen, bedarf es einer effektiv arbeitenden behördlichen Aufsicht. Die Basis dafür wird im Kommissionsentwurf durch die oben genannten spezifischen Befugnisse der Aufsichtsbehörden für den Grundrechtsschutzschutz im Zusammenhang mit KI-Systemen sowie durch Strukturen für deren Vernetzung, Kooperation und den kohärenten Vollzug geschaffen. Bedenken ergeben sich allerdings in Bezug auf die Gewährleistung einer hinreichenden Ausstattung der Behörden, die für eine angemessene Erfüllung ihrer Aufgaben zwingend ist. Überdies fehlt es im KI-VO-E an Betroffenenrechten.

1. Selbstregulative Elemente und Anreizstruktur

Die weitgehende Integration selbstregulativer Elemente in das Vollzugskonzept begegnet Bedenken, soweit es an einer wirksamen Anreizstruktur für deren angemessenen Befolgung fehlt. Den bekannten Interessenkonflikten, die sich aus dem Zusammenfallen der Rolle des Regulierers und des Regulierten ergeben, kann von der Seite des Rechts durch starke Anreize für die Einhaltung rechtlicher Pflichten oder gegen Rechtsverstöße begegnet werden.[22] Der Verordnungsentwurf arbeitet diesbezüglich vor allem mit Negativanreizen in Form von starken Untersuchungs- und Abhilfebefugnissen der Marktüberwachungsbehörden, insbesondere der Verhängung hoher Bußgelder. So drohen etwa für einen Verstoß gegen die Daten- und Daten-Governance-Vorgaben aus Art. 10 Geldbußen bis zu 30.000.000 € oder 6 % des weltweiten Jahresumsatzes eines Unternehmens (Art. 71 Abs. 3), ferner für die Nichtkonformität eines Systems bis zu 20.000.000 € oder 4 % des weltweiten Jahresumsatzes (Art. 71 Abs. 4). Für die Wirksamkeit des Anreizes ist allerdings nicht nur das Ausmaß, sondern auch die Eintrittswahrscheinlichkeit der negativen Konsequenzen relevant. Ist die Verhängung eines behördlichen Bußgeldes unwahrscheinlich, mindert dies die Anreizfunktion seiner noch so hoch angesetzten Androhung.[23] Aus dem Wortlaut der Art. 71 Abs. 2–5 »werden Geldbußen […] verhängt« und ihrer ausdrücklich vorgesehenen abschreckenden Wirkung (Abs. 1 Satz 2) lässt sich zwar ableiten, dass die Entscheidung der zuständigen Behörden, im Fall eines festgestellten Verstoßes Bußgelder zu verhängen, eine gebundene ist, sie also zur Verhängung eines Bußgelds verpflichtet sind, und sich ihr Ermessenspielraum auf die Bußgeldzumessung beschränkt.[24] Damit es tatsächlich zu einer Bußgeldverhängung für Rechtsverstöße kommt, muss aber erstmal eine Überprüfung des Systems durch die Behörde erfolgen, in deren Rahmen der Verstoß festgestellt wird. Ein wirksamer Grundrechtsschutz auf Grundlage des selbstregulativ abgestützten Regulierungskonzepts ist folglich auf eine effektiv arbeitende behördliche Aufsicht angewiesen.

2. Unzureichende Ressourcen – Die Datenschutzaufsicht als Lehrstück

Am Beispiel des Vollzugsdefizits im Datenschutzrecht wird deutlich, dass die staatliche Aufsicht über Datenverarbeitungsvorgänge bzw. datenverarbeitende Technologien eine »Herkulesaufgabe« ist, deren angemessene Bewältigung häufig aufgrund mangelhafter Ausstattung der zuständigen Behörden scheitert. Die mit der voranschreitenden Digitalisierung verbundene stetig wachsende Menge an verarbeiteten Daten und die steigende Zahl der zu kontrollierenden Akteure bzw. Produkte führt zu einer immensen Aufgabenlast. Zusätzlich nimmt mit der technischen Entwicklung und der Entstehung internationaler, netzwerkartiger Geschäftsmodelle die Komplexität der zu kontrollierenden Materien zu, so dass Aufsichtsmaßnahmen arbeitsintensiver werden sowie ein besonders hohes Maß an technischer Expertise erfordern.[25]

Das Vollzugsdefizit zu reduzieren war gleichwohl ein zentrales Ziel bei der Harmonisierung und Reformierung des europäischen Datenschutzrechts.[26] Hierzu wurden behördliche Aufgaben und Kompetenzen erweitert und neue Verfahren der Kooperation und Kohärenzsicherung geschaffen.[27] Neben strukturellen Defiziten des reformierten Unionsrechts, die insbesondere für grenzüberschreitende Datenverarbeitungsprozesse im Zusammenhang mit dem One-Stop-Shop-Prinzip analysiert wurden,[28] liegt eine zentrale Ursache für das verbleibende Vollzugsdefizit in der unzureichenden Ressourcenausstattung der Behörden.[29] Wie sich aus einem Bericht des Irish Council for Civil Liberties (ICCL) ergibt, belief sich 2021 der Anteil Deutschlands an den europäischen Gesamtausgaben für die Datenschutzaufsicht fast auf ein Drittel.[30]

22 Vgl. dazu *Winau/Kaiser/Schultmann/Wiens/Spiecker gen. Döhmann* LNI-Proceedings INFORMATIK 2021, 999; zum Effekt der hohen Sanktionsandrohungen in der DSGVO, *Weichert* DuD 2020, 293, 296; Roßnagel/Friedewald/*Karaboga/Martin/Friedewald*, Die Zukunft von Privatheit und Selbstbestimmung, 2022, S. 49, 77 ff.

23 Vgl. jeweils m.w.N. *Winau/Kaiser/Schultmann/Wiens/Spiecker gen. Döhmann* LNI-Proceedings INFORMATIK 2021, 999, 1005 ff.; Roßnagel/Friedewald/*Karaboga/Martin/Friedewald* (s. Fn. 22), S. 49, 78.

24 Vgl. zur Auslegung des Art. 83 Abs. 4–6 DSGVO, der die gleiche Formulierung trifft, Simitis/Hornung/Spiecker gen. Döhmann/*Boehm*, Datenschutzrecht, 2019, Art. 83 DSGVO Rn. 15 ff.

25 Vgl. auch *Römer/Ulbricht*, Datenschutzaufsicht, S. 8; in Bezug auf den Individualrechtsschutz *Spiecker gen. Döhmann* KritV 2014, 28, 41 f.; *dies*. K&R 2012, 717, 720.

26 Simitis/Hornung/Spiecker gen. Döhmann/*Albrecht* (s. Fn. 24), Einleitung Rn. 186, Simitis/*Hornung/Spiecker gen. Döhmann*, ebd., Rn. 209.

27 Vgl. die Übersicht zu Neuerungen der DSGVO bei Simitis/*Hornung/Spiecker gen. Döhmann* (s. Fn. 24), Einleitung Rn. 213.

28 *Gentile/Lynskey* International and Comparative Law Quarterly 2022, 799; *Bretthauer* Common Market Law Review 2022, 1, 7 ff.

29 Vgl. auch *Weichert* DuD 2020, 293, 296; *Römer/Ulbricht* (s. Fn. 25), S. 6; *Golla* JIPITEC 2017, 70, 72 Rn. 12; *Smuha* et al., How the EU can achieve legally trustworthy AI, 2021, S. 47; *Lancieri* Maine Law Review 74 (2022), 15, 52 ff.

30 ICCL Europe's enforcement paralysis, 2021, https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf [15.11.2022]; vgl. auch die, allerdings auf älteren Zahlen basierende, Übersicht zum Budget der Aufsichtsbehörden in der EU bei Roßnagel/Friedewald/*Schütz*, Die Fortentwicklung des Datenschutzes, 2018, S. 252, 253 ff.

Zwar dürfte die Unterhaltung von insgesamt 18 Datenschutzaufsichtsbehörden in Deutschland[31] kostenaufwändiger sein als eine zentral organisierte Behörde, wie sie in anderen Mitgliedstaaten besteht, allein damit dürfte sich der erhebliche deutsche Anteil an den Gesamtausgaben aber nicht erklären lassen. Hinzu kommt, dass auch einzelne deutsche Datenschutzaufsichtsbehörden über eine unzureichende Ressourcenausstattung klagen.[32] Nach den Zahlen der DPA verfügten die Hälfte der europäischen Datenschutzaufsichtsbehörden über weniger als 5.000.000 € Jahresbudget und der Anteil an technisch spezialisierten Vollzeitkräften belief sich bei den europäischen Aufsichtsbehörden insgesamt auf nur 9,7 %.[33] Besonders gravierend ist ein unzureichendes Budget, wenn es mit einer erheblichen Aufgabenlast zusammenfällt, wie das Beispiel Irland zeigt. Die DPC (Irish Data Protection Commission), die für eine unverhältnismäßig große Zahl bedeutender Tech-Unternehmen federführend zuständig ist, ließ nahezu 98 % der bedeutenden Datenschutzfälle in ihrem Zuständigkeitsbereich ungelöst.[34]

Zwar sind die Mitgliedstaaten gem. Art. 52 Abs. 4 DSGVO verpflichtet ihre Behörden angemessenen mit personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen auszustatten, um eine effektive Aufgabenwahrnehmung zu ermöglichen, jedoch erweist sich die Norm in der Praxis als stumpfes Schwert.[35] Von den Aufsichtsbehörden selbst ist die Vorschrift nicht einklagbar. Zwar ist es Aufgabe der Kommission für die Einhaltung des Unionsrechts durch die Mitgliedstaaten zu sorgen (Art. 17 Abs. 1 Satz 3 EUV)[36] und könnte sie ein Vertragsverletzungsverfahren gegen den betreffenden Mitgliedstaat einleiten (Art. 258 AEUV).[37] Tatsächlich scheint dies angesichts der Untätigkeit der Kommission in Bezug auf die unzureichende Ausstattung der Datenschutzaufsicht jedoch ein geringes Risiko zu sein.[38]

Im Kommissionsentwurf findet sich eine vergleichbare Vorschrift in Art. 59 Abs. 4 Satz 1 KI-VO-E. Die Mitgliedstaaten haben für eine angemessene Ausstattung mit finanziellen und personellen Ressourcen zu sorgen. Satz 2 spezifiziert, dass sie ständig über eine ausreichende Zahl an Mitarbeitern verfügen müssen, die »ein tiefes Verständnis der Technologien der künstlichen Intelligenz, der Daten und Datenverarbeitung, der Grundrechte und Gesundheits- und Sicherheitsrisiken sowie [über] die Kenntnis der bestehenden Normen und rechtlichen Anforderungen« mitbringen. Neu ist im Vergleich zur DSGVO zudem die Einführung eines Berichtsverfahrens hinsichtlich der Ressourcenausstattung in Abs. 5. Die Mitgliedstaaten haben der Kommission jährlich einen Bericht über den Stand der finanziellen und personellen Ressourcen der zuständigen Behörden inklusive einer Bewertung ihrer Angemessenheit vorzulegen. Die Kommission leitet die Informationen an den Ausschuss weiter, wo sie erörtert werden. Der Ausschuss kann eine Empfehlung abgeben.

Grundsätzlich sind die Spezifizierung hinsichtlich der erforderlichen Fachexpertise und die Ergänzung um das Berichtsverfahren zu begrüßen. Dass hierdurch eine angemessene Ressourcenausstattung der Behörden erreicht werden kann, ist allerdings zweifelhaft. Zunächst bleiben Einzelheiten des Berichtsverfahrens unklar und mögliche Konsequenzen eines Berichts über eine unzureichende Ressourcenausstattung vage. So stellt sich etwa die Frage, auf welcher Grundlage die Mitgliedstaaten ihre Bewertung der Angemessenheit der Ressourcenausstattung zu treffen haben. Der Begriff der Angemessenheit der Mittel in Art. 58 Abs. 4 Satz 1 ist von einer gewissen Unschärfe geprägt.[39] Zwar lässt sich aus dem zweiten Halbsatz ableiten, dass die Mittel zur Wahrnehmung der behördlichen Aufgaben ausreichen müssen, dies schafft allerdings nur begrenzt Klarheit.[40] Der von der Kommission abgeschätzte Bedarf über nur eine bis fünfundzwanzig Vollzeitkräften[41] lässt einen erheblichen Spielraum. Auch begegnet diese Bedarfsprognose angesichts der umfangreichen und komplexen Aufgaben der Behörden Zweifeln.[42] Es bleibt die Frage, ab welcher Kontrolldichte die Überwachungsaufgabe angemessen wahrgenommen wird, so dass die negativen Anreize wie insbesondere die Bußgeldandrohung effektiv wirken. Um die mitgliedstaatliche Bewertung der Angemessenheit auf eine solidere Grundlage zu stellen, könnten bspw. unabhängige Gutachten zur Einschätzung des Ressourcenbedarfs,[43] der für eine angemessene Regelungsdichte im jeweiligen Mitgliedstaat erforderlich wäre, gefordert werden. Ebenso sollte eine Pflicht, die mitgliedstaatlichen Aufsichtsbehörden in die Bewertung miteinzubeziehen oder zumindest ihre jährlichen Tätigkeitsberichte heranzuziehen, in Betracht gezogen werden.

31 16 Landesdatenschutzbeauftragte, das Bayerische Landesamt für Datenschutzaufsicht und der Bundesdatenschutzbeauftragte.

32 Z.B. LfDI M-V Tätigkeitsbericht 2021, S. 10, https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb17.pdf [15.11.2022]; LfDI Saarland, Tätigkeitsbericht 2021, S. 28, https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb30_DS_2021.pdf [15.11.2022]; LfDI Hamburg, Tätigkeitsbericht 2021, S. 7, https://datenschutz-hamburg.de/assets/pdf/30._taetigkeitsbericht_datenschutz_2021.PDF [15.11.2022]; zu den erheblichen Unterschieden der Behördenausstattung in den Bundesländern,vgl. Roßnagel/Friedewald/*Schütz* (s. Fn. 30), S. 251, 258 ff.

33 ICCL Europe's enforcement paralysis (s. Fn. 30), S. 3.

34 ICCL Europe's enforcement paralysis (s. Fn. 30), S. 3. Beispielhaft ist auch der Fall des Nichteinschreitens der irischen Behörde gegenüber Facebook wegen veränderter Nutzungs- und Datenschutzbedingungen des Messenger-Dienstes WhatsApp, das zum ersten Dringlichkeitsverfahren nach Art. 66 DSGVO geführt hat, dazu *Bretthauer*, in: Verfassungsblog, Hamburg schreitet ein, 14.05.2021, https://verfassungsblog.de/hamburg-schreitet-ein/ [15.11.2022].

35 Vgl. auch *Bretthauer* Common Market Law Review 2022, 1, 11.

36 Näher zur Funktion der EU-Kommission als »Hüterin des Unionsrechts« Callies/*Ruffert*, EUV/AEUV, 6. Aufl. 2022, Art. 17 EUV Rn. 7 ff.

37 Für eine weitergehende Überwachung der Ressourcenausstattung und gegebenenfalls ein Tätigkeitwerden der Kommission *Bretthauer* Common Market Law Review 2022, 1, 11.

38 Als »kein besonders scharfes Schwert« bewertet *Roßnagel* die Androhung eines Vertragsverletzungsverfahrens auch in Bezug auf unionsrechtswidrige Datenschutz-Gesetzgebung in den Mitgliedstaaten, MMR 2020, 657, 661.

39 Vgl. zur Parallellnorm in Art. 52 Abs. 4 DSGVO Wolff/Brink/*Schneider*, BeckOK DSchR, 41. Lfg. 2022, Art. 52 DSGVO Rn. 25; Kühling/Buchner/*Boehm*, DS-GVO/BDSG, 3. Aufl. 2020, Art. 52 DSGVO Rn. 24.

40 Die Grenze des gesetzgeberischen Einschätzungsspielraums dürfte nicht erst, aber jedenfalls dann, erreicht sein, wenn die Aufsichtsbehörden mangels finanzieller Mittel nicht in der Lage sind bestimmte Aufgaben überhaupt wahrzunehmen, etwa wenn von der Verhängung von Bußgeldern abgesehen werden muss, weil das Budget etwaige Prozesskosten nicht abdeckt, Simitis/Hornung/Spiecker gen. Döhmann/*Polenz* (s. Fn. 24), Art. 52 DSGVO Rn. 16; so auch Wolff/Brink/*Schneider* (s. Fn. 39), Art. 52 DSGVO Rn. 25.

41 COM (2021) 206 final (s. Fn. 1), Begründung, S. 13.

42 So auch ICCL, Flaws in ex-post enforcement in the AI-Act, 2022, S. 3, https://www.iccl.ie/news/flaws-in-ex-post-enforcement-in-the-ai-act/ [15.11.2022]; *Veale/Borgesius* Cri 2021, 97, 111 Rn. 102.

43 Anlässlich der Einführung der DSGVO wurde etwa ein Gutachten über die erhöhte Arbeitslast von den Landesdatenschutzaufsichtsbehörden in Auftrag gegeben: *Roßnagel*, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, 2017.

Die Konsequenzen für einen Mitgliedstaat, der über die unzureichende behördliche Ausstattung berichtet, sind zaghaft gewählt. Nach Erörterung der Ressourcenbewertung kann der Ausschuss eine Empfehlung aussprechen. Nicht ausdrücklich benannt, aber aus dem Normkontext ableitbar ist, dass Adressat der Empfehlung der betreffende Mitgliedstaat ist. Worauf sich die Empfehlung konkret beziehen sollte, etwa auf einen zahlmäßig bestimmten Bedarf an Personal oder Mitteln oder auf das zur Verfügung zu stellende Budget, lässt der Gesetzestext ebenfalls offen. Jedenfalls dürfte eine bloße Empfehlung des Ausschusses ohnehin kein besonders wirksames Druckmittel gegenüber Mitgliedstaaten, die nicht bereit sind, mehr finanzielle Mittel für ihre Aufsichtsbehörden zur Verfügung zu stellen, darstellen. Gleichwohl ist der zunächst milde und kooperative Ansatz vor dem Hintergrund der mitgliedstaatlichen Souveränitätsrechte und dem Grundsatz der loyalen Zusammenarbeit (Art. 4 Abs. 3 EUV) begrüßenswert. Es sollte allerdings seine Ergänzung im Sinne eines abgestuften Verfahren erwogen werden. So könnte bspw. eine Pflicht des betreffenden Mitgliedstaates eingeführt werden, zu der Empfehlung Stellung zu nehmen und unter Einbeziehung der nationalen Aufsichtsbehörde zu erklären, wie eine hinreichende Ressourcenausstattung künftig sichergestellt werden kann. Dadurch würde zumindest erreicht, dass sich der jeweilige Mitgliedstaat mit der Problematik der unzureichenden Ressourcenausstattung und möglichen Lösungsansätzen ernsthaft auseinandersetzen muss. Auf zweiter Stufe könnte den nationalen Aufsichtsbehörden ein Recht eingeräumt werden, den Ausschuss anzurufen, falls der betreffende Mitgliedstaat dennoch untätig bleibt oder nicht hinreichend Abhilfe schafft. Ergäbe eine darauf folgende erneute Erörterung im Ausschuss, dass die Verletzung der Pflicht aus Art. 58 Abs. 4 andauert, könnte auf dritter Stufe dem Ausschuss die Befugnis eingeräumt werden an die KOM zu berichten und die Einleitung eines Vertragsverletzungsverfahrens vorzuschlagen. Folgt die Kommission dem Vorschlag, bildete das Vertragsverletzungsverfahren die letzte Stufe, die zur einer Entscheidung des Europäischen Gerichtshofs führen kann (Art. 258 Abs. 2 AEUV) und im Fall, dass der Mitgliedstaat einem gerichtlich festgestellten Vertragsverletzung nicht abhilft, zu einer Zwangsgeld- oder Pauschalbetragverhängung (Art. 260 Abs. 3 AEUV).

3. Grundrechtsschutz ohne Individualrechtsschutz

Auch wenn der individuelle Rechtsschutz im Zusammenhang mit Datenverarbeitungsvorgängen von den genannten Schwächen geprägt ist, bildet er eine Säule für einen effektiven Grundrechtsschutz. Den Schwächen kann rechtlich zumindest begegnet werden, etwa durch Informationspflichten, Beweiserleichterungen und der Ergänzung kollektiven oder administrativen Rechtsschutzes. Der Verzicht auf KI-spezifische Betroffenenrechte insgesamt bedeutet hingegen, dass der Einzelne gar keine, auch keine von gewissen Schwächen geprägte, Möglichkeit hat, sich gegen eine vermutete Verletzung seiner Rechte zur Wehr zu setzen, so lange kein bereichspezifisches Recht, etwa aus dem Datenschutz- oder dem Antidiskriminierungsrecht, greift. Dass die Kommission den effektiven Grundrechtsschutz zwar als Ziel des Verordnungsentwurfs formuliert, sich aber auf die gesetzliche Festlegung von Produktstandards beschränkt, wird daher vielfach kritisiert.[44] Das Fehlen von Betroffenenrechten wirkt sich insgesamt negativ für den Grundrechtsschutz aus. Gerade angesichts der Begrenztheit staatlicher Ressourcen, die für die behördliche Aufsicht und Rechtsdurchsetzung zur Verfügung stehen, wären individuelle Rechte zugunsten Betroffener und die Möglichkeiten deren effektiver Geltendmachung und Durchsetzung als zweite Säule wichtig.[45] Starke Anreize für die Einhaltung der Produktsicherheitsstandards können etwa auch drohende Schadensersatzklagen bei deren Verletzung und potenziell damit verbundene Reputationsschäden sein.[46] Mit Blick auf die Effektivität des behördlichen Vollzugs können individuelle oder kollektive Klagen oder gar eine Beschwerdemöglichkeit für Betroffene bei den Aufsichtsbehörden zudem wichtige Anhaltspunkte für ein strategisches Vorgehen bei der Marktüberwachung liefern.[47]

IV. Fazit

Das Ziel der Kommission, einen effektiven Grundrechtsschutz durch einen spezifischen Rechtsrahmen für Künstliche Intelligenz zu gewährleisten und dessen Einhaltung durch eine Stärkung der Rechtsdurchsetzungsinstrumente abzusichern, ist begrüßenswert. Wie man anhand des verbleibenden Vollzugsdefizits im Datenschutzrecht eindrucksvoll sieht, können allerdings auch erweiterte behördliche Befugnisse, Kommunikations- und Kooperationsmechanismen in der Vollzugspraxis keine hinreichende Wirksamkeit entfalten, wenn es an einer angemessenen Ausstattung der Behörden fehlt. Im Verordnungsentwurf gelingt es nicht durch rechtliche Mittel eine angemessene Ressourcenausstattung hinreichend abzusichern, so dass vergleichbare Vollzugsdefizite im KI-Recht zu befürchten sind. Angesichts dessen und des Verzichts auf KI-spezifische Betroffenenrechte und effektive Durchsetzungsmechanismen, die den behördlichen Vollzug wirksam ergänzen könnten, besteht die Gefahr, dass der angestrebte Grundrechtsschutz gleichwohl nicht effektiv umgesetzt werden kann.

44 Siehe *Ebert/Spiecker gen. Döhmann* NVwZ 2021, 1188, 1193; *Alfieri/Carocia/Inveradi*, AI Act and Individual Rights: A Juridical and Technical Perspective, IAIL 2022, 2.1; *Hornung* DuD 2022, 561, 565; ICCL (s. Fn. 42), S. 1; *Veale/Borgesius* CRi 2021, 97, 111 Rn. 98 ff.; *Smuha* et al. (s. Fn. 29), S. 44.

45 Vgl. auch *Smuha* et al. (s. Fn. 29), S. 44 ff.; den Vorschlag eines »multistakeholder Ansatz[es]« durch Einbeziehung zivilgesellschaftlicher Aktur, *Roth-Isigkeit* ZRP 2022, 187, 190 und die Vorschläge des *ICCL* nach einem Beschwerderecht für Betroffenen und Möglichkeiten des kollektiven Rechtsschutzes (s. Fn. 42), S. 4 f.

46 Zur Bedeutung von Reputationsschäden in Bezug auf datenschutzrechtliche Bußgeldverfahren Roßnagel/Friedewald/*Karaboga/Martin/Friedewald* (s. Fn. 22), S. 49, 78.

47 Vgl. auch Roßnagel/Friedewald/*Karaboga/Martin/Friedewald* (s. Fn. 22), S. 49, 78; *Smuha* et al. (s. Fn. 29), S. 45 f.