„Legal Design“ für HessenData (§ 25a HSOG) – ein abgestuftes Kontrollkonzept

Nitharshini Santhakumar

A. „Rechtfragen virtueller Welten

I. Kontrollmechanismen für das „Internet von morgen“

Der JuWissDay 2024 lud unter dem Titel „Rechtsfragen virtueller Welten“ zu einem Austausch über „das „Internet von morgen“ ein. So soll dieses „unser Verhältnis zum digitalen Raum revolutionieren, indem es physische, erweiterte und virtuelle Realität miteinander verschmelzen lässt.“[1]

Eine potenziell irreversible Verschmelzung der realen und virtuellen Welten erfordert eine strategische Auseinandersetzung mit der Frage, ob traditionelle rechtliche Kontrollmechanismen, wie etwa der Richtervorbehalt, in solchen erweiterten Realitäten Anwendung finden können. Sowohl die Judikative als auch die Legislative auf Landes-, Bundes- und Unionsebene haben sich diesen Herausforderungen gestellt. Unter Berücksichtigung der unterschiedlichen Terminologien lassen sich Überschneidungen und Berührungspunkte finden. Dieser Beitrag zielt darauf ab, die Relevanz und die mögliche Ausgestaltung von Kontrollmechanismen zu untersuchen, indem die Ansätze der Rechtsprechung aus einer deutsch-europäischen Perspektive analysiert werden.

II. Schaffung von Strategien aus deutsch-europäischer Perspektive

1. Pionierszenario: „Automatisierte Datenanalyse“

Den Ausgangspunkt der Forschung bildet das Urteil des Bundesverfassungsgerichts zur „automatisierten Datenanalyse“ aus dem Jahr 2023.[2] In diesem Urteil führte das Verfassungsgericht, soweit ersichtlich, erstmalig

1 Beschreibung der Tagung durch den Veranstalter auf dessen Webseite: https://www.juwiss.de/juwissday-2024/ (zuletzt abgerufen am 04.09.2024).

2 BVerfG NJW 2023, 1196 ff.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

den Begriff des „abgestuften Kontrollkonzepts“ ein und eröffnete damit dem Gesetzgeber die Möglichkeit, sich der Thematik durch ein spezifisches „Legal Design“ anzunähern. Aus der Wechselwirkung zwischen Gesetzgebung und Rechtsprechung sowie der anhängigen Verfassungsbeschwerde folgt eine rechtliche Strategie, die im Kontext der „automatisierten Datenanalyse“ in der Bundesrepublik Deutschland als wegweisendes Szenario betrachtet werden könnte.

2. Unionale Strategien

Die deutsche Rechtsprechungsperspektive soll in diesem Beitrag um eine unionale Sichtweise ergänzt werden. Dabei ist zu betonen, dass der zeitliche Aspekt (Time Management) eine wesentliche Rolle spielen dürfte. Bereits im Jahr 2022 hat der EuGH sich in der Entscheidung zur „Passenger Name Records-Richtlinie“[3] zum Einsatz von KI geäußert. Ergänzt wird dies um die Rechtsprechung zur „automatisierten Entscheidung im Einzelfall“ – dem Schufa Scoring Urteil aus 2023. Zwar ist die Tiefgründigkeit zu Kontrollmechanismen im Hinblick auf die Automatisierung nicht mit dem „HessenData“-Urteil des Bundesverfassungsgerichts vergleichbar, gleichwohl sind Tendenzen erkennbar, die auch im Einklang zur europäischen Legislative eine rechtspolitische Strategie erkennen lassen. Aufgrund des Umfangs wird in diesem Beitrag auf nähere Ausführungen zur Legislative – insbesondere JI-Richtlinie[4], DSGVO[5] und KI-VO[6] verzichtet.

3 EuGH ZD 2022, 553 ff.

4 Richtlinie 2016/680/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr […]; hier insbesondere Art. 11 „Automatisierte Entscheidungsfindung im Einzelfall“.

5 Verordnung 2016/679/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr […]; hier insbesondere Art. 22 „Automatisierte Entscheidungen im Einzelfall einschließlich Profiling“.

6 Verordnung 2024/1689/EU zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen […]; hier insbesondere Art. 8–15; Art. 64–69.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

B. „HessenData" – als Demonstrator

I. „Automatisierte Anwendung zur Datenanalyse"

Als Vorreiter in der Bundesrepublik Deutschland entschied sich das Bundesland Hessen für die Implementierung einer technischen Innovation in seine Polizeiarbeit: Die „automatisierte Anwendung zur Datenanalyse". Bei der technischen Innovation „HessenData" handelt es sich um eine Software, die dazu dient, „bisher unverbundene, automatisierte Dateien und Datenquellen in Anwendungen zur Datenanalyse bzw. Analyseplattformen zu vernetzen, die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen und die polizeiliche Aufgabenerfüllung auf diese Weise zu erleichtern und zu verbessern."[7] Die Software wurde von dem US-amerikanischen Unternehmen „Palantir" entwickelt, welches seine Standardsoftware „Gotham" auf die spezifischen Anforderungen des Landes Hessen anpasste, wodurch sie den Namen „HessenData" erhielt.[8] Parallel zur Einführung dieser Software wurde die gesetzliche Ermächtigungsgrundlage in § 25a des Hessischen Sicherheits- und Ordnungsgesetzes (HSOG) geschaffen.[9] Diese Ermächtigungsgrundlage zum Einsatz der „automatisierten Anwendung zur Datenanalyse" war Gegenstand eines Verfahrens vor dem Bundesverfassungsgericht (1 BvR 1547/19 u.a.), das im sogenannten „HessenData-Urteil" mündete.

II. Time Management

„HessenData" zum Kern dieses Beitrags zu machen, erfolgt vor dem Hintergrund, dass diese Entscheidung als wegweisend erachtet wird. Deutlich wird, dass vor allem der Zeitaspekt eine besondere Rolle zukommt:

---

7 Hessischer Landtag: Änderungsantrag […] für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen, Drs. 19/5412, S. 41.

8 Mit Begründung der besonderen Dringlichkeit wurde zunächst in einem freihändigen Vergabeverfahren „Gotham" von Palantir beschaffen. Im Anschluss folgte ein zweites Verfahren, welches in eine Zuschlagserteilung am 14.12.2017 mündete – hierzu ausführlich Hess. Landtag, Zwischenbericht des Untersuchungsausschusses 19/3 zur Drucksache 19/6574 Teil A, Drs. 19/6864, S.19 f.

9 Ursprünglich: Hessischer Landtag: Änderungsantrag […] für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen […] vom 14.12.2017, Drs. 19/5782; GVBl Hessen 2018, S. 302.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

> „Unter Time Management wird hier eine Perspektive verstanden, die „Wissen" in Relation zu Zeit/Datum setzt und so veränderungsoffen wie nachhaltig die Herausforderungen effizient analysieren will. Konsequent fokussiert wie adressiert dieser Beitrag Kernherausforderungen, die im geltenden Recht (de lege lata) bewältigt werden müssen und die – unabhängig vom Ergebnis aktueller Normgebungsverfahren wie Initiativen wie Pläne (de lege ferenda) – Ideen/ Herausforderungen für zukünftig geltendes Recht (lex futura) liefern."[10]

Die Bewältigung der Kernherausforderung „automatisierte Datenanalyse" wird in einem Wechselspiel zwischen Rechtsprechung und Gesetzgeber am Demonstrator[11] „HessenData" konturiert. Die jeweiligen Gesetzesinitiativen und Entscheidungen sind dabei stets aus einer zeitlichen Perspektive zu betrachten:

- 2017: Erwerb der Software & Gesetzeserlass (§ 25a HSOG a.F.)
- 2019: Verfassungsbeschwerde (VB I)
- 2023: Urteil des BVerfG (1 BvR 1547/19 u.a.)
- 2023: Erlass der neuen Ermächtigungsgrundlage (§ 25a HSOG n.F.)
- 2024: Anhängige Verfassungsbeschwerde (VB II).

III. Pioniersvorhaben „HessenData": Ein Gesetz für ein Produkt

1. Normierung der „automatisierten Datenanalyse"

§ 25a HSOG in der alten Fassung bildet den Grundstein für die „automatisierte Datenanalyse". Bereits in der alten Fassung hatte der Gesetzgeber

10 *V. Schmid/T. Kretschmann*, Operative Herausforderungen einer „Drohnenwelt" – (Luftverkehrs)Management (ATM und UTM) inklusive der „Drohnendetektion", in: K. Chibanguza/C. Kuß/H. Steege (Hrsg.), Künstliche Intelligenz – Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden 2022, S. 529, Rn. 128.

11 „Grundsätzlich zu unterscheiden sind „Pilot" und „Demonstrator" (Terminologie V. Schmid). Piloten" sind szenarienorientierte, projektierte Anwendungen von (Recht und) Technik. „Demonstratoren" erlauben die Überprüfung der Machbarkeit, Nachhaltigkeit, Qualität wie Anfälligkeit des "Piloten" – sie unterscheiden sich also in der Funktions-, Rechts- und Marktreife. Dies ist in einer ökonomischen Perspektive auch der Unterschied zwischen Business Opportunity und Business Case bzw. die Entdeckung der sog. „Killerapplikation"." Zitat aus *V. Schmid/ J. Toptaner*, Integration von „Flugdrohnen" in das (deutsch-europäische) Rechtssystem – eine Kartographie (Fn. 10), Rn. 11.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

die Erforderlichkeit von Kontrollmechanismen erkannt und in § 25a Abs. 3 HSOG wiedergegeben.

§ 25a Abs. 3 (HSOG)
(3) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. Die oder der Hessische Datenschutzbeauftragte ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

Weitere „Kontrollmechanismen" waren der Norm hingegen nicht zu entnehmen.

2. Praktische Handhabe von Kontrollmechanismen für die „automatisierte Datenanalyse"

Das Fehlen einer spezifischen Normierung zusätzlicher Kontrollmechanismen impliziert nicht, dass die Hessische Polizei bei der Einführung von „HessenData" notwendige Vorkehrungen vernachlässigt hat. Vielmehr wurden bei der Implementierung von „HessenData" wesentliche Kontrollmechanismen integriert, die im Gesetzestext nicht ausdrücklich festgelegt worden sind. Eine umfassende Untersuchung dieser Maßnahmen wurde im Rahmen des Untersuchungsausschusses[12] durchgeführt. Dabei sind zwei tragende Säulen erkennbar geworden: Zum einen werden Schutzvorkehrungen durch die „Hessische Zentrale für Datenverarbeitung (HZD)"[13] getroffen, zum anderen hat die Hessische Polizei selbst Sicherheitsvorkehrungen getroffen, die sowohl den unbefugten Zugriff als auch die unbefugte Übertragung von Daten verhindern sollen.[14]

12 Hessischer Landtag, Zwischenbericht des Untersuchungsausschusses 19/3 zur Drucksache 19/6574, Drs. 19/6864 vom 03.01.2019 (https://starweb.hessen.de/cache/DRS/19/4/06864.pdf).

13 Ausführlich zu den Sicherheitsvorkehrungen etwa *HZD-Report 2023,* Zukunft ist jetzt, „Sicherheit neu denken", S. 27 (https://tinyurl.com/47rey2ju).

14 *Hessisches Ministerium des Inneren und Sport,* Hessische Cybersicherheitsstrategie 2023, S. 30.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

a) Schutz vor Abfluss sensibler Daten

Der Schutz vor dem Abfluss sensibler Daten wird in mehrfacher Hinsicht erreicht. Aus dem Untersuchungsbericht geht hervor, dass neben der Zurverfügungstellung von Endgeräten für die Palantir-Mitarbeiter zum Zwecke der Einrichtung von HessenData auch Firewalls und die Methodik des „Housings"[15] eine zentrale Rolle spielen.[16] Aus dem Bericht des Untersuchungsausschusses geht auch hervor, dass die Plattform in die gleiche Firewall-Umgebung gesetzt wurde wie andere polizeiliche Anwendungen. So kann der gleiche Sicherheitsstandard erfüllt werden.[17]

b) Schutz vor unbefugtem Zugriff

Das HZD hat auch besondere Vorkehrungen getroffen, um vor unbefugtem Zugriff zu schützen. Diese umfassen insbesondere Zugriffsbeschränkungen etwa durch vorherige Anmeldungen, Sicherheitstoken, Firewall oder Bestimmung von Arbeitsplätzen.[18] Schutzvorkehrungen dieser Art werden am hessenweiten Mindeststandard für IT-Sicherheit gemessen.

3. Technisch-organisatorische Maßnahmen der Exekutive

Festzuhalten bleibt insofern, dass der Landesgesetzgeber zwar in der Ermächtigungsgrundlage von ausdifferenzierten Kontrollmechanismen abgesehen hat, dagegen aber die Exekutive eine Vielzahl von technischen und organisatorischen Maßnahmen (TOMs) ergriffen hat. Charakteristisch ist, dass mittels ihnen kurzfristig auf den „Stand der Technik" reagiert und

15 Das sogenannte Housing bedeutet, dass ein Interessent die Infrastruktur in Anspruch nehmen kann, ohne unmittelbaren Zugriff auf die Systemarchitektur zu haben. Konkret bedeutet dies, dass sichere Zugangskontrollen, redundante Netze und Stromleitungen sowie Klimatechnik zur Verfügung gestellt werden; vertiefend *A. Auer-Reinsdorff*, § 21 Providerverträge, A. Auer-Reinsdorff/I. Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 41.

16 Hessischer Landtag, Zwischenbericht des Untersuchungsausschusses (Fn. 12), S.69.

17 Hessischer Landtag, Zwischenbericht des Untersuchungsausschusses (Fn. 12), S.70.

18 Hessischer Landtag Zwischenbericht des Untersuchungsausschusses (Fn. 12), S. 72.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

dadurch die Sicherheitsarchitektur angepasst werden kann.[19] Der konkreten Gestaltung der TOMs dürfte eine hohe Wichtigkeit zukommen, denn fehlende materielle Substanz kann zur Beeinträchtigung des Informationsanspruchs des Bürgers führen.[20] Gleichzeitig streben auch Sicherheitsbehörden zum Zwecke der „effektiven und resilienten Gefahrenabwehr" einen hohen Grad an Datensicherheit an.[21]

IV. Neukonzeptionierung der „automatisierten Datenanalyse"

Im Februar 2023 entschied das Bundesverfassungsgericht dahingehend, dass die „automatisierte Datenanalyse" grundsätzlich ein zulässiges Mittel sein könnte.

1. Maßstab der Verhältnismäßigkeit

In seiner Entscheidung betonte das BVerfG unter Verweis auf seine „BKAG I-Entscheidung, dass der Grundsatz der Verhältnismäßigkeit Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle stellt.[22] Zudem nennt das Gericht einige Maßnahmen, die dem Verhältnismäßigkeitsgrundsatz Rechnung tragen sollen – etwa das „abgestufte Kontrollkonzept", staatliches Monitoring und die Protokollierungspflicht.[23] Das BVerfG hat in der Vergangenheit bereits entschieden, dass bei verminderter Gewährleistung subjektiven Rechtsschutzes die Anforderungen an „an eine wirksame aufsichtliche Kontrolle und an die Transparenz des Behördenhandelns steigen."[24] Es gilt daher Maßnahmen zu finden, die sich praktisch umsetzen lassen und gleichzeitig die Trias „Transparenz, individueller Rechtsschutz und aufsichtliche Kontrolle" stärken.

---

19 Ausführlich zur Begrifflichkeit „Stand der Technik" – *C. Piltz* in P. Gola/D. Heckmann (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage, Art. 32 Rn. 15–19 sowie *S. Schulz* Art. 6 Rn. 141.

20 *C. Arzt*, PolG NRW § 22 Datenspeicherung, Prüfungstermine, in: M. Möstl/D. Kugelmann (Hrsg.), BeckOK Polizei- und Ordnungsrecht Nordrhein-Westfalen, 28. Edition, München 2024, § 22 Rn. 5.

21 *D. Kugelmann/A. Buchmann*: Der Algorithmus und die Künstliche Intelligenz als Ermittler – Zum Rechtsrahmen für sicherheitsbehördliche Datenanalysen und für den Einsatz von Verfahren künstlicher Intelligenz, GSZ 2024, 1 (4).

22 Urteil des BVerfG ADA (Fn. 2), Rn. 109.

23 Vgl. zu den durch das BVerfG genannten möglichen Maßnahmen Urteil des BVerfG ADA (Fn. 2), Rn. 109.

24 BVerfGE 141, 220 (378) Rn. 135.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

a) Transparenz

Durch das Inkrafttreten der KI-VO hat der Diskurs zur Bedeutung von Transparenz neuen Wind bekommen. In der Entscheidung zum BKAG I stellte das BVerfG fest, dass die „Transparenz der Datenerhebung und -verarbeitung zum Vertrauen beitragen soll."[25] Häufig findet sich in diesem Zusammenhang die Terminologie „Blackbox" wieder und meint dabei, dass nur die Eingabe- und Ausgabedaten bekannt sind, nicht jedoch wie das System zu dem Ergebnis kam.[26] Diesem Prozess schließt sich aus rechtswissenschaftlicher Perspektive die Frage an, wie eine Überprüfung erfolgen könnte, wenn die Entscheidung automatisiert erfolgt.[27] Zu einer der europäischen Strategie annähernden Überlegung kam *Henning Radtke* beim EDV-Gerichtstag 2024:

> *„Ein verfassungsrechtliches Problem ist die Frage nach Transparenz oder der Intransparenz. […]* ***Fehler aufdecken und überprüfen kann jedoch nur wer die Datengrundlage wie die Gewichtung des Entscheidungsprozesses und der Entscheidungskriterien kennt und versteht. Intransparenz der Entscheidungsabläufe bei der Nutzung der KI und damit eine fehlende Nachvollziehbarkeit der Funktionsweise von KI-Technologien können daher mit dem rechtstaatlichen Transparenzgebot in Konflikt stehen.*** *Deshalb wird aus meiner Sicht – ein zentraler Eckpfeiler der Regulierung von KI eben auch die Transparenz in Form von Kennzeichnungs- und Informationspflichten sein. Insofern glaube ich, dass der AI Act der Europäischen Union da auf einem richtigen Weg ist.""*[28]

Demnach wären zur Erfüllung der Transparenzanforderungen bei der Nutzung von KI drei Voraussetzungen zu erfüllen: Kenntnis hinsichtlich Datengrundlage, Gewichtung des Entscheidungsprozesses und die Entscheidungskriterien. Die Offenlegung dieser drei Voraussetzungen geht häufig einher mit der Kritik, dass dadurch das „Geschäftsgeheimnis offenbart

25 BVerfGE 141, 220 (378) Rn. 135.

26 *L. Merkle:* Transparenz nach KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, 414 (415).

27 *J. Eisele,* Verarbeitung der PNR-Fluggastdaten, ZD 2022, 553 (559).

28 Richter am BVerfG Prof. Dr. Radtke am EDVGT am 12.09.2024 in Saarbrücken, Siehe hierzu „Eröffnung 33. EDV-Gerichtstag" vom 12.09.2024: Zitat bei 1:34:30 – 1:35:35. https://www.youtube.com/watch?v=WK0i2ckBDD8.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

wird".[29] Dabei muss die Offenlegung nicht bedeuten, dass der Algorithmus als Open-Source-Projekt frei und für jeden zugänglich zur Verfügung steht, denn damit wäre im Regelfall auch nicht die Transparenzpflicht erfüllt. Gegenwärtig dürfte die Mehrheit der Betroffenen nicht über die entsprechende Fachkompetenz besitzen, um mittels des Quellcodes die Entscheidungsfindung nachzuvollziehen. Dagegen dürfte zur Annäherung der Transparenz die bildliche Darstellung etwa in Form von Entscheidungsbäumen oder Gewichtsdarstellungen hilfreich sein.[30]

Ein Nachteil muss sich hierdurch für die großen privaten Akteure auch nicht ergeben. Vielmehr könnten sie durch die (visuelle/nachvollziehbare) Offenlegung der Funktions- und Wirkungsweise der Algorithmen einer Machtasymmetrie entgegenwirken und so ggf. der ihnen drohenden Erweiterung der mittelbaren Drittwirkung zu einer nahezu „unmittelbaren Drittwirkung" entgegenwirken.[31]

b) Aufsichtliche Kontrolle

In seiner Entscheidung zum Anti-Terrorgesetz sah das BVerfG die aufsichtliche Kontrolle als objektivrechtliche Maßnahme im Verhältnis zur subjektivrechtlichen Kontrolle durch Gerichte an. Sie ziele auf die Gewährleistung der Gesetzmäßigkeit der Verwaltung ab und umfasse auch den subjektiven Schutz der Betroffenen, die nur mittelbar oder im Zusammenwirken mit anderen Maßnahmen von ihrer Betroffenheit Kenntnis erlangen."[32]

Im Rahmen der Verhältnismäßigkeitsprüfung solle die aufsichtliche Kontrolle anhand ihrer Wirksamkeit geprüft werden: Konkret ist zu überprüfen, mit welchen Befugnissen die aufsichtliche Kontrolle ausgestattet ist,

29 Insofern hatte der BGH im Kontext eines datenschutzrechtlichen Auskunftsersuchens geurteilt, dass der Algorithmus Bestandteil des Geschäftsgeheimnisses der Schufa-Scoring ist, vgl. *BGH* Urteil vom 28.01.2014 VI- ZR 156/13, MMR 2014, 489 LS 3, Rn. 27.

30 *V. Bortnikow/ J. Dukart,* Informationelle Selbstbestimmung und KI, ZD 2024, 558 f. (560).

31 *W. Hoffmann-Riem*, Die digitale Transformation als rechtliche Herausforderung, JuS 2023, 617 (619).

32 BVerfGE 133, 277 (370).

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

ob also die auszuwertenden Daten vollständig sind und für den Prüfenden in einer praktikablen Form zur Verfügung stehen.[33]

c) Individueller Rechtsschutz

Die Ausgestaltung des individuellen Rechtsschutzes stellt mitunter einer der größten Herausforderungen dar. Für die Geltendmachung von Ansprüchen wäre die Nachvollziehbarkeit der Entscheidungsfindung maßgeblich. Da diese jedoch durch Intransparenz geprägt ist, wird die effektive Durchsetzung rechtlicher Ansprüche gefährdet.[34]

Für zivilrechtliche Themengebiete wird in der Literatur als Lösungsansatz zur Bewältigung der Informationsasymmetrie bei der Anwendung automatisierter Entscheidungsfindungssysteme (ADM-Systeme) die Beweislastumkehr erörtert, um die Hürden für die Geltendmachung von Diskriminierungsansprüchen zu senken.[35] Offen bleibt vorerst, wie es für das Verwaltungsprozessrecht eingeführt werden könnte.

2. Konkrete Ausgestaltung & Umsetzung durch Rechtsprechung und Gesetzgeber

Das Bundesverfassungsgericht erklärte die Ermächtigungsgrundlage zur „automatisierten Anwendung zur Datenanalyse" nicht für nichtig, sondern lediglich für unvereinbar und setzte hierzu eine Frist bis zum 30.09.2023.[36] In seiner Entscheidung ging das Gericht auf die „Transparenz, den individuellen Rechtsschutz und [die] aufsichtliche […] Kontrolle" ein und nannte hierzu auch mögliche Kriterien. Noch im Juli 2023 erließ der hessische Gesetzgeber eine neue Ermächtigungsgrundlage, die teilweise in der Be-

33 *K. Graulich,* Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr in H. Lisken/E. Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, Rn. 716.

34 *I. Spiecker gen. Döhmann/E. V. Towfigh*, Automatisch benachteiligt – Das Allgemeine Gleichbehandlungsgesetz und der Schutz vor Diskriminierung durch algorithmische Entscheidungssysteme, Rechtsgutachten im Auftrag der Antidiskriminierungsstelle des Bundes, 2023, S. 70.

35 *M. Grünberger*, Reformbedarf im AGG: Beweislastverteilung beim Einsatz von KI, ZRP 2021, 232 (234); deutlicher so der auf die Wirtschaft bezogene Gleichstellungsbericht BReg (2020), Drs. 19/30750, S. 138 und S. 169, für den Arbeitsbereich.

36 Urteil des BVerfG ADA (Fn. 2).

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

gründung auf das Urteil rekurrierte.[37] Zu den konkret durch das Gericht genannten und durch den hessischen Gesetzgeber neu geregelten Maßnahmen gehören:

- Rollen- & Rechtekonzept, § 25a Abs. 3 Nr. 1 HSOG
- Technisch-organisatorische Vorkehrungen, § 25a Abs. 3 Nr. 2 lit. b HSOG
- Zugriffskontrolle, § 25a Abs. 4 S. 1–2 HSOG
- Protokollierungspflicht, § 25a Abs. 4 S. 2–3 HSOG
- Abgestuftes Kontrollkonzept, § 25a Abs. 4 S. 6 u. Abs. 5 HSOG
- Anhörungsrecht des hessischen Datenschutzbeauftragten, § 25a Abs. 5 HSOG.

Zwar hatte die hessische Polizei einige Maßnahmen bereits implementiert, doch verlangte das Gericht die gesetzliche Kodifizierung: Im Ergebnis seien abstrakt-generelle Regelungen erforderlich, die in einer öffentlich zugänglichen Weise dokumentiert werden. Die konkrete Gestaltung des Konzepts wiederum kann durch eine Verwaltungsvorschrift erfolgen.[38] Dem kam der hessische Gesetzgeber auch im neuen § 25a Abs. 3 Nr. 1 HSOG n.F. nach: Die Gestaltung des Rollen- und Rechtekonzepts ist nicht an den polizeilichen Berufsgrad/Hierarchiengrad gebunden, sondern orientiert sich am Schutzwert des betroffenen Rechtsguts sowie an der Dringlichkeit des polizeilichen Handelns, wobei die Anwendergruppe sich nach Phänomenbereichen unterteilt.[39] Solche Rollen- und Rechtekonzepte sollen Tätigkeiten mit Authentifizierung verknüpfen und vor Manipulationen schützen.[40] Darüber hinaus gewährleisten sie, dass der jeweils zuständige Organisationsbereich über die erforderliche Schulung, Belehrung und Freistellung verfügt, um die datenschutzrechtlichen Vorgaben sachgerecht umsetzen zu können.[41] Die Sicherstellung der praktischen Wirksamkeit soll durch sogenannte „technisch-organisatorische Vorkehrungen" erfolgen. Aus deutsch-europäischer Perspektive wäre hier terminologisch die Verwendung „technisch-organisatorische Maßnahmen" wünschenswert gewesen.[42] Die Aufforderung durch „TOM" zu regeln, welche Daten in die Analyse einbezogen

37 GVBl. Hessen 2023 Nr. 22, S. 456 ff.
38 Urteil des BVerfG ADA (Fn. 2), Rn. 140.
39 Verwaltungsvorschrift zu § 25a HSOG StAnz. 2023 S. 946, 2.1 Anwendergruppen.
40 *K.Schürmann*, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, 316 (320).
41 Verwaltungsvorschrift zu § 25a HSOG (Fn. 39), 2.3 Schulung.
42 Vgl. hierzu Art. 19 JI-RL, Art. 32 DSGVO, Urteil des BVerfG ADA (Fn. 2), Rn. 163, nunmehr auch Art. 15 KI-VO.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

werden, zählt der Gesetzgeber lediglich nummerisch in der Verwaltungsvorschrift auf, die auf § 25a HSOG n.F. basiert.[43]

Der § 25a Abs. 4 HSOG n.F. regelt die Zugriffskontrolle und die Protokollierungspflicht. Während die Zugriffskontrolle quantitativ eingrenzen soll, dient die Protokollierungspflicht der qualitativen Eingrenzung. Sie dient – so der unmittelbare Gesetzeswortlaut – „der Selbstvergewisserung und der nachträglichen Kontrolle". Diese verfassten Protokolle, wieso also eine automatisierte Datenanalyse durchgeführt wurde, sollen der stichprobenartigen Kontrolle zugrunde gelegt werden.[44] Grundsätzlich ist dies zu begrüßen, denn die schriftliche Fixierung der Tatsachen, die den Einsatz sowohl rechtfertigen als auch den Zweck benennen, dient der Vergewisserung über die Rechtmäßigkeit der Maßnahme. Zudem wird hierdurch eine spätere Kontrolle ermöglicht. Für ihre tatsächliche Wirksamkeit sind jedoch konkrete Anforderungen der Genauigkeit erforderlich – etwa in Gestalt der Subsumtion unter dem Rechtssatz.[45]

Das „abgestufte Kontrollkonzept" sieht aufgrund der hohen Zahl der Maßnahmen die Verteilung der Kontrollbefugnis zwischen verschiedenen Kontrollinstanzen vor – hier zwischen dem behördlichen und dem hessischen Datenschutzbeauftragten sowie dem Behördenleiter."[46] In der konkreten Neugestaltung des § 25a HSOG sieht dies wie folgt aus: Bei der Einrichtung oder einer wesentlichen Änderung liegt die Anordnungsbefugnis beim Behördenleiter und der hessische Datenschutzbeauftragte ist anzuhören. Für jeden Fall der automatisierten Datenanalyse hat der behördliche Datenschutzbeauftragte das Recht der stichprobenartigen Kontrolle – hierfür sind die Protokolle Grundlage. Vor dem Hintergrund, dass der Richtervorbehalt aufgrund „der Komplexität der Datenverarbeitung einer zügigen Beurteilung entgegensteht"[47], dürfte das abstrakte Kontrollkonzept ein besserer Ansatz sein.

Nicht durch den hessischen Gesetzgeber umgesetzt ist das „staatliche Monitoring" bei der Entwicklung der eingesetzten Software. Wobei das Gericht die Anforderungen hieran nicht als Verfahrensgegenstand sah.[48]

43 Verwaltungsvorschrift zu § 25a HSOG (Fn. 39), 2.2.1 – 2.2.7.
44 *Hess. LT,* Änderungsantrag vom 20.06.2023, Drs. 20/11235, S. 17.
45 *Graulich,* Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr (Fn. 33), Rn. 699–700.
46 Urteil des BVerfG ADA (Fn. 2), Rn. 109.
47 *Kugelmann/ Buchmann*, Der Algorithmus und die Künstliche Intelligenz als Ermittler (Fn. 21), 1 (7).
48 Urteil des BVerfG ADA (Fn. 2), Rn. 109.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

Auch wenn sich im Bericht des Untersuchungsausschusses mehrfach die „Beteuerung" wiederfindet, dass ein privater Akteur keinen Zugriff auf die Daten habe, so bietet es sich für einen rechtssicheren Umgang an, ein eigenes technisches Analysesystem zu entwickeln.[49]

V. Kritik an der Neukonzeptionierung

Auch die Neukonzeption der Ermächtigungsgrundlage stößt auf Kritik. Dabei wird auf formaler Ebene der Gesetzgebungsprozess kritisiert und in materieller Hinsicht die Umsetzung moniert. Am 23.06.2023 kritisierte die Humanistische Union in einem offenen Brief an die Abgeordneten des Hessischen Landtags, dass der Änderungsantrag (Drs. 20/11235) für die Öffentlichkeit noch nicht einsehbar sei, die Abgeordneten erst seit dem 20.06.2023 Einsicht haben und dass es das Schnellverfahren unter Ausschluss der Anhörung/Stellungnahme zivilrechtlicher Organisationen nahezu unmöglich mache, außerparlamentarisch die Thematik zu erörtern.[50] Obwohl die Komplexität der Thematik es angeboten hätte, verzichtete die Regierungskoalition auf die Anhörung von Sachverständigen,[51] bzw. dem hessischen Datenschutzbeauftragten[52], was auf erhebliche Kritik stieß.[53]

Im Juni 2024 erhob die Gesellschaft für Freiheitsrechte e.V. Verfassungsbeschwerde gegen die neue Ermächtigungsgrundlage und beanstandete, dass keine der Varianten der § 25a Abs. 2 S. 1 Nr. 1–3 HSOG n.F. die Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Überwachung erfülle. Es mangele an einem adäquaten Kontrollmechanismus innerhalb des § 25a HSOG. Zwar sei gemäß § 25a Abs. 4 S. 6 HSOG

49 *A. Meister,* Wir veröffentlichen den Entwurf zum neuem BKA-Gesetz, 15.08.2024 (https://tinyurl.com/37sym42u) (zuletzt abgerufen am 17.10.2024).

50 *P. Dingeldey & Bundesvorstand der Humanistischen Union,* Offener Brief an die Abgeordneten des Hessischen Landtags vom 23.06.2023 (https://tinyurl.com/p3t7da9c) (zuletzt abgerufen am 17.10.2024).

51 Hierzu äußerte sich die Abgeordnete Eva Goldbach wie folgt: „Wir hätten keine Zeit mehr gehabt, in dieser Legislaturperiode eine dritte Anhörung […]. durchzuführen und die Auswertung vorzunehmen. Das hätten wir nicht mehr geschafft. […] Wir setzen das jetzt um – aus verschiedenen Gründen, weil wir es abschließen wollten […]", Hess. Lt. Plenarprotokoll 20/136 vom 27.06.2023, 11238.

52 *Hess. Datenschutzbeauftragter, A. Roßnagel,* Hess. LT, Drs. 21/27 vom 31.12.2023, S. 49.

53 Siehe *Hanning Voigts,* Hessen: Kritik an Reform zur „Hessendata" – Software, Frankfurter Rundschau vom 23.06.2023 (https://tinyurl.com/59czae35, zuletzt abgerufen am 10.10.2024).

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

der behördliche Datenschutzbeauftragte berechtigt, stichprobenartige Kontrollen durchzuführen, jedoch handele es sich lediglich um eine Erlaubnis und nicht um eine Verpflichtung, wodurch eine regelmäßige Kontrolle nicht garantiert sei.[54]

Da jedoch die aufsichtliche Kontrolle den schwachen Individualrechtsschutz kompensieren soll, ist eine restriktivere Kontrollhandhabe erforderlich, um auch von ihrer Wirksamkeit auszugehen.[55] Sehr umstritten ist der Einsatz einer solch komplexen Methode unter Einbeziehung eines ausländischen privaten Akteures. Während das gerichtlich geforderte „staatliche Monitoring" nicht umgesetzt wurde, aber durch die Literatur verlangt wird,[56] wird innerhalb der Politik der Einsatz auch auf Bundesebene gefordert.[57]

C. Anwendungsorientierte Kontrollmechanismen – eine europäische Strategie

Auch der EuGH hat in seinen Entscheidungen in Ansätzen den Einsatz automatisierter Vorgänge an besondere Voraussetzungen geknüpft, wenn auch nicht mit entsprechender Schwerpunktsetzung.

I. Verzicht auf KI? – Drei Kriterien des EuGHs zur PNR-Entscheidung

Im Jahre 2022 entschied der EuGH über die Verarbeitung von Fluggastdaten und die Rechtmäßigkeit der PNR-Richtlinie.[58] Die Entscheidung des Gerichts unterstützt den Einsatz der automatisierten Verarbeitung, nennt für ihren rechtmäßigen Einsatz auch Kriterien, gleichwohl schiebt sie einen

54 *T. Singelnstein,* Verfassungsbeschwerde vom 21.06.2024, S. 95 veröffentlicht über freiheitsrechte.org (https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf, zuletzt besucht am 10.10.2024).

55 *M. Bäuerle,* in: M. Möstl/M. Bäuerle (Hrsg.): BeckOK Polizei- und Ordnungsrecht Hessen, 33. Edition, §25a Rn. 115.

56 *M. Bäuerle,* § 25a HSOG (Fn. 55), Rn. 65a.

57 Antrag der CDU/CSU Fraktion BT-Drucks. 20/9495 vom 27.11.2023: „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren".

58 EuGH, Urteil PNR (Fn. 3).

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

Riegel beim Einsatz selbstlernender Systeme vor, da diese „ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können."[59] Diese sehr klare Feststellung unterliegt der Kritik, dass sich der Gerichtshof „auf ein juristisch, technologisch und politisch hochbrisantes Themengebiet begab", gleichwohl „den Unterschied zwischen Mustererstellung und Musterabgleich nicht klarer ausarbeitete."[60] Wird auf selbstlernende Systeme verzichtet, bedeutet dies auch, dass auf das Gesamtpotenzial der Technologie verzichtet wird, mit der Konsequenz, dass letztlich „wieder" eine menschliche Kraft den Abgleich durchgeführt und die gegenwärtige Vorgehensweise unverändert fortgesetzt wird.[61] Folgt man trotzdem der Auffassung des Gerichts, bleiben – auch im Rückgriff auf die Ausführungen des Generalanwalts drei entscheidende Kriterien beim Einsatz „automatisierter Verarbeitung": Wesentlich sei, so das Gericht,

- „die Erkennbarkeit, dass eine algorithmische Entscheidung erfolgte"[62],
- „die Funktionsweise des Algorithmus muss bekannt sein"[63] und
- „die Nachvollziehbarkeit des Ergebnisses"[64], sodass eine Überprüfung erfolgen kann.

Die Herausforderung in dieser Entscheidung ist, dass zwar die Erforderlichkeit von Kriterien klar benannt wird, die konkrete Ausgestaltung aber durch den Gerichtshof offengelassen wird und letztlich der Exekutive auf-

59 EuGH, PNR (Fn. 3), Rn. 194.

60 *I. Kostov,* Die Fluggastdatenverarbeitung zu Sicherheitszwecken, GSZ, 2023 13 (15).

61 *K. Korte*, I-Anwendungen müssen transparent und diskriminierungsfrei sein. RDI 2022, 538 (540).

62 *G. Pitruzella,* Schlussantrag vom 27.01.2022, C-817/19, ECLI:EU:C:2022:65 Rn. 228: „[…] dass die Funktionsweise der Algorithmen, die im Rahmen der in Art. 6 Abs. 3 Buchst. b vorgesehenen Analyse verwendet werden, transparent und das Ergebnis ihrer Anwendung nachvollziehbar sein muss. […] Es verlangt jedoch, dass die Erkennbarkeit der algorithmischen Entscheidungsfindung gewährleistet ist."

63 *G. Pitruzella.* (Fn. 63): „Die Transparenz der Funktionsweise der verwendeten Algorithmen ist auch eine notwendige Bedingung, um den Betroffenen die Ausübung ihrer Beschwerderechte und ihres Rechts auf effektiven gerichtlichen Rechtsschutz zu ermöglichen."

64 *G. Pitruzella.* (Fn. 63):„Zum anderen muss –[…] bei der automatisierten Verarbeitung von PNR[…] auf andere, nicht automatisierte Art individuell überprüft wird, nachvollzogen werden können, weshalb das Programm zu einem solchen Treffer gelangt ist[…]".

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

erlegt wird.[65] So lässt sich aus der Entscheidung nicht erschließen, wie die „Bekanntheit der Funktionsweise" oder die „Nachvollziehbarkeit" geartet sein muss. Zu beachten ist auch, dass das „Verständnis" zur Funktionsweise nicht zur Erhöhung des Schutzes des Betroffenen führt.[66]

II. Das Recht auf menschliche Entscheidung – EuGH zum Schufa Scoring

Bei der sog. Schufa-Scoring-Entscheidung ging es um voll- bzw. teilautomatisierte Entscheidungen unter Berücksichtigung von Art. 22 DS-GVO. Der Gerichtshof verhandelte die automatisierte Erstellung der Entscheidungsgrundlage, wobei der EuGH drei wesentliche Kriterien hervorhob:

- „Verwendung geeigneter mathematischer oder statistischer Verfahren
- Konzeptionierung und Durchführung von technisch-organisatorischen Maßnahmen
- Rechtsschutzmöglichkeiten für den Betroffenen"[67]

Diese drei Kriterien dürften sich mit der bereits begonnen Rechtsprechungslinie des EuGHs decken und nach Auffassung der Verfasserin auch die Strategie der KI-VO und der europäischen Gesetzgebung widerspiegeln.[68] Diese abstrakten Regeln werden bei ihrer Anwendung jedoch auf Herausforderungen stoßen, etwa bei der Prüfung, ob der Anwendungsbereich eröffnet wird. Sofern der Scorewert und die damit einhergehende Entscheidung ausschließlich auf Grundlage des Systems erfolgt, ist der Anwendungsbereich eröffnet. Schwierig(er) wird es, wenn sich an den automatisiert errechneten Score eine menschliche Entscheidung anschließt. Die Ermittlung der Grenzen dürfte jedoch in naher Zukunft (wenn schon nicht sogar gegenwärtig) eine Vielzahl von Anwendungsfälle betreffen.[69] Zur Umgehung des Anwendungsbereichs müsste daher nach der Rechtspre-

65 *A. Sandhu,* EuGH: Datenschutzrecht: Achtung der Grundrechte erfordert Beschränkung in der PNR-Richtlinie vorgesehenen Befugnisse auf das absolut Notwendige, EuZW 2022, 706 ff. (718).

66 *I. Kostov,* Die Fluggastdatenverarbeitung zu Sicherheitszwecken (Fn. 60), 13 (17).

67 *EuGH,* Urteil vom 07.12.2023, C-634/21ECLI:EU:C:2023:957 Rn. 59.

68 *T. Radtke,* Das Verhältnis von KI-VO und Art. 22 DS-GVO unter besonderer Berücksichtigung der Schutzzwecke, RDi 2024, 353 ff.; vgl. Art. 9–15, 64–70 KI-VO und zur „vertrauenswürdigen KI", – Erw.Gr. 27 KI-VO HILEG (2019) (https://tinyurl.com/56zwd89y).

69 Ausführlich hierzu: *T. Fuchs, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Auswirkungen des Schufa-Urteils auf KI-Anwendungen – auto-

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

chung bei jedem einzelnen Vorgang eine Kontrolle durch einen Menschen erfolgen, der sowohl die Funktionsweise versteht und die Möglichkeit der Übersteuerung hat.[70] Zu prüfen ist jedoch auch, welchen Einfluss ein Ergebnis auf die menschliche Entscheidungskontrolle hat, denn die Abweichung vom Ergebnis verlangt meist eine Begründung, die oft mit erhöhtem Rechtfertigungsaufwand einhergeht.[71]

D. Ausblick

Anhand der Konturierung der deutschen und europäischen Rechtsprechung wird deutlich, dass zwei unterschiedliche Strategien bei der Konzipierung von Kontrollmechanismen für automatisierte Datenvorgänge möglich sind.

Das Legal Design des BVerfG zeigt sich „innovationsoffen" und ermöglicht den frühen Einsatz einer wenig erprobten Software eines privaten Akteures. Es versucht dem Verhältnismäßigkeitsgrundsatz durch hohe Anforderungen an den Anwender Rechnung zu tragen. Dabei soll die „aufsichtliche Kontrolle" durch das „abgestufte Kontrollkonzept" ergänzt werden. Deutlich wird allerdings, dass dies durch ihren stichprobenartigen Charakter letztlich eher zu einem Transparenzkriterium wird. Auch im Hinblick auf die bereits anhängige Verfassungsbeschwerde dürfte abzuwarten sein, ob weitere Ausführungen zum „staatlichen Monitoring" folgen – dies insbesondere deshalb, weil die enge Kooperation zwischen einem privaten (ausländischem) Akteur sowie einer Sicherheitsbehörde weitere Rechtsfragen aufwirft. Der EuGH nähert sich der Herausforderung hingegen von einer funktionalen Perspektive. Seine Kriterien an die „Bekanntheit" und „Nachvollziehbarkeit" sind tendenziell eher anwendungsorientiert und dürften auch mit der KI-VO im Einklang stehen, weshalb hier eine „europäische Strategie" deutlicher wird.

Für eine wirksame aufsichtliche Kontrolle gilt es nun beide Strategien einerseits zu harmonisieren und andererseits auf mögliche „positive bzw.

matisierte Entscheidungen dürfen keine maßgebliche Rolle spielen, Pressemitteilung vom 07.12.2023, https://tinyurl.com/4vcazu4b.

70 *A. Golland,* KI und KI-Verordnung aus datenschutzrechtlicher Sicht, EuZW 2024, 846 (850).

71 *B. Paal/J. Hüger*, Die KI-VO und das Recht auf menschliche Entscheidung, MMR 2024, 540 (541).

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -

negative Kompetenzkonflikte“[72] zu prüfen. Denn in Konkurrenz treten nicht nur mitgliedstaatliche und europäische Regelungen, sondern auch daten(schutz)rechtliche (DSGVO/DSA/DMA/DA/JI-Richtlinie) und KI-rechtliche (KI-VO) Regelungen. Die Bestimmung des Anwendungsbereichs und die Ausgestaltung der wirksamen Kontrollmechanismen dürften daher Kernaspekte der Diskussion über den sicherheitsbehördlichen KI-Einsatz in den kommenden Jahren sein, denen sich sowohl die Legislative als auch die Judikative zu stellen haben wird.

72 *Vogel/Eisele*, in: E. Grabitz/M. Hilf/M. Nettesheim/Vogel/Eisele (Hrsg.), Das Recht der Europäischen Union, 82. EL Mai 2024, Art. 82 AEUV Rn. 73.

https://doi.org/10.5771/9783748949121-103 - am 07.12.2025, 11:07:10. https://www.inlibra.com/de/agb - Open Access -