Neues Spiel, neues Glück

Rege Aktivitäten der Gesetzgeber von Bund und Ländern seit dem „Palantir-Urteil“ des Bundesverfassungsgerichts

Michael Bäuerle

02.09.2026 doi: 10.59704/f4da774a1ed19046

Mit seinem Urteil vom 16.2.2023[1] hatte das Bundesverfassungsgericht die 2018 in Hessen und 2019 in Hamburg geschaffenen polizeirechtlichen Ermächtigungsgrundlagen zum Einsatz einer sog. automatisierten Anwendung zur Datenanalyse (§ 25a HSOG, § 49 HmbPolDVG) für nichtig (Hamburg) bzw. mit der Verfassung unvereinbar (Hessen) erklärt.

Wie schon in fast drei Dutzend früheren verfassungsgerichtlichen Entscheidungen zum Informationsrecht der Sicherheitsbehörden,[2] verwarf das Gericht auch diesmal das Instrument der automatisierten Datenanalyse nicht vollständig, sondern verlangte gesetzgeberische „Nachbesserungen“ im Hinblick auf die Verhältnismäßigkeit der damit verbundenen Grundrechtseingriffe.[3]

Als Reaktion auf das Urteil überarbeiteten nicht nur die betroffenen Länder ihre Regelungen,[4] sondern es setzte in Bund und Ländern eine regelrechte Welle von Gesetzgebungsverfahren zum Erlass entsprechender Befugnisnormen ein.

Hamburg, Hessen und Nordrhein-Westfalen als Vorreiter der automatisierten polizeilichen Datenanalyse

Hessen schuf § 25a HSOG a.F., nachdem es als erstes Bundesland das von der umstrittenen US-amerikanischen Firma Palantir Inc.[5] angebotene Programm „Gotham“ erworben hatte. Mit Hilfe des entsprechend angepassten Programms sollten die umfangreichen und heterogenen landespolizeilichen Datenbestände zusammengeführt und analysiert werden.[6] Hamburg schuf zwar eine Ermächtigungsgrundlage, erwarb das Palantir-System jedoch nicht.[7]

Außer in Hessen und Hamburg gab es in Bund und Ländern zunächst keine vergleichbaren Regelungen. Im April 2022 trat dann in Nordrhein-Westfalen mit § 23 Abs. 6 NRWPolG eine Vorschrift in Kraft, die ebenfalls die automatisierte Analyse der dortigen polizeilichen Datenbestände ermöglichen soll;[8] auch gegen diese wurde Verfassungsbeschwerde erhoben.[9]

„Gesetzgebungswelle“ nach der Entscheidung

Auf die Entscheidung des Bundesverfassungsgerichts folgten nun zahlreiche Gesetze zur automatisierten Datenanalyse. Den Anfang machte der Bund mit § 29a Abs. 2a bis c Geldwäschegesetz[10], mit dem die Zentralstelle für Finanztransaktionsuntersuchungen zu entsprechenden Datenanalysen ermächtigt wird.[11]

Auf Länderebene schufen – in dieser zeitlichen Reihenfolge – sodann Bayern mit § 61a BayPAG[12], Rheinland-Pfalz mit § 65a POG Rh.-Pf.[13], Baden-Württemberg mit § 47a BW PolG[14], Berlin mit § 47a BlnASOG[15], Sachsen-Anhalt mit § 30a SOG LSA[16] und Sachsen mit § 62a SächsPVDG[17] entsprechende Ermächtigungsgrundlagen. Nordrhein-Westfalen reagierte auf das Urteil durch die Überarbeitung der bisherigen Regelung.[18]

Noch 2025 erließ der Bund – in Anknüpfung an nicht mehr umgesetzte Gesetzentwürfe der Ampelkoalition[19] – auch für den Zoll in § 13 Abs. 2 bis 6 ZFdG

[1] BVerfG, 1 BvR 1547/19, 1 BvR 2634/20, 16.2.2023, ZD 2023, 338 ff. (m. Anm. Petri).

[2] Vgl. deren Aufzählung bei Michael Bäuerle, *(R)Evolution im hessischen Polizeirecht*, HessVBl. 2026, S. 145 ff. (S. 146, Fn. 16).

[3] Vgl. zu den insoweit vom Gericht angelegten Maßstäben und Kriterien sowie zum prozessualen Hintergrund der großen Zahl an Entscheidungen zum Informationsrecht der Sicherheitsbehörden Fn. 2 (146 f.).

[4] Hessen mit einer am 12.7.2023 in Kraft getretenen Neufassung von § 25a HSOG und Hamburg mit einer am 5.2.2025 in Kraft getretenen Fassung von § 49 HmbPolDVG.

eine Befugnisnorm.[20] Nunmehr legte die Bundesregierung mehrere Gesetzentwürfe vor[21], mit denen entsprechende Ermächtigungsgrundlagen auch für das repressiv-polizeiliche Handeln (§ 98c StPO-E), die Bundespolizei (§ 58b BPolG-E) und – gestaffelt nach dessen Aufgaben gleich dreifach – das Bundeskriminalamt (§§ 9b, 39b, 63 BKAG-E) geschaffen werden sollen.[22]

Große Bandbreite an Regelungskonzepten

Infolge dieser regen gesetzgeberischen Tätigkeit liegt inzwischen eine große Vielfalt an Regelungsmustern für die automatisierte Datenanalyse vor. Die erlassenen Normen und Entwürfe unterscheiden sich hinsichtlich Textumfang, vorgesehener Eingriffsschwellen und Form- und Verfahrensvorschriften ganz erheblich. Sie müssen daher jeweils im Einzelnen anhand der vom Bundesverfassungsgericht in seinem Urteil vom 16.2.2023 aufgestellten Maßstäbe und Kriterien beurteilt werden. Diese sind infolge zahlreicher Je-Desto-Erwägungen hinsichtlich Eingriffstiefe und verfassungsrechtlicher Rechtfertigung alles andere als einfach.

Auch das Gericht wird in absehbarer Zeit über weitere Regelungen entscheiden. Zwar nahm es die Verfassungsbeschwerde gegen die nordrhein-westfälische Regelung – nach deren Änderung im Jahr 2025[23] – im Februar 2026 nicht zur Entscheidung an,[24] jedoch sind noch Verfassungsbeschwerden gegen die bayerische Regelung und die Neuregelungen in Hessen anhängig.[25]

Auf dem Weg zu Palantir II

Die vom Gericht aufgestellten Grundsätze boten und bieten den jeweiligen Beschwerdeführern in beiden Fällen jedenfalls genügend Anknüpfungspunkte für eine Behauptung der Verfassungswidrigkeit.

Sollte das Gericht die Maßstäbe aus dem ersten Urteil aufrechterhalten, werden bei der Überprüfung der Normen die bekannten Je-Desto-Relationen eine entscheidende Rolle spielen. Je stärker der Gesetzgeber Art und Umfang der Datenbestände begrenzt, die in eine Analyse integriert werden dürfen, und je mehr er die zulässigen Analysemethoden und Verwendungen der Ergebnisse limitiert, desto geringer dürfen die normativ vorgegebenen Eingriffsanlässe und -schwellen sein; gleiches gilt für die Anforderungen an die mit der Analyse verbundene Zweckänderung der Daten.[26]

Interessant wird sein, ob das Bundesverfassungsgericht insoweit auf die inzwischen lauter werdende Kritik an diesen – nicht selten als zu kleinteilig empfundenen Kriterien und Maßstäben[27] – reagiert und die Maßstäbe verändert oder neu justiert.

Eine größere Rolle könnten in der Folgeentscheidung die Fragen spielen, ob und unter welchen Voraussetzungen eine automatisierte Datenanalyse KI-gestützt erfolgen darf und inwieweit der Einsatz des Systems der umstrittenen Firma Palantir unter dem Gesichtspunkt der nationalen digitalen Souveränität[28] vertretbar ist.

KI-Einsatz und digitale Souveränität im verfassungsgerichtlichen Fokus?

Diese beiden Aspekte kamen im Urteil vom 16.2.2023 – immerhin, aber auch nur – am Rande zur Sprache. Den Gesichtspunkt der digitalen Souveränität verarbeitete das Gericht in der schlichten Wendung: „Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte“.[29] Der Aspekt des Einsatzes selbstlernender Systeme/künstlicher Intelligenz findet im Urteil an vier Stellen Erwähnung,[30] war aber im Hinblick auf die

[5] Vgl. zu den politischen Bedenken hinsichtlich der Seriösität der Anbieterfirma Andreas Brenneis, Kai Denker und Petra Gehring, *Data is Power – Code is Ideologie: Selbstmarketing und politische Positionierungen an der Spitze Palantirs in Big Data und KI*, in: Bäuerle/Denker/Geminn/Schöndorf-Haubold (Hrsg.), *Big Data und KI bei der Polizei – Das Palantir-Urteil in der interdisziplinären Diskussion*, 2025, S. 225 ff. sowie aus journalistischer Perspektive etwa Heike Wipperfürth, *Superstar der US-Überwachungsindustrie*, Deutschlandfunk 10.7.2020, https://www.deutschlandfunk.de/software-firma-palantir-superstar-der-us-100.html und Fiene Oswald, *Wo die Software-Firma Palantir bereits überall mitmischt*, Basecamp 12.4.2023, https://www.basecamp.digital/big-data-wo-die-software-firma-palantir-bereits-ueberall-mitmischt/, zuletzt abgerufen am 28.7.2026.

[6] Zu dem Erwerb wurde ein Untersuchungsausschuss im Hessischen Landtag eingesetzt, der vor allem beschaffungsrechtliche Fragen zum Gegenstand hatte, vgl. HessLT-Drs. 19/6864 (Teile A und B).

teilweise Unzulässigkeit der Verfassungsbeschwerde nicht Gegenstand der konkreten Prüfung.[31]

Unabhängig von dem Urteil ist die digitale Souveränität inzwischen in den Fokus der rechtspolitischen Diskussion geraten.[32] Unter diesem Gesichtspunkt ist das System der umstrittenen Firma Palantir besonders brisant, gerade wenn es von Sicherheitsbehörden eingesetzt wird.[33] Zwar betreiben das Programm bisher – soweit ersichtlich – nur Hessen, Bayern, Nordrhein-Westfalen und Baden-Württemberg (letzteres probeweise). Daher sind die Befugnisnormen und entsprechende Gesetzentwürfe im Bund und den übrigen Ländern bisher noch reine „Vorratsregelungen". Das Bundesamt für Verfassungsschutz setzt wohl inzwischen auf eine europäische Palantir-Alternative.[34] Daraus leitet die rechtspolitische Debatte ab, dass politisch die Abkehr von Palantir begonnen habe.[35] Andererseits hat sich der baden-württembergische Landtag jüngst mehrheitlich explizit für den Einsatz des Palantir-Programms ausgesprochen.[36]

Da auch Hessen an der Nutzung von Palantir-Gotham – also dem „Einsatz der Software privater Akteure oder fremder Staaten" – festhält, dürfte die verfassungsgerichtlich festgestellte Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte in der Argumentation der Beschwerdeführer gegen die Neuregelung sicher nicht zu kurz kommen.

Die hessische Neuregelung bietet – anders als etwa die bayerische Parallelnorm[37] – auch Anlass für eine konkrete verfassungsgerichtliche Entscheidung über das Ob und Wie einer KI-gestützten Datenanalyse. Hessen hat mit seiner Neuregelung nach dem erklärten Willen des Gesetzgebers[38] den Einsatz selbstlernender Systeme bei der automatisierten Datenanalyse legitimiert.[39]

2023 hatte das Gericht die Gefahren einer KI-gestützten Datenanalyse sehr plastisch umschrieben und die damit verbundene Erhöhung des Eingriffsgewichts betont.[40] Daran muss sich die hessische Neuregelung nun konkret messen lassen. Im Bund und den anderen Ländern verhalten sich die Vorschriften und Gesetzentwürfe zur Zulässigkeit eines KI-Einsatzes unterschiedlich. Das Spektrum reicht von explizit unzulässig (neben Bayern in Sachsen-Anhalt) über explizit zulässig (NRW, Berlin), bedingt zulässig (GwG, Sachsen) bis unklar (übrige Regelungen). Einige Regelungen beschränken sich etwa auf die aus dem Urteil übernommene Formulierung, dass „diskriminierende Algorithmen weder herausgebildet noch verwendet werden dürfen" (z.B. § 98c StPO-E), ohne sich zur Zulässigkeit von KI weiter zu verhalten.

Ob vor diesem Hintergrund der KI-Einsatz und die digitale Souveränität in den verfassungsgerichtlichen Fokus geraten, bleibt abzuwarten. Feststehen dürfte, dass sich die Serie der verfassungsgerichtlichen Entscheidungen zum Informationsrecht der Sicherheitsbehörden in absehbarer Zeit durch eine „Palantir II"-Entscheidung fortsetzen wird.[41]

[7] Und hat dies nach Presseinformationen auch im Jahr 2025 noch ausgeschlossen, vgl. die Meldung auf Zeit-Online vom 29.7.2025, abzurufen unter https://www.zeit.de/news/2025-07/29/innenbehoerde-schliesst-nutzung-von-palantir-software-aus, zuletzt abgerufen am 28.7.2026.

[8] Vgl. Clemens Arzt, in: *Möstl/Kugelmann, BeckOK Polizei- und Ordnungsrecht Nordrhein-Westfalen* (25. Aufl., 2023), § 23 PolG NRW, Rn. 50a ff.

[9] Vgl. die Meldung der klageführenden Gesellschaft für Freiheitsrecht vom 6.10.2022 unter https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-stop-data-mining, zuletzt abgerufen am 1.9.2026.

[10] In Kraft getreten am 18.11.2023.

[11] Vgl. Jan Ziegner, in: *Brian/Pelz, BeckOK Geldwäschegesetz* (26. Aufl., 2026), § 29, Rn. 7a ff.

AUTOR*IN
Michael Bäuerle
Michael Bäuerle ist Professor für öffentliches Recht an der Hessischen Hochschule für öffentliches Management und Sicherheit und stv. Direktor des Hessischen Zentrums verantwortungsbewusste Digitalisierung (ZEVEDI).

EMPFOHLENE ZITATION
Bäuerle, Michael: Neues Spiel, neues Glück: Rege Aktivitäten der Gesetzgeber von Bund und Ländern seit dem „Palantir-Urteil“ des Bundesverfassungsgerichts, Verfassungsblog, 02.09.2026, doi: 10.59704/f4da774a1ed19046.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260902-150521-0.

[12] In Kraft getreten am 1.4.2024.
[13] In Kraft getreten am 1.3.2025.
[14] In Kraft getreten am 3.12.2025.
[15] In Kraft getreten am 24.12.2025.
[16] In Kraft getreten am 14.4.2026.
[17] In Kraft getreten am 1.7.2026.
[18] Durch Schaffung des am 2.12.2025 in Kraft getretenen § 23 Abs. 6a NRWPolG.

[19] Vgl. dazu m.w.N. Michael Bäuerle, *Rechtspolitischer Rück – und Ausblick – hessenDATA und der schmale Grat zwischen polizeilicher Effizienz und Grundrechtsschutz*, in: Bäuerle/Denker/Geminn/Schöndorf-Haubold (Hrsg.), *Big Data und KI bei der Polizei – Das Palantir-Urteil in der interdisziplinären Diskussion*, 2025, S. 251 ff. (252).

[20] In Kraft getreten am 30.12.2025.

[21] BT-Drs. 21/6132 und 21/6808.

[22] Vgl. zu Inhalten und Stand der Gesetzgebungsverfahren die Dokumentation unter https://www.bundestag.de/dokumente/textarchiv/2026/kw28-de-strafprozessordnung-1192534, zuletzt abgerufen am 1.9.2026.

[23] Oben Fn. 18.

[24] Vgl. die Meldung der klageführenden Gesellschaft für Freiheitsrechte unter https://freiheitsrechte.org/themen/freiheit-im-digitalen-zeitalter/automatisierte-datenanalyse#abgeschlossene-verfahren, zuletzt abgerufen am 28.7.2026.

[25] Vgl. die Meldungen der klageführenden Gesellschaft für Freiheitsrecht unter https://freiheitsrechte.org/themen/freiheit-im-digitalen-zeitalter/hessen-big-data-analyse und https://freiheitsrechte.org/themen/freiheit-im-digitalen-zeitalter/palantir-bayern, zuletzt abgerufen am 28.7.2026.

[26] S. Fn. 1, Rn. 72 ff.

[27] Vgl. m.w.N. Fn. 2 (S. 147 und Fn. 22 und 23).

[28] Vgl. dazu auch Elena Esposito und Simon Egbert, *Palantir und digitale Souveränität*, Verfassungsblog, 26.8.2026, DOI: 10.59704/70233c5f9182b075, zuletzt abgerufen am 1.9.2026.

[29] S. Fn. 26, Rn.100.

[30] S. Fn. 26, Rn. 100, 121, 147.

[31] S. Fn. 26, Rn. 48: „Gegenstand der Prüfung ist damit weder die Frage, ob (…). Noch ist hier zu überprüfen, ob die für Transparenz und Rechtsschutz sorgenden Verfahrens- und Organisationsregelungen verfassungsrechtlichen Anforderungen genügen, *ob insbesondere auch mit Blick auf komplexe Formen automatisierten Datenabgleichs bis hin zu selbstlernenden Systemen (Künstliche Intelligenz, „KI") hinreichende verfahrensrechtliche Sicherungen bestehen*." (Hervorheb. d. Verf.).

[32] Vgl. etwa Michael Denga, *Datensouveränität und Data Cloud,* MMR 2026, 91 ff.

[33] Schon früh in Bezug auf Behörden mit Sicherheitsaufgaben Ulrich Kelber und Vyacheslav Bortnikov, *Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten*, NJW 2023, 2000 ff.

[34] Vgl. die Online-Meldung der Tagesschau vom 13.5.2026 unter https://www.tagesschau.de/investigativ/ndr-wdr/verfassungsschutz-palantir-100.html, zuletzt abgerufen am 28.7.2026.

[35] Vgl. die Meldung vom 19.5.2026 unter https://correctiv.org/aktuelles/gesellschaft-2/2026/05/19/die-abkehr-von-palantir-hat-begonnen/, zuletzt abgerufen am 28.7.2026.

[36] Vgl. die Meldung von SWR Aktuell vom 23.7.2026 unter https://www.swr.de/swraktuell/baden-wuerttemberg/abstimmung-zu-palantir-im-landtag-100.html, zuletzt abgerufen am 28.7.2026.

[37] Die in § 61a Abs. 5 Nr. 2 BayPAG die Verwendung selbstlernender Systeme für unzulässig erklärt.

[38] Vgl. HessLT-Drs. 21/1448, S. 10.

[39] Wenn auch fraglich ist, ob die Regelung zu dieser Rechtsfolge in verfassungsmäßiger Form ermächtigt, vgl. dazu näher Michael Bäuerle, in: *Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen* (39. Aufl., 2026), § 25a HSOG, Rn. 30 ff., 69 ff.

[40] Vgl. Fn. 26, Rn. 100: „Besonderes Eingriffsgewicht kann je nach Einsatzart die Verwendung lernfähiger Systeme, also Künstlicher Intelligenz (KI), haben. Deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines „predictive policing" getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein (vgl. EuGH ECLI:EU:C:2022:491 = EuZW 2022, 706 Rn. 195 = NJW 2022, 2903 Ls. – Ligue des droits humains). Dann droht zugleich die staatliche Kontrolle über diese Anwendung verloren zu gehen. Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte (vgl. Wiss. Dienst des Deutschen Bundestags, Datenbank-Analysen durch die Polizei. Grundrechte und Datenschutzrecht, 2.3.2020, WD3-3000-018/20, S. 8 mwN). Eine spezifische Herausforderung besteht darüber hinaus darin, die Herausbildung und Verwendung diskriminierender Algorithmen zu verhindern. Daher dürften selbstlernende Systeme in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern."

[41] Vgl. auch Michael Bäuerle, *Karlsruhe locuta, causa non finita – Palantir, die Polizei und kein Ende*, Verantwortungsblog 12.9.2024, https://zevedi.de/karlsruhe-locuta-causa-non-finita-palantir-die-polizei-und-kein-ende/, DOI: 10.60805/vp3w-fk07, zuletzt abgerufen am 28.7.2026.