LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/4971

A09, A12

Stellungnahme

der Gesellschaft für Freiheitsrechte e.V.

zu dem Entwurf eines Gesetzes zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und anderer Gesetze an das Telekommunikation-Telemedien-Datenschutz-Gesetz

Gesetzentwurf der Landesregierung, Drucksache 17/16517

Datum: 28. März 2022

INHALTSVERZEICHNIS

A. VORBEMERKUNG

1 Der Termin zur Abgabe der Stellungnahme ist sehr kurz bemessen. Wir haben unsere Stellungnahme daher auf die neue Ermächtigungsgrundlage in § 23 Abs. 6 PolG NRW n.F. beschränkt. Mit dieser Auswahl ist keine Aussage über die Unbedenklichkeit der übrigen vorgesehen Änderungen getroffen.

B. ZUSAMMENFASSUNG DER ERGEBNISSE

2 § 23 Abs. 6 PolG NRW n.F. ermöglicht die automatisierte Zusammenführung von Daten sowie deren Abgleich, Aufbereitung und Analyse. Auf Bundesebene existierte bereits eine vergleichbare Vorschrift in § 6a des Gesetzes zur Errichtung einer standardisierten Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – **ATDG**). Das Bundesverfassungsgericht hat die Vorschrift in einem Beschluss aus dem November 2020 (*Antiterrordateigesetz II*) für unvereinbar mit dem Recht auf informationelle Selbstbestimmung und nichtig erklärt und formulierte hohe Anforderungen für die erweiterte Datennutzung (auch als „Data Mining“ bezeichnet).

3 Der Gesetzesentwurf geht davon aus, dass diese Anforderungen vorliegend nicht zur Anwendung kämen, da § 23 Abs. 6 PolG NRW n.F. nicht zu einer derartigen erweiterten Datennutzung ermächtige. Dem ist nicht zuzustimmen (siehe hierzu **C.I.1**), sodass § 23 Abs. 6 PolG NRW n.F. – der weit hinter den entsprechenden Anforderungen zurückbleibt – in der vorgeschlagenen Fassung nicht mit dem Grundgesetz vereinbar ist. Konkret ist die Vorschrift unverhältnismäßig, da sie den Einsatz auch bei nicht hochrangigen öffentlichen Interessen ermöglicht, keine hinreichenden Einsatzschwellen vorsieht und die Gefahr einer verfassungswidrigen Profilbildung nicht ausschließt (siehe hierzu **C.I.2.1**). Zudem mangelt es der Vorschrift an den erforderlichen Verfahrenssicherungen (siehe hierzu **C.I.2.2**). Schließlich ist die Vorschrift auch zu unbestimmt (siehe hierzu **C.I.2.3**).

4 Darüber hinaus ist aber auch anzumerken, dass erhöhte Anforderungen an Ermächtigungsgrundlagen nicht lediglich für erweiterte Datennutzung bestehen – wie dies die Gesetzesbegründung zu suggerieren scheint. Vielmehr ergibt sich aus dem Verhältnismäßigkeitsgrundsatz ganz allgemein, dass bei intensiven Eingriffen – um die es hier u.a. wegen der Datenvielfalt, Streubreite und

Anlasslosigkeit der Maßnahme geht – auch erhöhte Anforderungen an die Grundlage für derartige Eingriffe zu stellen sind. Selbst wenn es sich bei § 23 Abs. 6 PolG NRW n.F. nicht um eine Ermächtigung zur erweiterten Datennutzung im Sinne der Entscheidung *Antiterrordateigesetz II* handeln sollte – wovon nicht auszugehen ist – müsste die Vorschrift daher dennoch als verfassungswidrig eingestuft werden (siehe hierzu **C.II**).

5 Schließlich ist noch darauf hinzuweisen, dass bei der Verwendung von auf „Palantir Gotham“ basierender Software – oder vergleichbarer Software – nicht nur hohe Anforderungen an die gesetzliche Grundlage zum Einsatz dieser Software bestehen. Derartige Software birgt auch hohe Risiken in Bezug auf die Datensicherheit und den Datenschutz. Die Entscheidung zum Einsatz derartiger Software sollte damit auch mit gesetzlichen Vorkehrungen zum Schutz der verwendeten Daten verbunden werden. Diese lässt der Gesetzesentwurf vermissen (siehe hierzu **C.III**).

C. STELLUNGNAHME

I. SPEZIELLE ANFORDERUNGEN FÜR ERWEITERTE DATENNUTZUNG („DATA MINING“) NICHT ERFÜLLT

6 Das Bundesverfassungsgericht hat in seiner Entscheidung *Antiterrordateigesetz II* festgestellt, dass eine Datenauswertung einer Verbunddatei von Polizeibehörden in Form einer „erweiterten Nutzung“ einen vertieften Grundrechtseingriff darstellt.[1] Es hat darauf aufbauend Anforderungen für eine derartige erweiterte Nutzung (auch als „Data Mining“ bezeichnet) formuliert, welche auch für die Datenauswertung nach § 23 Abs. 6 PolG NRW n.F. gelten (unter **1.**).[2] § 23 Abs. 6 PolG NRW n.F. genügt diesen Anforderungen nicht und verletzt daher das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (unter **2.**).

---

1 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Leitsatz 2 sowie Rn. 109 ff.

2 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 115 ff.

1. VORSCHRIFT IST ERMÄCHTIGUNG ZUR ERWEITERTEN DATENNUTZUNG

7 Nach dem Bundesverfassungsgericht liegt eine erweiterte Datennutzung vor, wenn „in einer Datei gespeicherte Daten aus verschiedenen nachrichtendienstlichen und polizeilichen Quellen im Wege der Verknüpfung zur Erzeugung neuer Erkenntnisse und Zusammenhänge genutzt“ werden.[3] Die Datennutzung ist damit insofern erweitert, als dass nicht lediglich auf ein Grunddatum erneut Rückgriff genommen werden kann, sondern dass durch die Verknüpfung neue Informationen generiert werden. Aus diesem Grund kommt der erweiterten Nutzung laut Bundesverfassungsgericht grundsätzlich eine gesteigerte Belastungswirkung zu.[4]

8 Eine derartige Verknüpfung und damit verbundene Erzeugung neuer Erkenntnisse liegt bei § 23 Abs. 6 PolG NRW n.F. vor. Die Vorschrift ermöglicht die **Zusammenführung** von Daten sowie deren anschließenden **Abgleich**, **Aufbereitung** und **Analyse**. Dabei geht es laut Gesetzesbegründung insbesondere um das „Generieren von Erkenntnissen, die in polizeilichen Datenbanken isoliert bereits vorhanden sind“.[5]

9 Insoweit die **Gesetzesbegründung** davon auszugehen scheint, dass die Anforderungen an erweiterte Datennutzung im Falle § 23 Abs. 6 PolG NRW n.F. nicht zur Anwendung kämen, scheint diese Einordnung auf einem Fehlverständnis der erweiterten Datennutzung zu basieren: Die Gesetzbegründung unterscheidet fälschlicherweise im Wesentlichen danach, ob die erweiterte Datennutzung „selbständig“ angestoßen wird oder ob diese durch menschliche Bearbeiter*innen geschieht.[6] Die Begründung geht davon aus, dass durch Einfügen von § 23 Abs. 6 Satz 3 PolG NRW n.F. die verfassungsrechtlichen Anforderungen zur erweiterten Datennutzung nicht gelten würden.[7] Die Vorschrift verbietet es, die „zusammengeführten Daten mittels statistisch-mathematischer Verfahren oder in sonstiger Weise selbständig auf Zusammenhänge“ zu analysieren.

---

3 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 109.
4 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 109.
5 Landtag Nordrhein-Westfalen, Drucksache 17/16517, Gesetzesbegründung, S. 17.
6 Landtag Nordrhein-Westfalen, Drucksache 17/16517, Gesetzesbegründung, S. 18.
7 Landtag Nordrhein-Westfalen, Drucksache 17/16517, Gesetzesbegründung, S. 18.

10 § 23 Abs. 6 Satz 3 PolG NRW n.F. führt jedoch nicht dazu, dass sämtliche Analysevorgänge nur durch menschliche Bearbeiter*innen durchgeführt werden können. Die Gesetzesbegründung macht vielmehr deutlich, dass es bei der Beschränkung des Satzes 3 darum geht, durch wen Analysevorgänge in Gang gesetzt werden.

> *„Der Rechtsbegriff „selbständig“ meint dabei die **rein** automatisierte Auswertung von Datenbeständen ohne menschliches Zutun. Die Vorschrift erlaubt damit insbesondere keine **automatisierte Entscheidungsfindung** […]. Nicht ausgeschlossen sind dagegen vom menschlichen Bearbeiter […] **angestoßene** weitere Analysevorgänge.“*[8]

11 Die Unterscheidung danach, durch wen eine Analyse angestoßen wird, ist rein formalistischer Natur und vermag nicht darüber hinweghelfen, dass es sich auch bei § 23 Abs. 6 PolG NRW n.F. um eine Form der erweiterten Datennutzung handelt. Dies wird bereits durch die nähere Beschreibung der ermöglichten Datennutzung offensichtlich. § 23 Abs. 6 PolG NRW n.F. beschreibt zwar selbst lediglich, dass die Polizei Daten automatisiert zusammenführen, mit weiteren Daten aufbereiten und analysieren dürfe (zur Problematik dieser abstrakten Umschreibung siehe **2.3**). Die Gesetzesbegründung konkretisiert jedoch, dass die Vorschrift insbesondere Folgendes umfasse:

> *„das **Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen**, den **Ausschluss von unbedeutenden Informationen und Erkenntnissen**, die **Zuordnung eingehender Informationen zu bekannten Sachverhalten** sowie eine rein **statistische Auswertung der gespeicherten Daten,** ebenso die **Darstellung** in Form von **räumlichen und sonstigen Beziehungen zwischen Personen** sowie **Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen** aus den Ergebnissen der manuell angestoßenen Analyse.“* [9]

---

8 Landtag Nordrhein-Westfalen, Drucksache 17/16517, Gesetzesbegründung, S. 18 (Hervorhebung nur hier).

9 Landtag Nordrhein-Westfalen, Drucksache 17/16517, Gesetzesbegründung, S. 18 (Hervorhebung nur hier).

12 Damit enthält die Gesetzesbegründung exakt die Umschreibung, die bereits in § 6a Abs. 5 ATDG Grundlage der Entscheidung des Bundesverfassungsgerichts war. Dort heißt es:

> *„Eine erweiterte Nutzung sind das **Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen**, der **Ausschluss von unbedeutenden Informationen und Erkenntnisse**, die **Zuordnung eingehender Informationen zu bekannten Sachverhalten** sowie die **statistische Auswertung der gespeicherten Daten**. Hierzu dürfen die beteiligten Behörden des Bundes […] **räumliche und sonstige Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen darstellen** […].“*[10]

13 Die Beschränkung, dass Analysevorgänge von menschlichen Bearbeiter*innen angestoßen werden müssen, vermag nichts daran zu ändern, dass es sich um dieselbe Maßnahme handelt, über welche das Bundesverfassungsgericht in *Antiterrordateigesetz II* geurteilt hat. Entscheidend für die gesteigerten verfassungsrechtlichen Anforderungen ist die **erhöhte Eingriffsintensität** durch die Verbindung der Daten. Dementsprechend betont auch das Bundesverfassungsgericht, dass sich die gesteigerte Belastungswirkung der erweiterten Datennutzung daraus ergibt, dass diese „zur Erzeugung neuer Erkenntnisse und Zusammenhänge genutzt“ wird.[11]

14 Gerade aus Sicht von Menschen, die von einem solchen Grundrechtseingriff betroffen sind, macht es keinen Unterschied, ob nur die Zusammenführung automatisiert stattfindet oder bereits die Erhebung der personenbezogenen Daten oder auch eine weitere Analyse automatisiert erfolgt. Das Ziel und die dadurch bestehende typische Gefahr der erweiterten Datennutzung ist und bleibt in allen Fällen die Generierung neuer Erkenntnisse in Folge einer Zusammenführung und umfassenden Analyse und Auswertung der Querverbindungen gespeicherter Datensätze. Diese Gefahr besteht genauso, wenn menschliche Bearbeiter*innen jeweils anhand von bereits vorliegenden oder im Zuge der Analyse festgestellten Erkenntnissen weitere Analysevorgänge anstoßen. Es ist mithin die Gesamtwirkung zu betrachten.

---

10 § 6a Abs. 5 Satz 1 ATDG (Hervorhebung nur hier).

11 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 109.

15 Dabei geht die Eingriffsintensität von § 23 Abs. 6 PolG NRW n.F. sogar noch über die von § 6a ATDG hinaus.[12] Bei letzterer wurden bestimmte, besonders sensible Daten von der Zusammenführung ausgenommen (§ 4 ATDG). Eine solche Beschränkung enthält § 23 Abs. 6 PolG NRW n.F. nicht. Im Gegenteil können über § 23 Abs. 6 PolG NRW n.F. eine Vielzahl an Daten aus verschiedensten Quellen zusammengeführt werden. Dabei ergibt sich die Möglichkeit zur Erhebung der Daten bereits aus den allgemeinen Regelungen (§§ 9 ff. PolG NRW) und nicht aus § 23 Abs. 6 PolG NRW n.F. selbst. Nach §§ 9 ff. PolG NRW hat die Polizei NRW weitreichende Datenerhebungsbefugnisse und kann sich im Rahmen ihrer Aufgaben Daten von öffentlichen und privaten Stellen übermitteln lassen, beispielsweise vom Landesamt für Verfassungsschutz, der Ausländerbehörde, der Meldebehörde, den Sozialämtern und weiteren öffentlichen Stellen. Von privaten Stellen wie Banken, Verkehrsunternehmen oder Telekommunikationsanbietern kann sich die Polizei Kreditkarteninformationen, Reiserouten oder Verkehrs- und Verbindungsdaten übermitteln lassen. Auch Daten aus allgemein zugänglichen Quellen darf die Polizei nach § 9 PolG NRW erheben.[13] Dazu gehören auch Profile und Beiträge aus sozialen Netzwerken wie Facebook und Twitter. Da gerade hier Menschen teilweise äußerst viel und äußerst Privates über sich preisgeben, ermöglicht die Miterfassung dieser Daten eine erheblich detaillierte Analyse einzelner Personen, die bereits an eine verfassungswidrige Profilbildung grenzen dürfte (siehe hierzu unter **2.1.3**). Dementsprechend kann keinesfalls davon ausgegangen werden, dass für § 23 Abs. 6 PolG NRW n.F. geringere verfassungsrechtliche Anforderungen gelten könnten.

16 Zudem ist zu berücksichtigen, dass die Ermächtigungsgrundlage des § 23 Abs. 6 PolG NRW n.F. den Einsatz von auf „Palantir Gotham“ basierender Software – oder vergleichbarer Software – ermöglichen soll. Derartige Software geht weit über die Zusammenführung von einzelnen Daten in einer Verbunddatei hinaus und zielt gerade auf die Generierung neuer Erkenntnisse durch die Verknüpfung bereits vorhandener Datensätze ab.[14] Die Ermächtigungsgrundlage bezweckt

---

12 Vgl. zu vergleichbaren Vorschriften *Golla*, NRW 2021, 667 (671).

13 Siehe auch *Korte*, ZD-Aktuell 2021, 05192.

14 Vgl. *Korte*, ZD-Aktuell 2021, 05192; *Monroy*, Europol nutzt Palantir, Netzpolitik.org (11. Juni 2020), verfügbar unter https://netzpolitik.org/2020/europol-nutzt-palantir/.

also gerade den Einsatz von Software, deren elementare Funktion die erweiterte Datennutzung ist.

2. VERFASSUNGSRECHTLICHE ANFORDERUNGEN AN ERWEITERTE DATENNUTZUNG NICHT ERFÜLLT

17 § 23 Abs. 6 PolG NRW n.F. erfüllt nicht die Voraussetzungen, die das Bundesverfassungsgericht an die erweiterte Datennutzung aufgestellt hat. Die Vorschrift genügt weder den vom Bundesverfassungsgericht aufgestellten Anforderungen an die Verhältnismäßigkeit (unter **2.1**) noch enthält es die notwendigen Verfahrenssicherungen (unter **2.2**). Außerdem ist die Vorschrift nicht hinreichend bestimmt formuliert (unter **2.3**).

2.1 UNVERHÄLTNISMÄSSIG

18 Gemessen an der Intensität des Eingriffs genügt die Eingriffsermächtigung nicht dem Grundsatz der Verhältnismäßigkeit. Aus der hohen Eingriffsintensität ergibt sich, dass die erweiterte Datennutzung einem herausragenden öffentlichen Interesse dienen muss.[15] § 23 Abs. 6 PolG NRW n.F. ermöglicht aber auch Eingriffe aus geringeren Anlässen (unter **2.1.1**). Zudem ist für die komplexe Auswertung zu Zwecken der Gefahrenabwehr grundsätzlich eine „wenigstens hinreichend konkretisierte Gefahr in dem Sinne [...], dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr vorliegen“, zu fordern.[16] Auch diesem Erfordernis genügt § 23 Abs. 6 PolG NRW n.F nicht (**2.1.2**). Schließlich besteht aufgrund der Einbindung von Daten aus sozialen Medien die erhöhte Gefahr einer verfassungswidrigen Profilbildung, ohne dass Sicherungsmechanismen diesbezüglich vorhanden sind (**2.1.3**).

2.1.1 UNZUREICHENDE EINSCHRÄNKUNG DER GESCHÜTZTEN RECHTSGÜTER

19 Aufgrund des hohen Eingriffsgewichts der erweiterten Datennutzung fordert das Bundesverfassungsgericht, dass die Nutzung einem **herausragenden öffentlichen Interesse** dienen muss. Sie ist daher nur zum Schutz von

---

15 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 116.

16 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 118.

besonders gewichtigen Rechtsgütern wie Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zulässig.[17]

20 § 23 Abs. 6 PolG NRW n. F. ermöglicht hingegen auch eine erweiterte Datennutzung zum Schutz von Sachen von bedeutendem Wert. Bereits aus diesem Grund ist die Vorschrift unverhältnismäßig.

21 Ebenso ermöglicht die Einbeziehung des Straftatenkatalogs des § 100a Abs. 2 StPO eine unverhältnismäßige erweiterte Datennutzung bereits bei Rechtsgütern ohne herausragende Bedeutung. Als Anknüpfungspunkt nicht hinreichend sind mindestens das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB), Geldfälschung (§ 146 Abs. 1 StGB), Vorteilsgewährung (§ 333 Abs. 1 StGB) und Verleitung zur missbräuchlichen Asylantragsstellung (§ 84 AsylG). Zudem begrenzt § 100a StPO den Anwendungsbereich der Telekommunikationsüberwachung über den Straftatenkatalog hinaus im Abs. 1 auf Straftaten, die auch im Einzelfall schwer wiegen. Durch den unmittelbaren Verweis des § 23 Abs. 6 PolG NRW n.F. auf den Straftatenkatalog des § 100a Abs. 2 StPO fehlt diese Begrenzung.

22 Schließlich erweitert § 23 Abs. 6 PolG NRW n.F. den Straftatenkatalog sogar noch über § 100a Abs. 2 StPO hinaus um §§ 176a, 176b, 176e, 177, 178, 180, 181a und 182 StGB. Im Ergebnis bedeutet dies, dass zwar keine Telekommunikationsüberwachung nach § 100a Abs. 1 StPO möglich wäre, die erweiterte Nutzung von Daten hingegen schon, obwohl dies ebenfalls einen intensiven Grundrechtseingriff darstellt. (zur Eingriffsintensität siehe **II.1**).

2.1.2 KEINE HINREICHENDEN EINGRIFFSSCHWELLEN

23 Der Eingriff durch die erweiterte Nutzung muss zudem an hinreichend konkretisierte Eingriffsschwellen für die erweiterte Nutzung zu Zwecken der Gefahrenabwehr und Strafverfolgung auf Grundlage normenklarer Regelungen gebunden sein.[18] Dabei muss eine wenigstens **hinreichend konkretisierte Gefahr** in dem Sinne gegeben sein, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr vorliegen.[19] Für den Bereich der

---

17 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 116.
18 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 117.
19 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 118.

Strafverfolgung müssen konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht einer Straftat vorhanden sein.[20] Die Anforderungen gehen damit über das Vorliegen eines Anfangsverdachts im Sinne von § 152 Abs. 2 StPO hinaus.

24 Diesen Anforderungen genügt § 23 Abs. 6 PolG NRW n.F. nicht. Eine konkrete Gefahr, wie sie vom Bundesverfassungsgericht gefordert wird, ist nach der Vorschrift nicht notwendig, um die erweiterte Datennutzung einzusetzen. Stattdessen knüpft die Vorschrift weit im Vorfeld einer solchen Gefahr an. So ermöglicht diese das Tätigwerden bereits zur „vorbeugenden Bekämpfung von in § 100a Absatz 2 der Strafprozessordnung genannten oder [weiterer] Straftaten". Besonders der unscharfe Begriff der vorbeugenden Bekämpfung von Straftaten gewährleistet nicht, dass die Datenübermittlung an eine konkrete Gefahr im verfassungsrechtlichen Sinne gebunden wird, was jedoch geboten wäre. Denn die Erforderlichkeit der Datenauswertung zur vorbeugenden Bekämpfung von Straftaten lässt sich schon annehmen, lange bevor konkrete Tatsachen die Annahme rechtfertigen, dass eine Straftat begangen werden soll. Dementsprechend werden für die vorbeugende Bekämpfung **abstrakte Gefahrenlagen** als ausreichend angesehen.[21]

25 Auf welcher konkreten Tatsachengrundlage der Einsatz der automatisierten Zusammenführung und die anschließende Datennutzung fußen können, bleibt offen. Fast zwangsläufig wird es sich hierbei vor allem um vage und wenig aussagekräftige Faktoren wie die persönlichen Überzeugungen und sozialen Beziehungen des Betroffenen handeln, die für eine verfassungsrechtlich tragfähige Schadensprognose jedoch nicht ausreichen. Diese Gefahr wird durch die „Einschränkung" des § 23 Abs. 6 Satz 3 PolG NRW n.F. nur noch verstärkt. So wird durch das Erfordernis, dass Analysevorgänge von menschlichen Bearbeiter*innen angestoßen werden müssen, ein **Anreiz** gesetzt, dass diese möglichst viele Zusammenführungen in Gang setzen. Mangels einer konkretisierten Eingriffsschwelle, müssen jedoch keine hinreichenden Anknüpfungspunkte für ein solches Vorgehen nachgewiesen werden.

---

20 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 120.

21 BayVerfGH, Entscheidung vom 7. Februar 2006 – Vf. 69-VI-04; *Denninger*, in: Lisken/ders., Handbuch des Polizeirechts, 6. Aufl. 2018, Rn. D 1 ff., m.w.N; Kritisch *Bäcker*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Rn. D 263.

26 Zudem enthält § 100a Abs. 2 StPO strafrechtliche Vorfeldtatbestände, deren bevorstehende Verwirklichung nicht zwingend auf eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut schließen lässt. Im Straftatenkatalog des § 100a StPO finden sich neben Erfolgsdelikten auch **Gefährdungstatbestände**, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren. Teilweise verlagern diese Tatbestände die Strafbarkeit erheblich vor. Beispielhaft sei auf § 129a StGB und § 89a StGB verwiesen. Die Rechtsprechung begrenzt etwa § 89a StGB vor allem, indem sie hohe Anforderungen an den subjektiven Tatbestand stellt. Diese Begrenzung wirkt sich jedoch im präventiven Handlungsfeld allenfalls schwach aus. Denn im Voraus lassen sich die genauen Absichten und die Motivation des Betroffenen kaum erschließen. Eine präventiv ausgerichtete Überwachung muss darum ganz überwiegend an äußerliche, klar erkennbare Tatsachen anknüpfen. Vorfeldtatbestände wie § 129a oder § 89a StGB, die auf der objektiven Seite sehr weit gefasst sind, bieten deshalb kaum Anknüpfungspunkte, um die von § 23 Abs. 6 PolG NRW n.F. geforderte Prognoseentscheidung normativ anzuleiten. Diese Entscheidung kann vielmehr in weitem Umfang an hoch ambivalente und vage Erkenntnisse anknüpfen.

27 Insoweit überrascht auch, dass § 23 Abs. 6 PolG NRW n.F. gegenüber den derzeit vom Bundesverfassungsgericht überprüften Vorschriften, § 49 des Gesetzes über die Datenverarbeitung bei der Polizei Hamburg (**HmbPolDVG**) und § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (**HSOG**), zurückbleibt. Diese ermöglichen die erweiterte Datennutzung nur „in begründeten Einzelfällen“. Auch diese Einschränkung genügt den verfassungsrechtlichen Anforderungen im Ergebnis nicht,[22] stellt aber zumindest eine gewisse Eingriffsschwelle dar, auf die § 23 Abs. 6 PolG NRW n.F. vollkommen verzichtet.

2.1.3 KEINE BESCHRÄNKUNG VON DATEN AUS SOZIALEN MEDIEN

28 Besonders problematisch ist auch, dass § 23 Abs. 6 PolG NRW n.F. aufgrund der Vielzahl an Daten aus unterschiedlichsten Quellen dazu verwendet werden kann, Verhaltensprofile von Menschen zu erstellen. Eine derartige Profilbildung wurde vom Bundesverfassungsgericht als nicht mit der Verfassung vereinbar angesehen.[23] Besondere Gefahr birgt insbesondere der Zugriff auf soziale Medien (siehe hierzu bereits unter **1.**). Es ist zu begrüßen, dass dieser Zugriff in

---

22 *Golla*, NJW 2021, 667 (671).

23 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 – *BKAG*, Rn. 130.

der Praxis scheinbar beschränkt werden soll.[24] Aus verfassungsrechtlicher Sicht ist dies jedoch nicht hinreichend. Vielmehr bedürfte es bereits einer Einschränkung in § 23 Abs. 6 PolG NRW n.F. selbst, an der es aber fehlt.

2.2 FEHLENDE VERFAHRENSSICHERUNGEN

29 Es fehlt der Regelung darüber hinaus an ausreichenden begleitenden Verfahrenssicherungen. Bei der Speicherung und Nutzung personenbezogener Daten für die behördliche Aufgabenwahrnehmung hat der Gesetzgeber unter Verhältnismäßigkeitsgesichtspunkten auch Anforderungen an Transparenz, Rechtsschutz und Kontrolle zu beachten.[25] § 23 Abs. 6 PolG NRW n.F. erfüllt keine dieser Anforderungen.

2.2.1 FEHLENDE TRANSPARENZSCHAFFENDE REGELUNGEN

30 § 23 Abs. 6 PolG NRW n.F. enthält keine ausreichenden transparenzschaffenden Regelungen.

31 Zunächst findet die Benachrichtigungspflicht aus § 33a PolG NRW keine Anwendung auf § 23 Abs. 6 PolG NRW n.F. [26] Es besteht zwar ein Auskunftsanspruch nach § 49 DSG NRW, allerdings ist dies angesichts der Schwere des Eingriffs, der über die bereits vorhandenen personenbezogenen Daten einer Person weitergehende Erkenntnisse bis hin zu weitreichenden Persönlichkeitsprofilen generieren kann, nicht ausreichend. Es wäre zumindest eine Benachrichtigung der Betroffenen nach Abschluss des Einsatzes einer Anwendung zur automatisierten Datennutzung verfassungsrechtlich geboten.

---

24 Vgl. Schreiben des Innenministeriums Nordrhein-Westfalen vom 7. Mai 2021, Vorlage 17/5418, S. 14; *Rosenbach/Sarovic*, NRW Datenschutzbeauftragte hält Einsatz von Palantir-Software für unzulässig, Spiegel (15. April, 2021), verfügbar unter https://www.spiegel.de/netzwelt/palantir-nrw-datenschuetzerin-haelt-einsatz-von-software-fuer-unzulaessig-a-af196b3f-b93c-475d-86d7-8e569d25490c.

25 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 135.

26 Schreiben der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen vom 25. März 2021, Vorlage 17/5078, S. 11.

2.2.2 FEHLENDE KONTROLLE UND AUFSICHT

32 Auch in Bezug auf die Gewährleistung einer wirksamen Kontrolle und Aufsicht verfehlt § 23 Abs. 6 PolG NRW n.F. die verfassungsrechtlichen Anforderungen.

33 Zunächst bedarf es keiner gesonderten Anordnung. Zudem finden die Regelungen zur aufsichtlichen Kontrolle nach § 33c PolG NRW keine Anwendung auf § 23 Abs. 6 PolG NRW n.F.[27] Gerade der Einsatz (teil-)autonomer Systeme verleiht jedoch Maßnahmen zur Gefahrenabwehr einen gänzlich neuen Charakter und eine Intransparenz, die über das übliche Maß beim Einsatz technischer Hilfsmittel hinausgeht, auch wenn diese Analysesysteme zunächst von menschlichen Bearbeiter*innen initiiert werden müssen. Die Funktionsweisen derartiger Hilfsmittel sind technisch besonders komplex und entwickeln sich dynamisch weiter, so dass es einer kontinuierlichen Überprüfung bedarf, die weder Betroffenen noch den sicherheitsbehördlichen Endanwender*innen allein ohne Weiteres möglich ist. Es ist daher eine unabhängige Instanz einzusetzen, um die technische Dimension zur Umsetzung von § 23 Abs. 6 PolG NRW n.F. zu kontrollieren und die eingesetzte Software ggf. im Vorfeld zu zertifizieren.

34 Überraschenderweise steht § 23 Abs. 6 PolG NRW n.F. damit selbst hinter § 6a ATDG sowie Parallelvorschriften anderer Bundesländer zurück, namentlich § 49 HmbPolDVG und § 25a HSOG. Letztere enthalten immerhin den – im Ergebnis jedoch nicht ausreichenden[28] – folgenden Absatz 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.“*

35 Eine solche Regelung fehlt in § 23 PolG NRW gänzlich. Damit bedarf es keiner Anordnung durch die Behördenleitung. So kann die erweiterte Datennutzung zwar nicht „selbständig“ geschehen, jedoch durch jedwede Ermittlungsperson eingeleitet werden.

---

27 Schreiben der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen vom 25. März 2021, Vorlage 17/5078, S. 11.

28 *Golla*, NJW 2021, 667 (671).

36 Die Schwere des Eingriffs erfordert zur Durchführung von Maßnahmen nach § 23 Abs. 6 PolG NRW n.F. als rechtliche Kontrollmechanismen zunächst einen Richter*innenvorbehalt, zumindest jedoch die Zustimmung der mit Zugriffs- und Anordnungsbefugnissen ausgestatteten Datenschutzbeauftragten oder vergleichbare Mechanismen.

2.2.3 UNZUREICHENDE REGELUNGEN ZU DAUER UND LÖSCHUNG

37 Darüber hinaus fehlt es an eingrenzenden Vorgaben zur Dauer der Maßnahme, und zur Löschung der durch die automatisierte Datenanalyse generierten Erkenntnisse.[29]

38 Zwar mögen die allgemeinen Regelungen zur Dauer der Datenspeicherung (§ 22 PolG NRW) sowie zur Zweckbindung (§ 23 Abs. 2 bis 4 PolG NRW) anwendbar sein, aufgrund der Besonderheiten der automatisierten Datenzusammenführung und der anschließenden Analyse lassen diese Regelungen jedoch wesentliche Fragen unbeantwortet. Fraglich ist beispielweise, ob die Regelungen zur Löschung nach § 32 Abs. 1 Satz 2 PolG NRW und § 54 DSG NRW jeweils angepasst werden, wenn Daten innerhalb der automatisierten Zusammenführung generiert und diese Verknüpfungen dort gespeichert werden. Unklar ist auch, wie lange die Datenanalysen selbst und ihre Ergebnisse gespeichert bleiben.

2.2.4 KEINE SICHERUNG DER ART UND QUALITÄT DER DATEN

39 Außerdem fehlt es § 23 Abs. 6 PolG NRW n.F. an einer Eingrenzung der einzubeziehenden Daten und Vorkehrungen zur Sicherung ihrer Qualität. Dadurch ist die Regelung unverhältnismäßig, da sie ohne entsprechende Absicherung keine komplexen Analysen ermöglicht, welche wirksam zum Zweck der Gefahrenabwehr beitragen.

40 Eine komplexe Datenanalyse ist neben der Leistungsfähigkeit der Analysemethoden vor allem von der Art und Qualität der zugrunde liegenden Daten abhängig. Ohne eine ausreichend gesicherte Datenbasis kann sie keine

---

29 Vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 – *BKAG*, Rn. 144.

validen Ergebnisse liefern und letztlich nicht zum Zweck der Gefahrenabwehr beitragen.[30]

41 Werden komplexe Datenanalysen ohne weitere Überprüfung mit Informationen aus polizeilichen Datenbeständen gespeist, besteht erstens die Gefahr, dass sie den Kontext der ursprünglichen Erhebung der Daten vernachlässigen. Die konkrete Aussagekraft personenbezogener Daten erschließt sich nur aus dem sozialen Kontext ihrer Erhebung.

42 Zweitens kann eine ungeprüfte Einbeziehung vorhandener Datenbestände dazu führen, dass sich menschliche Vorurteile oder Fehlwahrnehmungen, die bereits in den Datenbeständen festgehalten sind, in der Anwendung zur Auswertung perpetuieren. Hieraus ergeben sich schwerwiegende Diskriminierungsrisiken, die einerseits die Eingriffsintensität der Datenverarbeitung steigern und andererseits eine prozedurale Absicherung erfordern.[31]

43 Dass sich neuartige Risiken der Diskriminierung durch moderne Überwachungstechnologien auf internationaler Ebene bereits realisieren, lässt sich beispielsweise anhand des Einsatzes von Software zur intelligenten Gesichtserkennung [32] oder zur Vorhersage von Bandenkriminalität nachvollziehen.[33]

44 Derartigen Risiken ist bei der komplexen Datenauswertung unter anderem durch Anforderungen an die Qualität von Daten, die in die Analysen einbezogen werden, vorzubeugen. § 23 Abs. 6 PolG NRW n.F. sieht hierzu allerdings keine Regelung

---

30 *Härtel*, LKV 2019, 49 (54).

31 *Härtel*, LKV 2019, 49; Singelnstein, NStZ 2018, 1 (6). In der Vergangenheit führte bspw. der Einsatz einer anderen Variante der Software bereits zur Diskriminierung marginalisierter Gruppen, *Moorstedt*, Vor dem Algorithmus sind nicht alle gleich, Süddeutsche Zeitung (2. Januar 2021), verfügbar unter https://www.sueddeutsche.de/digital/usa-palantir-corona-impfung-diskriminierung-kapitalismus-1.5158261.

32 *Gierlinger*, Warum Tech-Konzerne der Gesichtserkennung abschwören, Süddeutsche Zeitung (12. Juni 2020), verfügbar unter https://www.sueddeutsche.de/digital/microsoft-gesichtserkennung-rassismus-1.4934730.

33 *Grüner*, Amnesty kritisiert Polizei für diskriminierende Algorithmen, Golem.de (30. September 2020); verfügbar unter https://www.golem.de/news/predictive-policing-amnesty-kritisiert-polizei-fuer-diskriminierende-algorithmen-2009-151209.html.

vor. Der Gesetzgeber wäre verpflichtet gewesen, den Mindeststandard der Qualität der einbezogenen Daten genauer zu definieren.

2.3 MANGELNDE BESTIMMTHEIT UND NORMENKLARHEIT

45 Insbesondere in Fällen, in denen – wie hier – Grundrechte ohne Wissen der Betroffenen und ohne die Möglichkeit gerichtlicher Einzelfallkontrolle eingeschränkt werden, muss der Inhalt der einzelnen Normen verständlich und ohne größere Schwierigkeiten durch Auslegung zu konkretisieren sein.[34]

46 Vorliegend fehlt es allerdings an der Bestimmtheit der Norm. Das rechtsstaatliche Bestimmtheitsgebot verlangt vom Gesetzgeber bezogen auf Eingriffsbefugnisse, dass er technische Eingriffsinstrumente genau bezeichnet und dadurch sicherstellt, dass Adressaten den Inhalt der Norm jeweils erkennen können.[35] Anders als § 6a ATDG enthält § 23 Abs. 6 PolG NRW n.F. keinerlei **Konkretisierung**, was unter der Zusammenführung, dem Abgleich sowie der Aufbereitung und Analyse von Daten zu verstehen ist. Diese Konkretisierung überlässt die Vorschrift vollumfänglich der Gesetzesbegründung, die die Beschreibung des § 6a Abs. 5 ATDG aufgreift. Ohne Zuhilfenahme der Begründung ist nicht einmal im Ansatz klar, welche Bedeutung der Vorschrift zukommt. Dass es dabei auch um den Einsatz von auf „Palantir Gotham“ basierender Software gehen soll oder kann, erschließt sich nicht.

47 Zudem verstößt § 23 Abs. 6 PolG NRW n.F. gegen das Gebot der Normenklarheit. Dieses erfordert unter anderem, dass keine langen und intransparenten **Verweisungsketten** vorliegen.[36]

48 So geht aus § 23 Abs. 6 PolG NRW n.F. bereits nicht hinreichend hervor, ob auf die jeweils aktuelle Fassung von § 100a Abs. 2 StPO Bezug genommen wird – eine Vorschrift, die regelmäßig verändert wird – oder eine spezifische Fassung als Anknüpfungspunkt festgelegt sein soll. Darüber hinaus handelt es sich um eine Vorschrift des Bundesgesetzgebers. Der Landtag Nordrhein-Westfalen kann damit nicht beeinflussen, ob und wann § 100a Abs. 2 StPO geändert wird. Zudem

---

34 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 88.
35 BVerfG, Urteil vom 12. April 2005 – 2 BvR 581/01 – *Global Positioning System*, Rn. 51.
36 BVerfG, Beschluss vom 3. März 2004 – 1 BvF 3/92 – *Zollkriminalamt*, Rn. 57, 62 f.; BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 – *BND - Ausland-Ausland-Fernmeldeaufklärung*, Rn. 215.

liegt der landesgesetzgeberischen Abwägung die derzeitige Fassung von § 100a Abs. 2 StPO zugrunde. Sofern eine flexible Verweisung vorliegen soll – was bei der derzeitigen Formulierung naheliegt – führt eine Änderung von § 100a Abs. 2 StPO dazu, dass nunmehr auch Maßnahmen aus Gründen möglich sind, die der Landesgesetzgeber nicht in die notwendige Abwägung miteinbezogen hatte.

49 Darüber hinaus ist aufgrund der Verweisungstechnik kaum ersichtlich, wie umfangreich der Anwendungsbereich tatsächlich ist. So verweist § 23 Abs. 6 Satz 2 Nr. 1 PolG NRW n.F. auf § 100a Abs. 2 StPO, dieser dann unter anderem auf § 89c StGB (§ 100a Abs. 2 Nr. 1 lit. a StPO), dieser dann unter anderem auf § 51 Abs. 1 bis 3 des Waffengesetzes (§ 89c Abs. 1 Nr. 6 StGB). Somit besteht in diesem Beispiel eine Verweisungskette mit vier Gliedern in vier verschiedenen Gesetzen. Dies überschreitet die Grenzen der Normenklarheit.[37]

50 Hinzu kommt, dass § 23 Abs. 6 PolG NRW n.F. – der in seiner Eingriffsintensität die restlichen Ermächtigungen des § 23 PolG NRW n.F. übertrifft – in Absatz 6 dieser Norm **„**versteckt**“** ist. Dies spiegelt die Bedeutung der Vorschrift nicht wider.

II. ALLGEMEINE ANFORDERUNGEN AN INTENSIVE GRUNDRECHTSEINGRIFFE NICHT ERFÜLLT

51 Auch unabhängig von der konkreten Einstufung als erweiterte Datennutzung bestehen strenge Voraussetzungen an intensive Eingriffe in das Recht auf informationelle Selbstbestimmung Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

1. ERHÖHTE EINGRIFFSINTENSITÄT

52 Die erhöhte Eingriffsintensität des § 23 Abs. 6 PolG NRW n.F. ergibt sich insbesondere aus der Komplexität der Verarbeitung, der Menge und Vielfalt der einbezogenen Daten, dem einbezogenen Personenkreis, der Persönlichkeitsrelevanz der Daten, der Gefahr der Profilbildung, der verdeckten erweiterten Datennutzung, aus der Anreizwirkung zu weiteren Maßnahmen und aus möglichen Folgemaßnahmen.

---

37 Vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 – *BND - Ausland-Ausland-Fernmeldeaufklärung*, Rn. 215.

- Komplexität der Verarbeitung:

  Durch die Nutzung automatisierter, rechnergestützter Operationen zur Verarbeitung nahezu beliebig großer und komplexer Informationsbestände in großer Schnelligkeit können Ermittlungstätigkeiten eine bislang unbekannte Durchschlagskraft erlangen. Durch die komplexen softwarebasierten Verarbeitungs- und Verknüpfungsmöglichkeiten gewinnen zuvor möglicherweise belanglose Informationen einen neuen Gehalt.[38]

- Menge und Vielfalt der einbezogenen Daten:

  Die Intensität des Eingriffs ergibt sich zudem aus der Menge und Vielfalt der in den Abgleich einbezogenen personenbezogenen Daten. Diese erlangen durch die Verarbeitung und Verknüpfung einen neuen Stellenwert.[39] Es bestehen weitgehende Möglichkeiten der Polizei, Daten zunächst aus verschiedenen Quellen zu erheben und in Dateisystemen zu speichern, um sie im nächsten Schritt auszuwerten. Dies betrifft private und behördliche Datenbestände ebenso wie Daten aus öffentlichen Quellen (siehe bereits **I.1**).

- Einbezogener Personenkreis:

  Zudem wirkt sich eingriffsintensivierend aus, dass eine große Menge an Menschen betroffen ist, die für den Eingriff keinen Anlass gegeben haben.[40] Maßnahmen, bei denen zahlreiche Personen in den Wirkungsbereich einbezogen werden, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich von hoher Eingriffsintensität.[41] Das aus § 23 Abs. 6 Satz 2 Nr. 1 PolG NRW n.F. und der Gesetzesbegründung ablesbare Ziel der Befugnis „zur vorbeugenden Bekämpfung von Straftaten Beziehungen oder Zusammenhänge zwischen Personen herzustellen“, legt es gerade

---

38 BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – *Rasterfahndung II*, Rn. 104 ff.; BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 109 ff.

39 BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – *Rasterfahndung II*, Rn. 102 ff.

40 BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – *Rasterfahndung II*, Rn. 116 ff.

41 BVerfG, Beschluss vom 14. Juli 1999 – 1 BvR 2226/94, 2420/95, 2437/95 – *Telekommunikationsüberwachung I*, Rn. 219, 270; BVerfG, Urteil vom 11. März 2008 – 1 BvR 2074/05, 1254/07 –*Automatisierte Kennzeichenerfassung*, Rn. 78; BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15 – *Kfz-Kennzeichenkontrollen 2*, Rn. 98.

nahe, dass Personen mit in die Maßnahme einbezogen werden sollen, die hierfür keinen eigenen Anlass gegeben haben.[42]

- Persönlichkeitsrelevanz der Daten:

  Das Gewicht des Eingriffs durch den Abgleich und die Analyse verstärkt sich, wenn die einbezogenen Daten eine besondere Persönlichkeitsrelevanz aufweisen, für sich und in Verknüpfung mit anderen Daten. Besonders hoch ist die Eingriffsintensität, „wenn Informationen betroffen sind, bei deren Erlangung Vertraulichkeitserwartungen verletzt werden, vor allem solche, die unter besonderem Grundrechtsschutz stehen, wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG“.[43] In den Polizeidatenbanken, die in Analysen nach § 23 Abs. 6 PolG NRW n.F. einfließen, können sich besonders persönlichkeitsrelevante Daten befinden. Dies betrifft etwa Informationen über politische Meinungen oder religiöse Überzeugungen. Dazu ist es möglich, dass die Polizei (Meta-) Daten aus Maßnahmen wie der Wohnraumüberwachung und der Telekommunikationsüberwachung in Dateien speichert und in die Analyse mit einbezieht.

- Gefahr der Profilbildung:

  Die Eingriffsintensität erhöht sich zudem durch die Gefahr einer Profilbildung von den Betroffenen durch die automatisierte Zusammenführung und der anschließenden Analyse der personenbezogenen Daten. Dies ist eine Annäherung an die verfassungsrechtlich verbotene Erstellung umfassender Persönlichkeitsprofile.[44] So können die Inhalte polizeilicher Datenbanken über die Erhebung und Speicherung von Informationen aus sozialen Medien und anderen öffentlichen und nicht-öffentlichen Quellen angereichert werden

---

42 Das Innenministerium des Landes Nordrhein-Westfalen erläutert selbst, dass auch sogenannte Nichtstörer*innen von der erweiterten Datennutzung erfasst werden: § 25 Abs. 1 Satz 2 PolG NRW (welcher ausdrücklich in § 23 Abs. 6 Satz 2 PolG NRW n.F. genannt wird) lasse einen Abgleich von Daten jedenfalls mit eigenen polizeilichen Dateien zu, wenn dieser im Einzelfall zur Aufgabenerfüllung erforderlich ist. Auf das Feststehen der Störereigenschaft der Personen, deren Daten abgeglichen werden, komme es hierfür also gerade nicht an. Schreiben des Innenministeriums Nordrhein-Westfalen vom 7. Mai 2021, Vorlage 17/5418, S. 4 - 5.

43 BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – *Rasterfahndung II*, Rn. 98.

44 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 – *BKAG*, Rn. 130.

und damit einen weitreichenden Einblick in das Leben, die Beziehungen und Netzwerke betroffener Personen gewähren (siehe hierzu bereits unter **I.1**).

- Verdeckte erweiterte Datennutzung:

  Zudem erfolgt das gesamte Vorgehen heimlich. Die Betroffenen werden weder über das nach § 23 Abs. 6 PolG NRW n.F. mögliche automatisierte Zusammenführen noch über den anschließenden Abgleich, die Aufbereitung oder die Analyse ihrer personenbezogenen Daten von der Polizei informiert. Diese verdeckte erweiterte Datennutzung schränkt Rechtsschutzmöglichkeiten in erheblichem Maße ein und steigert zusätzlich die Eingriffsintensität.[45]

- Anreizwirkung:

  Zudem schafft die Möglichkeit, verschiedene Datensätze vereinfacht miteinander zu verknüpfen, einen Anreiz zur Generierung weiterer Grunddaten durch vermehrte und intensivierte Ermittlungsmaßnahmen.

- Mögliche Folgemaßnahmen:

  Schließlich ergibt sich die hohe Intensität des Eingriffs aus dem Risiko für Betroffene, Gegenstand weiterer staatlicher Maßnahmen zu werden im Anschluss an die Analyse nach § 23 Abs. 6 PolG NRW n.F. Es erscheint möglich, dass wenn sich aus einer mit Hilfe der Datenanalyse generierten Hypothese ein Ermittlungsansatz ergibt, dies zu weiteren Ermittlungsmaßnahmen führen kann, sei es offenen Charakters wie Befragungen oder verdeckten Charakters wie Observationen oder Telekommunikationsüberwachung. Die Einbeziehung in die Datenanalyse kann aus diesem Grund eine **stigmatisierende Wirkung** auf die Betroffenen haben. Dies gilt nicht nur, wenn dieser Umstand öffentlich bekannt wird. Auch dass eine Person durch diese Einbeziehung stärker ins Visier von polizeilichen Ermittlungen gerät, kann ihre Identität im Sinne einer Stigmatisierung beschädigen, da sie sich in der Folge möglicherweise vermehrt Kontrollen und Folgeermittlungen ausgesetzt sieht.

---

45 BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06 – *Beschlagnahme von Emails*, Rn. 68.

Ein Beispiel für einen möglichen Anwendungsbereich des § 23 Abs. 6 PolG NRW n.F., der zu Folgemaßnahmen führen kann, zeigt ein Projekt zur Früherkennung und zum Umgang mit Personen mit „Risikopotenzial“, bei dem es aufgrund von erstellten Persönlichkeitsprofilen bereits zur Anordnung von Untersuchungshaft, der Unterbringung in einer psychiatrischen Klinik und einer erstmaligen oder erneut angepassten Medikation kam.[46]

2. VORAUSSETZUNGEN WERDEN NICHT ERFÜLLT

53 Dementsprechend bestehen auch unabhängig von der Einordnung als erweiterte Datennutzung erhöhte Anforderungen an § 23 Abs. 6 PolG NRW n.F.

54 Erforderlich sind demensprechend:

1) Die Beschränkung des Einsatzes auf den Schutz von Gütern von überragender Bedeutung.[47]

2) Das Erfordernis einer hinreichenden Eingriffsschwelle in Form einer konkreten Gefahr.[48]

---

46 Das **Projekt „PeRiskoP“** (Handlungs- und Prüffallkonzept zur Früherkennung von und zum Umgang mit Personen mit Risikopotenzial) des Landeskriminalamtes Nordrhein-Westfalen. Im Rahmen dieses noch laufenden Pilotprojekts werden Prüffälle anhand von (teil-)automatisierten Analyseverfahren der polizeiinternen Datenbanken und in Kooperation mit anderen Behörden und Institutionen generiert. Die geheime Datenverarbeitung wird zur Erstellung eines umfassenden Persönlichkeitsprofils genutzt, um eine niedrigschwellige Früherkennung von Risikopersonen zu ermöglichen. Innenministerium Nordrhein-Westfalen, Abschlussbericht Projekt „PeRiskoP“ vom 31. Januar 2022, Vorlage 17/6371.

47 BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 – *Antiterrordateigesetz II*, Rn. 116; BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 – *BKAG*, Rn. 212; BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – *Rasterfahndung II*, Rn. 138.

48 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, 595/07 – *Online-Durchsuchungen*, Rn. 249 ff.; BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, 263/08, 586/08 – *Vorratsdatenspeicherung*, Rn. 231 ff.; BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – *Rasterfahndung II*, Rn. 138; BVerfG, Beschluss vom 14. Juli 1999 – 1 BvR 2226/94, 2420/95, 2437/95 – *Telekommunikationsüberwachung I*, Rn. 240 ff.; BVerfG, Urteil vom 3. März 2004 – 1 BvR 2378/98, 1084/99 – *Großer Lauschangriff*, Rn. 245 ff.

3) Verfahrensrechtliche Absicherungen.[49]

4) Eine hinreichend bestimmte und normenklare Regelung.[50]

55 Diese Voraussetzungen sind allesamt nicht erfüllt (siehe **I.2**).

III. FEHLENDE VORKEHRUNGEN ZUR DATENSICHERHEIT UND ZUM DATENSCHUTZ

56 Schließlich ist noch darauf hinzuweisen, dass die Verwendung von Software, die auf „Palantir Gotham“ basiert – oder vergleichbarer von Dritten erstellte oder betriebene Software – nicht nur zu dem dargestellten intensiven Grundrechtseingriff führt, sondern insbesondere auch das Risiko besteht, dass die Daten an Dritte gelangen können.[51] Dass es dazu kommt, wird zwar bereits von anderen nationalen und europäischen Bestimmungen untersagt. Das Gesetzgebungsverfahren zum Erlass einer Ermächtigungsgrundlage zum Einsatz derartiger Software sollte aber einen Anlass bieten, sich dieser Anforderungen und Gefahren zu vergegenwärtigen und sicherzustellen, dass hinreichende Sicherungsmaßnahmen auch praktisch getroffen werden. Eine Auseinandersetzung mit diesen erweiterten Risiken fehlt jedoch in dem Gesetzesentwurf.

Charlotte Baldauf Jürgen Bering

---

49 BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/17 – *Antiterrordateigesetz I*, Rn. 205 ff.; BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 – *BND – Ausland-Ausland-Fernmeldeaufklärung*, Rn. 265 ff.

50 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/90, 1140/09 – *BKAG*, Rn. 94; BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 – *Ausland-Ausland-Fernmeldeaufklärung*, Rn. 137; BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 – *Rasterfahndung II*, Rn. 150.

51 Vgl. bspw. *Mersi*, Wird Polizei-Hoffnung „VeRa“ zum Datenschutz-Alptraum?, beck-aktuell (28. Mai 2021).