Ausarbeitung

Datenbank-Analysen durch die Polizei

Grundrechte und Datenschutzrecht

Datenbank-Analysen durch die Polizei
Grundrechte und Datenschutzrecht

Aktenzeichen: WD 3 - 3000 - 018/20
Abschluss der Arbeit: 2. März 2020
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Fragestellung

Die Ausarbeitung befasst sich mit der Bedeutung der Grundrechte im Bereich der polizeilichen Auswertung verschiedener Datenbanken und Quellen und den Anforderungen des Datenschutzrechts an diese. Für diese Datenanalysen kann unterschiedliche Software genutzt werden, die zum Teil die Informationen verschiedener Datenbanken miteinander verknüpft auswerten kann. Im Fokus steht eine Software, die neben polizeiinternen Quellen auch auf externe Quellen (insbesondere Facebook) zurückgreifen kann. Dies wirft datenschutzrechtliche und verfassungsrechtliche Fragestellungen auf. Die Ausarbeitung prüft zunächst die Analyse bestehender polizeilicher Daten und geht sodann auf die Einbeziehung externer Quellen in die Datenanalyse ein (8. und 9.). Unterstellt wird dabei, dass es sich bei den bereits gespeicherten Daten um solche handelt, die rechtmäßig erlangt wurden.[1]

2. Einführung

Das Bundesland Hessen hat 2017 eine Software von der US-Firma **Palantir** erworben, die nach Anpassungen unter dem Namen **„Hessendata“** bekannt wurde. Diese Software ermöglicht es, drei unterschiedliche polizeiinterne Datenbanken und Facebook zeitgleich nach bestimmten Informationen oder Beziehungen zu durchsuchen. Auch Europol nutzt nach Angaben der Bundesregierung eine Software von Palantir zur Analyse und Auswertung von Daten, insbesondere für die Erstellung sogenannter Cross-Match-Berichte (Kreuztreffer). Die Funktionen des Produkts umfassen „die Anwendung von Methoden und Algorithmen zur automatischen Extraktion von Zusammenhängen zwischen Erkenntnissen der Mitgliedstaaten und den bei Europol vorliegenden Informationen.“[2] Darüber hinaus bestehen erste weitere Ansätze zur Massendatenauswertung bei Europol.[3] Zudem plant das Land Nordrhein-Westfalen den Einsatz einer ähnlichen Software von Palantir ab Herbst 2020.[4] Auf der Bundesebene gab es nach Angaben der Bundesregierung im August 2018 keine

---

1 Vgl. auch: BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 8; Gesetzesbegründung zu § 25a HSOG: Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen, Drucksache 19/5412, Hessischer Landtag, LT-Drs. 19/6502, S. 41.

2 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Inge Höger, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/13194, Techniken zur Internetermittlung bei der Polizeiagentur Europol, BT-Drs. 18/13310, Antwort auf Frage 8; Vgl. ebenso: Antwort des Parlamentarischen Staatssekretärs Dr. Peter Tauber vom 26. April 2018 auf Anfrage des Abgeordneten Omid Nouripour (BÜNDNIS 90/DIE GRÜNEN), Frage 77 der Schriftlichen Fragen mit den in der Woche vom 30. April 2018 eingegangenen Antworten der Bundesregierung, BT-Drs. 19/1979.

3 Vgl. dazu Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/9318, Neue Verfahren zur Massendatenauswertung bei Europol („Big Data“), BT-Drs. 19/9701. Europol will bezüglich des Datenbankabgleichs zur Gesichtserkennung nach eigenen Angaben eine IT-Lösung inhouse entwickeln; vgl. dazu: http://www.europarl.europa.eu/doceo/document/E-8-2018-002894-ASW_EN.pdf (zuletzt aufgerufen am 25.2.2020); Auch: Ergänzender Bericht der Fraktion DIE LINKE, Hessischer Landtag, Zwischenbericht Teil B des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 6.

4 „Automatisch verdächtig: Polizei setzt zunehmend auf umstrittene US-Software“, Frankfurter Rundschau vom 24.1.2020, https://www.fr.de/politik/hessen-umstrittene-polizei-software-palantir-automatisch-verdaechtig-13454012.html (zuletzt aufgerufen am 27.2.2020).

Geschäftsbeziehungen oder Planungen, mit Palantir im Bereich Software-Entwicklung für Ermittlungen im Bereich islamistischer Terrorismus oder organisierte Kriminalität zusammenzuarbeiten.[5]

3. Anforderungen des Datenschutzrechts an die Kreuzsuche

Die Analyse der Datenbanken wirft datenschutzrechtliche Fragen auf. Unter der hier relevanten Kreuzsuche wird die Möglichkeit verstanden, getrennte polizeiliche Datenbanken miteinander in Beziehung zu setzen und so gemeinsam zu analysieren und auszuwerten.

Für den Schutz personenbezogener Daten gilt bei polizeilicher Ermittlungs- oder Gefahrenabwehrarbeit ein besonderer Rechtsrahmen. Die Datenschutzgrundverordnung (DSGVO) findet gemäß Art. 2 Abs. 2 lit. d) keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Diese unterliegt dem speziellen europäischen Regelwerk, der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2000/383/JI des Rates (**JI-Richtlinie**). Die Richtlinie wurde allgemein in den §§ 45 bis 84 **Bundesdatenschutzgesetz** (BDSG) umgesetzt. Jedoch gehen diesen allgemeinen Regelungen bereichsspezifische Datenschutzregelungen der Fachgesetze vor, § 1 Abs. 2 S. 1 BDSG. Fachgesetzlich geregelt wurde der spezielle Datenschutz zunächst im Bundeskriminalamtsgesetz und Ende 2019 auch in der **Strafprozessordnung** (StPO). Die Ausarbeitung wird hier im Wesentlichen auf die Vorschriften aus dem BDSG und der StPO beschränkt.

Zunächst legt § 500 StPO die entsprechende Geltung der §§ 45 bis 84 BDSG fest, soweit in der StPO nichts Spezielleres geregelt ist. Das BDSG regelt in § 47 die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten. Danach müssen personenbezogene Daten:

> „1. auf **rechtmäßige Weise** und nach **Treu und Glauben** verarbeitet werden,
>
> 2. für **festgelegte, eindeutige** und **rechtmäßige Zwecke** erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
>
> 3. dem **Verarbeitungszweck entsprechen**, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen,
>
> 4. **sachlich richtig** und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

5 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Irene Mihalic, Dr. Konstantin von Notz, Stefan Schmidt, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/3707, Situation und Planungen der Bundespolizei 2018, BT-Drs. 19/3932, Antworten auf Frage 40 und 41.

> 5. nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und
>
> 6. in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der **personenbezogenen Daten gewährleistet**; hierzu gehört auch ein durch geeignete **technische und organisatorische Maßnahmen** zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung."[6]

Darüber hinaus werden weitere Anforderungen an die Verarbeitung **besonderer Kategorien personenbezogener Daten** nach § 48 BDSG gestellt. Diese besonderen Kategorien personenbezogener Daten umfassen nach § 46 Nr. 14 BDSG Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen; genetische Daten; biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person; Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung. Die Verarbeitung dieser Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist. Für die Verarbeitung sind **geeignete Garantien**[7] für den Schutz der Rechtsgüter der betroffenen Personen vorzusehen.

Aus den **speziellen Regelungen** soll hier insbesondere hingewiesen werden auf § 161 Abs. 3 StPO und § 479 Abs. 2 S. 1 StPO. § 161 Abs. 3 StPO besagt: „Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer entsprechenden Maßnahme nach anderen Gesetzen **erlangten personenbezogenen Daten ohne Einwilligung** der von der Maßnahme betroffenen Personen zu Beweiszwecken im Strafverfahren nur zur **Aufklärung solcher Straftaten verwendet** werden, zu deren Aufklärung eine solche **Maßnahme** nach diesem Gesetz **hätte angeordnet werden dürfen**."[8] § 479 Abs. 2 S. 1 StPO verweist für die Datenverwendung noch einmal explizit auf diese Regelung. Darüber hinaus regelt § 479 Abs. 2 S. 2 und Abs. 3 StPO, dass die Verwendung personenbezogener Daten ohne Einwilligung der betroffenen Person nur zu bestimmten Zecken zulässig ist, nämlich:

> 1. zu Zwecken der **Gefahrenabwehr**, soweit sie dafür durch eine entsprechende Maßnahme nach den für die zuständige Stelle geltenden Gesetzen erhoben werden könnten,
>
> 2. zur **Abwehr einer Gefahr** für **Leib**, **Leben** oder **Freiheit** einer Person oder für die **Sicherheit** oder den **Bestand des Bundes** oder eines **Landes** oder für **bedeutende Vermögenswerte**, wenn sich aus den Daten im Einzelfall jeweils konkrete Ansätze zur Abwehr einer solchen Gefahr erkennen lassen,
>
> 3. zur zulässigen Übermittlung von Informationen an die **Verfassungsschutzbehörden** nach § 18 des Bundesverfassungsschutzgesetzes oder

---

6 Hervorhebung nur hier.

7 Mehrere mögliche geeignete Garantien sind in § 48 Abs. 2 S. 2 BDSG exemplarisch aufgeführt.

8 Hervorhebung nur hier.

4. für Auskünfte und Akteneinsicht zu **Forschungszwecken** nach Maßgabe des § 476 StPO.

Daten, die durch **akustische Wohnraumüberwachung** (§ 101c StPO), **Online-Durchsuchung** (§ 101b) oder **Erhebung von Verkehrsdaten** (§ 101g StPO) erhoben wurden, dürfen nach § 479 Abs. 3 StPO zudem in bestimmten weiteren Gefahrensituationen verwendet werden. Diese aufgezeigten Anforderungen der Verwendung der unterschiedlichen Datenarten macht deutlich, dass es stets auf eine **Prüfung des Einzelfalls** ankommt, inwieweit Daten verwendet werden dürfen.

§ 481 Abs. 1 S. 1 StPO stellt darüber hinaus auch klar, dass die Befugnis der Polizei zur Verwendung von personenbezogenen Daten auch aus den **Polizeigesetzen** folgen kann. Insoweit ist besonders auf den im Juli 2018 eingefügten § 25a Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) zur automatisierten Anwendung zur Datenanalyse hinzuweisen. Die Norm wurde im Zuge der Installation der Software „Hessendata“ in das HSOG eingefügt und stellt nach der Überzeugung des Hessischen Landesdatenschutzbeauftragten die notwendige und erforderliche Grundlage für die Verarbeitung personenbezogener Daten dar.[9] Sie regelt:

> „(1) Die Polizeibehörden können in **begründeten Einzelfällen gespeicherte personenbezogene Daten** mittels einer **automatisierten Anwendung zur Datenanalyse** weiterverarbeiten zur vorbeugenden **Bekämpfung** von in § 100a Abs. 2 der Strafprozessordnung genannten **Straftaten** oder zur **Abwehr einer Gefahr** für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind.
>
> (2) Im Rahmen der Weiterverarbeitung nach Abs. 1 können insbesondere **Beziehungen** oder **Zusammenhänge** zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.
>
> (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.“[10]

---

9 Hessischer Landtag, Zwischenbericht Teil A des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 65 und Abweichender Bericht der Fraktion SPD, Hessischer Landtag, Zwischenbericht Teil B des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 7.

10 Hervorhebung nur hier. Zu der Norm im Einzelnen: BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 1 ff.

Die bekannte Software „Hessendata“ greift zunächst auf eigene Datenbanken der hessischen Polizei[11] und eventuell auf externe, frei zugängliche Quellen zu. Für den automatisierten Abruf von Daten anderer Strafverfolgungsbehörden böte § 488 StPO eine Rechtsgrundlage. § 25a HSOG bildet somit eine Rechtsgrundlage für das automatisierte systematische Analysieren und Auswerten von Daten, die an sich in getrennten Datenbanken gelagert sind. Ob § 25a HSOG alle verfassungsrechtlichen und datenschutzrechtlichen Anforderungen an eine Befugnisnorm erfüllt, ist nach der derzeitigen Literatur unklar.[12] Es besteht jedoch mindestens bei Aufnahme der dort genannten Kritikpunkte die Möglichkeit, eine **verfassungskonforme Grundlage** für die Kreuzsuche auf Bundesebene zu schaffen. Dann würde auch den Bedenken der Datenschutzbeauftragten des Bundes und der Länder Rechnung getragen, die den Einsatz solcher Datenanalysesysteme durch die Polizei nur in **engen Grenzen** als verfassungsrechtlich zulässig betrachten.[13]

Datenschutzrechtlichen Bedenken hinsichtlich der Möglichkeit des **Abfließens** von personenbezogenen Daten in die USA wurde in Hessen damit begegnet, dass die Software allein auf landeseigenen Rechnern in speziell gesicherten Räumlichkeiten installiert wurde. Sie kann auch nur innerhalb dieser Räume gewartet und verändert werden, stets unter Begleitung von Landesbediensteten. Ein versteckter automatischer Datenabfluss wird auch dadurch verhindert, dass die Rechner keine Verbindung zum Internet haben.[14] Vergleichbare Vorsichtsmaßnahmen werden auch durch die Bundesregierung als Standard bei den Sicherheitsbehörden geschildert.[15] **Offen bleibt** bei diesen Darstellungen aus laienhafter Sicht jedoch, wie insofern die Einspeisung neuer Daten insbesondere bei der Durchsuchung externer Quellen wie sozialen Netzwerken erfolgt und wie die Software durch die einzelnen Ermittlungseinheiten dann technisch nutzbar ist, wenn sie nicht über das Internet kommuniziert.[16] Gegebenenfalls ist diese Kommunikation aber auch sicher über das besonders geschützte Netz der Polizei möglich.[17] Diesbezüglich ist auch zu fragen, wie die

---

11 Hessischer Landtag, Zwischenbericht Teil A des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 18 f.

12 BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 28 ff.

13 Schaffland/Wiltfang in: dies. (Hrsg.), Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten vom 18. und 19. März 2015, juris.

14 Vgl. zu alledem: Hessischer Landtag, Zwischenbericht Teil A des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 66, 69 ff.

15 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/5560, Nutzung von Software ausländischer Hersteller im Sicherheitsbereich, BT-Drs. 19/5988, S. 9 und 10.

16 Vgl. dazu Hessischer Landtag, Zwischenbericht Teil A des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 19 und Ergänzender Bericht der Fraktion DIE LINKE, Hessischer Landtag, Zwischenbericht Teil B des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 7. Vgl. auch: https://netzpolitik.org/2019/hinweise-zu-bestimmten-milieus-bundeslaender-testen-polizeisoftware-mit-palantir-funktion/ (zuletzt aufgerufen am 26.2.2020).

17 So deutet es Zeuge Kaspar laut Untersuchungsausschusszwischenbericht an: Hessischer Landtag, Zwischenbericht Teil A des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 67.

laut Presseberichten bestehende Handy-App „Hessendata mobile“[18] für Polizisten mit dem System kommuniziert.

4. Anforderungen der Grundrechte an die Kreuzsuche

Die verknüpfte Analyse bestehender polizeilicher Datenbanken kann den Schutzbereich mehrerer Grundrechte berühren. Beachtlich für all diese Grundrechte ist, dass die Daten, die analysiert werden, bereits in Datenbanken gespeichert sind und somit der Eingriff in das Grundrecht bei der Datenerhebung bereits stattgefunden hat. Jedoch ermöglicht die spätere Datenanalyse die Nutzung der Daten losgelöst von dem konkreten Anlass, der zum Zeitpunkt der Erhebung die Rechtfertigung bot. Insofern bedarf es einer **neuen Rechtfertigung** des separaten Eingriffs der Datenanalyse und auch einer **eigenen Rechtsgrundlage** als Eingriffsermächtigung.[19] Da die Daten durch die Analyse für einen **neuen Zweck** genutzt werden sollen, erfolgt auch ein **neuer Eingriff** in die **Grundrechte**, in die schon durch die Erhebung der Daten eingegriffen wurde.[20]

Mangels eines konkreten Gesetzesvorschlags zur automatisierten Datenanalyse und einer konkreten Fallkonstellation kann keine detaillierte Grundrechtsprüfung einschließlich der Prüfung einer möglichen verfassungsrechtlichen Rechtfertigung vorgenommen werden. Vielmehr können nur Hinweise bezüglich einschlägiger Grundrechte und möglicher verfassungsrechtlicher Probleme aufgezeigt werden.

4.1. Recht auf informationelle Selbstbestimmung

Das Recht auf **informationelle Selbstbestimmung** wurde vom Bundesverfassungsgericht (BVerfG) aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG abgeleitet.[21] Es schützt die **persönlichen Daten** und den Grundsatz, dass jede Person selbst über die **Preisgabe und Verwendung** dieser entscheiden können soll.[22] Es umfasst auch das Recht am eigenen Bild und Wort sowie der Selbstdarstellung.[23] Das

---

18 „Analysesoftware ‚Hessendata‘ gibt es jetzt auch mobil“, Heise online vom 9.8.2019, https://www.heise.de/newsticker/meldung/Analysesoftware-Hessendata-gibt-es-jetzt-auch-mobil-4493288.html (zuletzt aufgerufen am 26.2.2020).

19 BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781, 1800, Rn. 277; BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 14 f.

20 BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781, 1801, Rn. 285; BVerfGE 100, 313, 360 und 391, BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 17 f.; Singelstein, NStZ 2018, 1, 6.

21 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1, 2. Leitsatz.

22 BVerfG, Urt. v. 19.4.2016 – 1 BvR 3309/13, NJW 2016, 1939, 1942; Lachenmann, DÖV 2016, 501, 502; Singelstein, NStZ 2018, 1, 6.

23 Di Fabio, in: Maunz/Dürig (Hrsg.), 88. EL August 2019, GG Art. 2 Abs. 1 Rn. 173; Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, S. 105.

Recht auf informationelle Selbstbestimmung stellt einen Abwehranspruch des Bürgers gegen die Ausforschung durch den Staat dar.[24]

Durch den Datenabruf und die mögliche Inbeziehungsetzung mit anderen Daten von anderen Personen kann bereits durch die erneute Verwendung der gespeicherten Daten ein **Eingriff** in das Recht auf informationelle Selbstbestimmung vorliegen.

Fraglich scheint, ob der Eingriff insoweit nicht nur durch den erneuten Datenabruf wiederholt wird, sondern auch dadurch, dass dies automatisiert passiert, vertieft wird. Nach einer Ansicht sei zu beachten, dass das Vernetzen der vorhandenen Datenbestände und deren systematische Erschließung durch logarithmische Suchfunktionen darauf ziele, Erkenntnisse zu gewinnen, die ohne dieses Instrument aus den Daten nicht hätten gewonnen werden können. Es würden so Daten auf einem neuen **Intensitätsniveau** erschlossen, die dem Anlegen von Profilen sehr nahe komme.[25] Dem entgegen steht jedoch, dass die Analyse der bestehenden Daten auch durch den Einsatz von viel gut geschultem Personal möglich wäre, dementsprechend das automatisierte Vorgehen die Analyse nur wesentlich beschleunigt und effektiviert.

Die im Rahmen des Grundrechts auf informationelle Selbstbestimmung bestehende Problematik der eventuell unzulässigen **Profilbildung** stellt sich bei einem reinen Zugriff auf polizeiinterne Datenbanken bislang nicht. Zum einen führen auch diese Datenbanken und Akten bereits in der Vergangenheit zu einer gebündelten Informationsspeicherung von bestimmten Personen. Zum anderen hat die Rechtsprechung des BVerfG und das Datenschutzrecht dieser bislang nur für den Fall der Profilbildung unter Nutzung öffentlich zugänglicher Daten Grenzen gesetzt.[26]

Problematisch scheint darüber hinaus auch, dass zumindest bei der bisher bekannten Software „Hessendata“ keine **Differenzierungen** vorgenommen werden betreffs der betroffenen Dateneigner. Daten von Verurteilten, Tatverdächtigen oder Beschuldigten auf der einen Seite und **Zeugen**, Hinweisgebern, Anzeigenden, Geschädigten, **Opfern** und unbeteiligten Dritten (deren Daten beispielsweise im Rahmen einer Überwachungsmaßnahme mit erfasst wurden) auf der anderen Seite werden gemeinsam verarbeitet. Letztere gelten grundsätzlich als **Nichtstörer** im Sinne des Gefahrenabwehrrechts und sind auch **nicht Tatverdächtige** im Rahmen der Strafverfolgung.[27] Auch für diese läge bei der automatischen Datenanalyse ein Eingriff in deren Grundrechte vor, der insofern mangels des Anknüpfungspunkts in der Verantwortlichkeit oder dem Verdacht einer Straftat erheblich schwerer zu rechtfertigen ist.[28] Ein alleiniger Verweis darauf, dass nach § 25 Abs. 2 HSOG „**unbedeutende Informationen** und Erkenntnisse ausgeschlossen“ werden können, verhindert einen

---

24 Lachenmann, DÖV 2016, 501, 502.

25 BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 22.

26 Vgl. dazu BVerfG Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 344 f.; Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, S. 105 ff.; Martini, VerwArchiv 2016, 307, 345, sowie in dieser Ausarbeitung unten Punkt 8.

27 BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 24.

28 Singelstein, NStZ 2018, 1, 6 m.w.N.

Eingriff nicht, zumal die Bewertung einer Information als „unbedeutend“ erst erfolgen kann, wenn sie einer entsprechenden Analyse unterzogen wurde.

4.2. Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

Das Recht auf **Vertraulichkeit und Integrität informationstechnischer Systeme** wurde vom BVerfG ebenfalls aus Art. 2 Abs. 1 iVm Art. 1 GG entwickelt.[29] Danach werden staatliche Zugriffe auf informationstechnische Systeme als besonders intensive Grundrechtseingriffe betrachtet, deren Rechtfertigung nur unter Einhaltung strenger Anforderungen des Verhältnismäßigkeitsgrundsatzes möglich ist. Es bedarf dazu einer richterlichen Anordnung und tatsächlicher Anhaltspunkte für eine Gefahr für ein überragend wichtiges Rechtsgut. Auch sind Vorkehrungen zur Vermeidung von Eingriffen in den **absolut geschützten Kernbereich privater Lebensführung** erforderlich.[30] So soll der Schutz des allgemeinen Persönlichkeitsrechts insbesondere vor der Ausspähung persönlicher Lebensbereiche verbessert werden.[31] Dieses Grundrecht ist insbesondere dann relevant, wenn bei der Datenanalyse auch auf solche Daten zurückgegriffen werden soll, die beispielsweise durch eine **Online-Durchsuchung** nach § 101b StPO oder über einen verdeckten Eingriff in informationstechnische Systeme (u.a. § 15c HSOG) in die Datenbanken gelangt sind. Die Rechtfertigung einer solchen erneuten Verwendung der Daten verlangt insoweit wiederum die Einhaltung der genannten ursprünglichen Rechtfertigungsanforderung.

4.3. Brief-, Post- und Fernmeldegeheimnis und Unverletzlichkeit der Wohnung

Das **Brief-, Post- und Fernmeldegeheimnis** (Art. 10 Abs. 1 3. Alt. GG) und die **Unverletzlichkeit der Wohnung** (Art. 13 Abs. 1 GG) können ebenso relevant werden, da die ursprünglich gespeicherten Daten auch aus einer **Telekommunikations-** oder **Wohnraumüberwachung** („großer Lauschangriff“) stammen können. Auch hier ist die Zweckänderung durch die Datenanalyse an den Grundrechten zu messen, die durch die Datenerhebung tangiert wurden.[32] Insoweit ist besonders an den **Schutz des unantastbaren Kernbereichs privater Lebensgestaltung** zu erinnern, der auch bei diesen Grundrechten relevant ist.[33] Dessen Schutz sollte auch im Rahmen der gesetzlichen Eingriffsgrundlage erfasst sein.[34]

---

29 BVerfG Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274.

30 BVerfG Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274; vgl. auch: Britz, DÖV 2008, 411.

31 Lachenmann, DÖV 2016, 501, 502.

32 BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781, 1801, Rn. 285; BVerfGE 100, 313, 360 und 391, BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 17 f.

33 BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781, 1786, Rn. 119 ff.; Durner, in: Maunz/Dürig (Hrsg.), 88. EL August 2019, GG Art. 10 Rn. 42.

34 BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 46.

4.4. Berufsfreiheit

Selbst die in Art. 12 Abs. 1 GG geschützte Berufsfreiheit kann tangiert werden, wenn bei der Analyse Daten genutzt oder hervorgebracht werden, die **Berufsgeheimnisträger** betreffen. Dazu äußerte das BVerfG:

> „Richtet sich eine strafrechtliche Ermittlungsmaßnahme gegen einen Berufsgeheimnisträger in der räumlichen Sphäre seiner Berufsausübung, so bringt dies darüber hinaus regelmäßig die Gefahr mit sich, dass unter dem Schutz des Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG stehende Daten von Nichtbeschuldigten, etwa den Mandanten eines Rechtsanwalts, zur Kenntnis der Ermittlungsbehörden gelangen, die die Betroffenen in der Sphäre des Berufsgeheimnisträgers sicher wähnen durften. Dadurch werden nicht nur die Grundrechte der Mandanten berührt. Bei der Anwendung strafprozessualer Eingriffsermächtigungen ist das Ausmaß der – mittelbaren – Beeinträchtigung der beruflichen Tätigkeit des Rechtsanwalts (Art. 12 Abs. 1 GG) zu berücksichtigen. Der Schutz der Vertrauensbeziehung zwischen Anwalt und Mandant liegt auch im Interesse der Allgemeinheit an einer wirksamen und geordneten Rechtspflege (vgl. BVerfG v. 12. 4. 2005, 2 BvR 1027/02, a.a.O.). Diese Belange verlangen eine besondere Beachtung bei der Prüfung der Angemessenheit der Zwangsmaßnahme.“[35]

Insoweit verlangt die Verfassung auch hier einen besonderen Schutz, der auch in der gesetzlichen Eingriffsgrundlage fixiert sein sollte.[36]

4.5. Allgemeine Überlegungen zur Rechtfertigung

Die Erhebung und Verarbeitung personenbezogener Daten sind nur zulässig, wenn sie einem **überwiegenden Gemeinwohlinteresse** erfolgen und auf einer **Rechtsgrundlage** erfolgen.[37] Weitere spezielle Anforderungen, die hinzutreten können, wurden bereits benannt.

In der Begründung des Gesetzentwurfs zu § 25a HSOG wurden die Ziele der dortigen Datenanalyse wie folgt beschrieben: Diese diene der Überwindung der Trennung unverbundener Dateien und Informationssysteme mit unterschiedlichen Zweckbindungen, Nutzerkreisen, Datenarten und Betroffenenkreisen. Die Trennung der Datenbestände erschwere die umfassende Analyse straf- und gefahrenabwehrrechtlich relevanter Sachverhalte auf gemeinsame Strukturen, Handlungsmuster, Personengruppen und hinsichtlich zeitlicher, sachlicher, organisatorischer, personaler und situativer Zusammenhänge. Durch die gemeinsame Analyse sollen wesentliche Anhaltspunkte für Gefahren und bevorstehende Straftaten gewonnen werden, die sonst wohl unerkannt bleiben. Dies diene der effektiven Bekämpfung von schweren Straftaten. Die polizeiliche Aufgabenerfüllung soll auf diese

---

35 BVerfG, Beschluss vom 18.3.2009 – 2 BvR 1036/08, DStRE 2009, 1344, 1349.

36 BeckOK Polizei- und Ordnungsrecht Hessen, Möstl/Bäuerle, 16. Edition, Stand: 1.1.2020, § 25a HSOG, Rn. 46.

37 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1, 2. Leitsatz; Singelstein, NStZ 2018, 1, 6.

Weise erleichtert und verbessert werden.[38] Diese Begründung ist auch für die Rechtfertigung der mit der automatisierten Datenanalyse verbundenen Grundrechtseingriffe relevant. Insbesondere kann als überwiegender Gemeinwohlbelang die **Gefahrenabwehr** oder **Verhinderung von Straftaten** dienen.

An die Rechtfertigung sind umso höhere Anforderungen zu stellen, je weiter die Informationserhebung und -verarbeitung im Vorfeld der Beeinträchtigung des Rechtsguts liegt.[39] Auch der Grad der Persönlichkeitssensitivität der verarbeiteten Daten kann zu höheren Rechtfertigungsanforderungen führen.[40] Insofern sollte insbesondere der unantastbare Kernbereich privater Lebensgestaltung geschützt werden.

5. Rechtlicher Unterschied der Kreuzsuche und der Ersterhebung der Daten

Jedes Verarbeiten der personenbezogenen Daten ist selbstständig datenschutzrechtlich (§ 45 S. 1 BDSG) und auch verfassungsrechtlich relevant. Dies wird bereits aus der Begriffsdefinition der **Verarbeitung** in § 46 Nr. 2 BDSG deutlich:

> „Verarbeitung“ [bezeichnet] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Die **Ersterhebung** der Daten, wie auch deren spätere **Abfrage** und **Analyse** im Rahmen der Kreuzsuche, sind Verarbeitungen personenbezogener Daten. Sowohl auf der Ebene des Datenschutzrechts als auch auf der des Grundrechtsschutzes müssen also bei der erneuten Verwendung der gespeicherten Daten die **gleichen Anforderungen** an deren **Rechtmäßigkeit** bzw. **Rechtfertigung** (vgl. oben 4.) erfüllt werden, wie dies bereits bei der ersten Erhebung erforderlich war. Das spezifische Datenschutzrecht in § 479 Abs. 2 S. 1 StPO iVm § 161 Abs. 3 StPO konkretisiert diesen Punkt noch weiter und erklärt, dass auch für gespeicherte Daten eine Verarbeitung ohne Einwilligung nur möglich ist, wenn zur Aufklärung der nun im Raum stehenden Straftat eine solche Maßnahme auch durch die handelnde Stelle nach der StPO angeordnet werden könnte. Auch, wenn die Daten zum Beispiel von einer anderen Stelle zu einem anderen Zweck gespeichert wurden, muss es also eine passende **Rechtsgrundlage** für die **hypothetische Datenerhebung** in der StPO geben.

---

38 Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen, Drucksache 19/5412, Hessischer Landtag, LT-Drs. 19/6502, S. 40 f.

39 Singelstein, NStZ 2018, 1, 6.

40 Martini, VerwArchiv 2016, 307, 343.

6. Zweckbindungsgebot

Die Zweckbindung der Datenverarbeitung stellt im allgemeinen Datenschutzrecht einen wichtigen Grundsatz dar, der sich in § 6 Abs. 4 DSGVO widerspiegelt und vom BVerfG als **„Kernelement des verfassungsrechtlichen Datenschutzes“**[41] bezeichnet wurde. Auch § 47 Nr. 2 BDSG nimmt den Grundsatz für den Bereich der polizeilichen Arbeit auf und bestimmt, dass personenbezogene Daten grundsätzlich nur für **festgelegte, eindeutige** und **rechtmäßige Zwecke** erhoben werden können und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden dürfen. Eine weitere Nutzung der erhobenen Daten kommt danach grundsätzlich insofern nur durch dieselbe Behörde zur ursprünglichen Zwecksetzung und im Rahmen derselben Aufgabe zum Schutz des gleichen Rechtsguts in Betracht.[42] Dieser Grundsatz wird durch Art. 4 Abs. 2 und Art. 9 der JI-Richtlinie und den diese umsetzenden § 49 BDSG **durchbrochen**. § 49 BDSG erklärt:

> „Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 45 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 45 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.“

Die in § 45 S. 1 BDSG genannten **zulässigen Zwecke** sind Verhütung, Ermittlung, Aufdeckung, Verfolgung und Ahndung von Straftaten oder Ordnungswidrigkeiten sowie Gefahrenabwehr und Vollstreckung. Der Verantwortliche muss zur Weiterverarbeitung befugt sein, also sein Handeln auf eine Rechtgrundlage stützen können. Insofern stellt § 49 S. 1 BDSG allein keine Befugnisnorm dar, sondern muss entsprechend ergänzt werden.[43] Der bereits genannte § 25a HSOG (siehe oben 3.) könnte insofern auf Landesebene als Befugnisnorm für die Zweckentfremdung dienen.

Die Weiterverarbeitung zu dem Sekundärzweck muss zudem **erforderlich** und **verhältnismäßig** sein. Erforderlich ist sie, wenn die vorgesehene Aufgabe durch die Exekutive nicht ohne die Weiterverarbeitung erfüllt werden kann.[44] Im Rahmen der Verhältnismäßigkeitsprüfung sind die Eingriffsintensität der Datenverarbeitung und die Interessen und Grundrechte der Betroffenen zu berücksichtigen.[45] § 45 S. 2 BDSG ermöglicht darüber hinaus eine Verarbeitung zu Zwecken außerhalb der JI-Richtlinie, soweit eine Rechtsgrundlage dafür gegeben ist. Diese könnte beispielsweise in der DSGVO oder dem BDSG gefunden werden. Grundsätzlich ermöglicht § 49 BDSG also eine Durchbrechung der Zweckbindung, sobald die entsprechenden Voraussetzungen vorliegen.

---

41 BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1801), Rn. 292. Hervorhebung nur hier.

42 Aden/Fährmann, ZRP 2019, 175, 177.

43 Heckmann/Scheurer, in: Gola/Heckmann, 13. Aufl. 2019, BDSG § 49, Rn. 12.

44 Heckmann/Scheurer, in: Gola/Heckmann, 13. Aufl. 2019, BDSG § 49, Rn. 13.

45 BeckOK DatenschutzR/Albers, 30. Ed. 1.11.2019, BDSG § 49, Rn. 17; Heckmann/Scheurer, in: Gola/Heckmann, 13. Aufl. 2019, BDSG § 49, Rn. 14.

Der Zweckbindungsgrundsatz stellt somit keine zwingende Hürde für eine polizeiliche Datenbankanalyse dar.

Ob die Norm des § 49 BDSG selbst mit der **Verfassung vereinbar** ist, ist in der Literatur **umstritten**. Rechtsprechung dazu besteht bislang nicht. Einerseits wird § 49 BDSG für eine nur moderate Lockerung des Zweckbindungsgrundsatzes gehalten,[46] andererseits für zu allgemein und unbestimmt und damit im Widerspruch zur Rechtsprechung des BVerfG.[47] Vermittelnd wird vorgeschlagen, dass mit der Zweckänderungsvorschrift restriktiv umzugehen sei, und die Verarbeitung zu einem anderen Zweck nur bei einem eigenen, hinreichend spezifischen Anlass erfolgen soll.[48]

7. Nutzung bereits erhobener Daten in Bezug auf „Überwachungs-Gesamtrechnung“

Zur sog. „Überwachungs-Gesamtrechnung“ äußerte sich das BVerfG 2010 in einer Entscheidung zur Vorratsdatenspeicherung.

> „Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.“[49]

Dazu merkt Roßnagel an:

> „Daher ist künftig eine doppelte Verhältnismäßigkeitsprüfung notwendig: Zum einen ist auf der Grundlage der Wirkungen eines Überwachungsinstruments dessen verhältnismäßiger Einsatz zu bewerten. Zum anderen ist aber zusätzlich auf der Basis einer Gesamtbetrachtung aller verfügbaren staatlichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbelastungen bürgerlicher Freiheiten zu prüfen. Danach kann der Gesetzgeber Überwachungsmaßnahmen eventuell nur austauschen, aber nicht kombinieren. Wenn er etwa auf die Vorratsdatenspeicherung des TK-Verkehrs setzt, darf er nicht zugleich auf Vorrat Daten über den Straßen- und Luftverkehr und den Energieverbrauch speichern lassen.“[50]

Insofern hat die Nutzung bereits gespeicherter Daten zwei Wirkungen. Zum einen kann sie im Rahmen der „Überwachungs-Gesamtrechnung“ positiv betrachtet werden, da durch die Nutzung bereits polizeilich zulässig erhobener Daten die Erhebung weiterer Daten **vermieden** werden kann und insofern weniger Instrumente der **Datenerhebung** zum Einsatz kommen. Der Einzelne könnte

---

46 Frenzel, in: Paal/Pauly (Hrsg.), 2. Aufl. 2018, BDSG § 49, Rn. 1.

47 Johannes/Weinhold, Das neue Datenschutzrecht bei Polizei und Justiz, § 1, Rn. 150.

48 Heckmann/Scheurer, in: Gola/Heckmann, 13. Aufl. 2019, BDSG § 49, Rn. 8.

49 BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u.a., NJW 2010, 833, 839.

50 Roßnagel, NJW 2010, 1238, 1240.

auf diese Weise vor weiteren Eingriffen durch die Erhebung in seine Grundrechte bewahrt werden. Zum anderen kommt es insbesondere bei einer **zweckentfremdeten Nutzung** der Daten zu einem erneuten und eventuell vertieften Eingriff in die Grundrechte (siehe oben 4.), der seinerseits rechtfertigungsbedürftig ist. Zudem droht bei einer unspezifischen Durchsuchung der gespeicherten Daten die ständige Wiederholung jeweils nuanciert anderer Eingriffe. Insgesamt handelt es sich bei der Datenbankanalyse aber gerade nicht um ein neues Überwachungsinstrument, bei dem Daten an der Quelle erhoben werden, so dass durch die Rechtsprechung des BVerfG hier keine weiteren Anforderungen hinzutreten.

8. Bedeutung der Einbeziehung externer Quellen

Die Erhebung, Speicherung und Verarbeitung **allgemein zugänglicher Daten** durch die Polizei, zum Beispiel durch eine Art Online-Streife in sozialen Netzwerken, stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[51]

Dazu führte das BVerfG aus:

> „Eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat grundsätzlich nicht verwehrt. Dies gilt auch dann, wenn auf diese Weise **im Einzelfall personenbezogene Informationen erhoben** werden können (vgl. etwa T. Böckenförde, Die Ermittlung im Netz, 2003, S. 196 f.; Zöller, GA 2000, S. 563 [569]). Daher liegt **kein Eingriff** in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an **jedermann** oder zumindest an einen **nicht weiter abgegrenzten Personenkreis** richten. So liegt es etwa, wenn die Behörde eine **allgemein zugängliche Webseite** im World Wide Web aufruft, eine jedem Interessierten offen stehende **Mailingliste** abonniert oder einen **offenen Chat** beobachtet.
>
> Ein **Eingriff** in das Recht auf informationelle Selbstbestimmung kann allerdings gegeben sein, wenn **Informationen**, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, **gezielt zusammengetragen, gespeichert** und **gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet** werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt. Hierfür bedarf es einer Ermächtigungsgrundlage.“[52]

Mithin weist schon das BVerfG bereits auf den wichtigen Unterschied hin, dass grundrechtlich das allgemeine Mitlesen öffentlicher Informationen keinen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt. Die **Online-Streife** oder auch gezielte Suche nach öffentlich zugänglichen Informationen ist insoweit unkritisch. Relevant wird jedoch der hier durch einen Softwareeinsatz mögliche gezielte **Verknüpfung** der freizugänglichen Daten untereinander, aber auch mit

---

51 BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 344 f.; Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, S. 105 ff.; Martini, VerwArchiv 2016, 307, 322.

52 BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 344 f. Hervorhebung nur hier.

weiteren polizeilich gespeicherten Daten. Diese bedarf stets einer hinreichend bestimmten gesetzlichen **Eingriffsermächtigung**.[53] Eine solche könnte in den Polizeigesetzen geschaffen werden.

Für die Art der Ermittlungsarbeit (zum Beispiel in sozialen Netzwerken) erklärt das BVerfG darüber hinaus, dass die Anlegung eines privat scheinenden Nutzerprofils in dem Netzwerk, auch unter Nutzung einer Legende, noch keinen Grundrechtseingriff darstellt. Das Recht auf informationelle Selbstbestimmung ist aber dann betroffen, wenn die Polizei unter Ausnutzung dieser Legende und des schutzwürdigen Vertrauens des Betroffenen in die Identität und die Motivation seines Kommunikationspartners persönliche Daten erhebt, die sie ansonsten nicht erhalten würde.[54]

Für die spezifische Nutzung der sozialen Netzwerke ist jedoch relevant, dass es sich bei den genannten verwertbaren Informationen um solche handelt, die öffentlich zugänglich sind. Abgrenzungskriterien für den Kreis der öffentlichen Informationen sind noch nicht eindeutig definiert, sodass verschiedene Literaturmeinungen mitunter eigene, aber auch nicht immer trennscharfe Kriterien heranziehen.[55] Eine mögliche Definition könnte lauten, dass es sich um **öffentlich zugängliche Daten** handelt, wenn diese automatisch und nicht nur nach Freischaltung durch den Informationsbereitstellenden und unter dessen individuellen Bedingungen zugänglich sind.[56] Soziale Netzwerke sind insofern zwar registrierungsbedürftig, gewähren aber zunächst jedem Zutritt, der sich anmeldet. Die Öffentlichkeit kann dort also nur durch **individuelle Einstellungen der Privatsphäre** oder beschränktem Zugang zu bestimmten Gruppen oder Seiten definiert werden.[57] Bei der Bewertung einer Information als öffentlich zugänglich kann darüber hinaus auch einbezogen werden, dass zahlreiche Informationen sozialer Netzwerke auch einsehbar sind, ohne überhaupt das soziale Netzwerk als angemeldeter Nutzer zu betreten. So sind beispielsweise zahlreiche Twitter-Nachrichten oder Facebookprofile und -posts über einfache Googlesuchen auffindbar. Fraglich scheint in Bezug auf das Recht auf informationelle Selbstbestimmung zudem, wie die Einbeziehung von Informationen, die **Dritte** über eine betroffene Person **ohne deren Wissen** in ein soziales Netzwerk gestellt haben, zum Beispiel über ein Gruppenfoto, zu behandeln sind.[58]

---

53 Martini, VerwArchiv 2016, 307, 325, 341.

54 BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, 345; Martini, VerwArchiv 2016, 307, 323.

55 Vgl. dazu u.a. Ihwas, Strafverfolgung in sozialen Netzwerken, 2014, S. 131.

56 Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, 128.

57 Dazu näher: Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, 129 ff.; und ausführlich: Ihwas, Strafverfolgung in sozialen Netzwerken, 2014, S. 117 ff.

58 Vgl. dazu ergänzender Bericht der Fraktion DIE LINKE, Hessischer Landtag, Zwischenbericht Teil B des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864 vom 3.1.2019, S. 3; Martini, VerwArchiv 2016, 307, 322.

Die Analyse der öffentlich zugänglichen Daten in sozialen Netzwerken etc. darf zudem die vom BVerfG erklärte Grenze der totalen Erfassung und Registrierung der Freiheitswahrnehmung der Bürger nicht erreichen.[59]

Das **Grundrecht** auf Gewährleistung der **Vertraulichkeit und Integrität informationstechnischer Systeme** setzt in seinem Schutzbereich voraus, dass die informationstechnischen Systeme dazu geeignet sind, die berechtigte Erwartung in die Vertraulichkeit der darin enthaltenen Daten zu bewirken.[60] Insoweit kommen Daten in einem Netzwerk, die darauf ausgerichtet sind, zumindest von einem bestimmten Personenkreis wahrgenommen zu werden und allgemein öffentlich zugängliche Daten nicht als tauglicher Anknüpfungspunkt für den Schutzbereich in Betracht.[61]

Auf die Frage, ob die **Bundesregierung** die Verbindung verschiedener Polizeidatenbanken mit Verbindungsdaten, Daten aus ausgelesenen Handys Verdächtiger und Fernschreibern sowie mit Daten aus sozialen Medien für mit dem deutschen Recht vereinbar hält, antwortete diese Ende 2018:

> „Ja, sofern die gesetzlichen Voraussetzungen für eine entsprechende Datenerhebung vorliegen, ist auch die Speicherung der Daten solange zulässig, bis Löschfristen greifen oder die Speicherung der Daten nicht mehr erforderlich ist. Die Zulässigkeit der Erhebung und Speicherung korrespondiert mit der Zulässigkeit der Nutzung der Daten zu ihrem bestimmungsgemäßen Erhebungszweck im Rahmen der Strafverfolgung und Gefahrenabwehr.“[62]

9. Rechtliche Hürden für die Nutzung von „open source“-Quellen durch Polizei

Diese Thematik wurde umfassend in einer im Jahr 2018 erschienenen Dissertation unter dem Titel „Soziale Netzwerke und strafprozessuale Ermittlungen“ von Dr. Sebastian Bauer untersucht.[63] Diese kann zur Vertiefung der hier nur zusammenfassend dargestellten rechtlichen Parameter herangezogen werden. Die rechtlichen Voraussetzungen ergeben sich aus der potentiellen Notwendigkeit der verfassungsrechtlichen **Rechtfertigung von Grundrechtseingriffen**, welche einschließlich ihrer Rechtfertigungsanforderungen bereits (oben 4.) skizziert wurden. Hinzu treten die spezifischen Voraussetzungen der möglichen gesetzlichen **Eingriffsbefugnisse**. Als solche kommen sowohl Normen aus dem Bereich der Gefahrenabwehr in Betracht, als auch aus dem Bereich der strafprozessualen Ermittlungsbefugnisse. Sie unterscheiden sich jedoch stark nach dem spezifischen Ziel der Nutzung sozialer Netzwerke durch die Polizei, der Art der Zugangsbeschränkung und der Art der Ermittlungsarbeit. Dabei kommt zum Beispiel den Umständen, ob es sich um eine offene oder eine verdeckte Ermittlung handelt, eine entscheidende Bedeutung zu. Ebenso sind die

---

59 BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u.a., NJW 2010, 833, 839.

60 BVerfG Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274,313.

61 Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, 109.

62 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/5560, Nutzung von Software ausländischer Hersteller im Sicherheitsbereich, BT-Drs. 19/5988, S. 7.

63 Vgl. zudem auch: Ihwas, Strafverfolgung in sozialen Netzwerken, 2014, et al.

Details bezüglich der öffentlichen Zugänglichkeit des jeweiligen Netzwerks in seinen unterschiedlichen Einstellungsvarianten des Schutzes der Privatsphäre von Bedeutung. Eine genaue Ermittlung der rechtlichen Voraussetzungen ist nur für bestimmte Situationen und hier nicht pauschal möglich.[64]

Sofern die Polizei nur im Einzelfall auf **öffentlich zugängliche Quellen** zurückgreift, liegen die Maßnahmen regelmäßig unterhalb der Eingriffsschwelle in die genannten Grundrechte.[65] Wenn die Polizei diese Daten nutzt, kann sie beispielsweise auf die strafprozessualen **Generalermächtigungsklauseln** §§ 161, 163 StPO zurückgreifen.[66] Das Vorgehen wäre vergleichbar mit einer **Online-Streife**, bei der in persona die frei zugänglichen Informationen durch einen Polizisten erfasst werden. Allein die Tatsache, dass durch die Software die Analyse wesentlich schneller erfolgt, kann für die rechtliche Bewertung keinen Unterschied machen.

Eingriffsgrundlagen, mit denen nicht öffentlich zugängliche Informationen analysiert werden sollen, sind für eine mögliche flächendeckende Datenanalyse nicht anwendbar. So ist beispielsweise in § 15c HSOG der **verdeckte Eingriff in informationstechnische Systeme** unter bestimmten Voraussetzungen für zulässig erklärt. Eine solche Maßnahme darf sich aber nach § 15 Abs. 2 HSOG nur gegen eine Person richten, die verantwortlich im Sinne des Gefahrenabwehrrechts ist und nur gegen die von dieser Person genutzten informationstechnischen Systeme, bzw. die Systeme einer anderen Person, wenn der Verantwortliche dort ermittlungsrelevante Informationen speichert. Ausnahmen bestehen zudem zur Verhütung terroristischer Straftaten. Ähnlich ist auch die Online-Durchsuchung in § 101b StPO geregelt. Durch den jeweiligen Anknüpfungspunkt an konkrete Gefahrensituationen, persönliche informationstechnische Systeme und spezifische Personen sind sie keine taugliche Eingriffsgrundlage für die Datenanalyse aus sozialen Netzwerken.

***

64 Zu den möglichen Eingriffsbefugnissen der Polizei und ihrer jeweiligen Bedeutung für die Ermittlung in den sozialen Netzwerken vgl. Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, et al; Ihwas, Strafverfolgung in sozialen Netzwerken, 2014, et al.

65 BVerfG Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274.

66 Ihwas, Strafverfolgung in sozialen Netzwerken, 2014, S. 134.