Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Der Landesbeauftragte für den Datenschutz Baden-Württemberg
Postfach 10 29 32 · 70025 Stuttgart

Bundesverfassungsgericht
Erster Senat
Postfach 1771
76006 Karlsruhe

Datum 4. Februar 2015
Name Herr Dr. [redacted]
Durchwahl 0711 61[redacted]
Aktenzeichen: H 1110/27
(Bitte bei Antwort angeben)

Verfügungen vom 31. Juli 2014 und vom 7. Oktober 2014 – 1 BvR 1782/09, 1 BvR 2795/09, 1 BvR 3187/10

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren Bundesverfassungsrichterinnen und Bundesverfassungsrichter,

für die Gelegenheit zur Stellungnahme zu den Verfassungsbeschwerden gegen Art. 33 Absatz 2 Satz 2 und 3 sowie Art. 38 Absatz 3 des Bayerischen Polizeiaufgabengesetzes (BayPAG), gegen §§ 22a des Polizeigesetzes (PolG) des Landes Baden-Württemberg und gegen §§ 14a, 22 Absatz 1 Satz 2 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) danke ich Ihnen. Mit Bezug vorwiegend auf die Regelungen des Polizeigesetzes in Baden-Württemberg führe ich hierzu aus:

A. Zur Zulässigkeit der Verfassungsbeschwerden – insbesondere zur Betroffenheit der Beschwerdeführer in eigenen Rechten

Die Beschwerdeführer führen aus, sie würden regelmäßig mit einem auf sie zugelassenen Kraftfahrzeug öffentliche Straßen im Geltungsbereich der genannten Polizeigesetze – soweit sie sich gegen § 22a PolG wenden, in Baden-Württemberg – nutzen. Es sei daher zu befürchten, dass ihr Kraftfahrzeugkennzeichen von einer der

aufgrund der angegriffenen gesetzlichen Bestimmungen eingerichteten automatischen Kennzeichenkontrollen erfasst und mit den im Gesetz genannten Fahndungslisten abgeglichen würden. Damit haben die Beschwerdeführer in einer für die Zulässigkeit der Verfassungsbeschwerden ausreichenden Weise ihre unmittelbare und gegenwärtige Betroffenheit in eigenen Rechten dargelegt; insbesondere ist ein weitergehender Nachweis, etwa dahingehend, dass die Kennzeichen der Beschwerdeführer tatsächlich in den polizeilichen Datenbeständen verzeichnet sind, bereits deshalb nicht zu verlangen, weil sich die Beschwerdeführer dadurch unter Umständen selbst einer Straftat bezichtigen müssten. Die Sachlage entspricht insoweit derjenigen, die der Entscheidung des Ersten Senats vom 11. März 2008 – 1 BvR 2074/05 und 1254/07 – zu den damaligen Regelungen des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung zugrunde lag (s. dort insbesondere die Absätze Nr. 59 f.).
Auch das Bundesverwaltungsgericht hat in der Entscheidung vom 22. Oktober 2014 – 6 C. 7.13 – eine gegen den Freistaat Bayern gerichtete Klage auf Unterlassung der Durchführung eines automatischen Kennzeichenabgleichs durch die Polizei gerichtete Klage für zulässig erachtet und die Klagebefugnis bejaht, obwohl das Kraftfahrzeugkennzeichen des Klägers nicht in den Fahndungslisten enthalten war.

B. Zur Begründetheit der Verfassungsbeschwerden

Die Regelung in § 22a Absatz 1 PolG erlaubt im Zusammenhang mit Kontrollen nach § 26 PolG unter weiteren Voraussetzungen die automatische Bildaufzeichnung von Kraftfahrzeugen und Erfassung von Kraftfahrzeugkennzeichen sowie die Bildaufzeichnung von Fahrzeuginsassen, die bei der Bildaufnahme der Fahrzeuge unvermeidbar betroffen werden. Absatz 2 der Vorschrift erlaubt den Abgleich der so ermittelten Kraftfahrzeugkennzeichen mit den dort genannten Sachfahndungsdateien. In Absatz 3 der Regelung wird das weitere Vorgehen bei mangelnder Übereinstimmung mit den angeglichenen Sachfahndungsdateien (Nichttrefferfall), insbesondere eine Verpflichtung zur unverzüglichen Löschung nach Durchführung des Abgleichs, normiert; Absatz 4 regelt das weitere Verfahren im Trefferfall.

I. Die von der Regelung erlaubte automatische Kennzeichenerfassung greift in das Grundrecht auf informationelle Selbstbestimmung ein.

1. Die Aufzeichnung von Lichtbildern des Fahrzeugs und des Kennzeichens sowie ggf. der Insassen sowie der Abgleich mit dem Fahndungsbestand stellen Eingriffe in den Schutzbereich des informationellen Selbstbestimmungsrechts (Artikel 2 Absatz 1

des Grundgesetzes - GG - in Verbindung mit Art. 1 Absatz 1 GG) dar. Insbesondere schützt das Grundrecht den Einzelnen nicht nur vor einer weitergehenden Verarbeitung, sondern schon vor der Erhebung der seine Person betreffenden Daten (vgl. z. B. BVerfG – Beschluss vom 28. Mai 2010 - 2 BvR 1447/10), wobei ein Kraftfahrzeugkennzeichen einen hinreichenden Personenbezug aufweist und nicht deswegen vom Schutzbereich des informationellen Selbstbestimmungsrechts ausgenommen ist, weil seine öffentliche Erkennbarkeit zu Zwecken der Individualisierung vorgeschrieben ist (BVerfG, Urteil vom 11. März 2008 – 1 BvR 2074/05 u. a. – Absatz-Nr. 67). Bereits die Erhebung von Daten – und nicht erst die weitere Speicherung, Übermittlung oder sonstige Verarbeitung – durch staatliche Organe kann nämlich beim Betroffenen das Gefühl der Beobachtung erzeugen und auf diese Weise sein Verhalten beeinflussen.

a) Auch durch die weiteren Regelungen in Absatz 2 bis 4 der Vorschrift, namentlich durch die Verpflichtung zur unverzüglichen Datenlöschung in Absatz 4, wird der Aufzeichnung die Eingriffsqualität nicht genommen. Das Bundesverfassungsgericht hat allerdings von dem Grundsatz, dass bereits in der Erhebung personenbezogener Daten ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung liegt, in mehreren Entscheidungen eine Ausnahme begründet in Fällen, in denen Daten ungezielt und allein technisch bedingt miterfasst, sie unmittelbar nach der Erfassung aber technisch wieder spurenlos gelöscht würden (insbesondere BVerfG 100, 313 [366 f.] – strategische Aufklärung durch den Bundesnachrichtendienst; BVerfGE 107, 299 [328 f.] – Zielwahlsuche; BVerfGE 115, 320 [342] – Rasterfahndung; BVerfG, Beschluss vom 17.02.2009 – 2 BvR 1372/07 u. a. – Absatz-Nr. 19 – Abfrage von Kreditkartendateien im strafrechtlichen Ermittlungsverfahren) und diese Voraussetzungen auch bei der automatisierten polizeilichen Kennzeichenerfassung als erfüllt angesehen, wenn ein Kraftfahrzeugkennzeichen im Rahmen einer polizeilichen automatisierten Kennzeichenüberprüfung zwar erfasst, aber unverzüglich ein Abgleich mit den polizeilichen Datenbeständen vollzogen wird, dieser negativ ausfällt (Nichttrefferfall) und rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden (BVerfG, Urteil vom 11. März 2008 – 1 BvR 2074/05 u. a. – Absatz-Nr. 68).

Ich räume ein, dass das Gewicht der Erhebung eines personenbezogenen Datums durch automatisierte Systeme in seiner Wirkung auf den Einzelnen maßgeblich dadurch gemindert wird, dass die automatisierte Erfassung unter den aufgestellten Kautelen durch Löschung gleichsam wieder rückgängig gemacht wird. Bei der Beur-

teilung der Eingriffstiefe – beispielweise im Rahmen einer Verhältnismäßigkeitsprüfung – ist der Umstand der unverzüglichen Löschung daher zweifelsohne zu berücksichtigen. Die Auffassung, dass deswegen bereits der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung nicht berührt sei, halte ich aber für überprüfungsbedürftig (ablehnend z. B. auch Stephan/Deger/Wöhrle/Wolf, Polizeigesetz für Baden-Württemberg, 7. Auflage 2014, Rn. 8). Denn eine anschließende Löschung von Daten macht – sofern sie technisch vollständig und erfolgreich durchgeführt wird – die Erhebung nicht ungeschehen. Bei einem Fehler des Programms zwischen Erfassung und Löschung, aber auch bei einer bewussten Manipulation (auch durch Dritte) kann es faktisch bei der Speicherung bleiben. Dass eine Löschung erfolgt, kann die Norm des § 22a Absatz 4 PolG zwar vorschreiben; dass eine vollständige Löschung auch in jedem Fall erfolgt, ist hierdurch jedoch nicht garantiert. Die Datenschutzgesetze gehen daher konsequenter Weise davon aus, dass jedes Erheben im Sinne einer Beschaffung von Daten einer Rechtsgrundlage oder Einwilligung bedarf, unabhängig davon, ob das Datum dauerhaft gespeichert wird bzw. binnen welcher Frist das Datum wieder gelöscht wird (vgl. §§ 3 Absatz 3, 4 Absatz 1 des Bundesdatenschutzgesetzes – BDSG – bzw. §§ 3 Absatz 2 Nr. 1, 4 Absatz 1 des Landesdatenschutzgesetzes Baden-Württemberg - LDSG).

Die vom Bundesverfassungsgericht vorgenommene Einschränkung des Schutzbereichs der informationellen Selbstbestimmung führt in der datenschutzrechtlichen Praxis immer wieder zu Abgrenzungsschwierigkeiten insbesondere hinsichtlich der Frage, wann eine Datenspeicherung noch kurzfristig im Sinne der Rechtsprechung ist und wann ggf. eine vollständige Löschung vorliegt. Beispielsweise wird bei dem von Niedersachsen beabsichtigten Pilotprojekt Section Control (http://www.heise.de/newsticker/meldung/Section-Control-Strecken-Radar-wird-erstmals-auf-der-Strasse-getestet-2461729.html) zur Feststellung etwaiger Geschwindigkeitsüberschreitungen von Kraftahrzeugen deren Durchschnittsgeschwindigkeit auf einem Streckenabschnitt dadurch ermittelt, dass bei der Einfahrt in den zu kontrollierenden Streckenabschnitt und bei der der Ausfahrt aus diesem Lichtbilder der Fahrzeuge mit jeweils einem Zeitstempel aufgenommen werden, so dass aus der Zeitdifferenz die Durchschnittsgeschwindigkeit errechnet werden kann. Hier stellt sich die Frage, ob für die Erhebung und die – u. U. mehrere Minuten bis zur Wiederausfahrt aus dem kontrollierten Abschnitt währende – Speicherung der Daten der Fahrzeuge, auch wenn sie mit erlaubter Geschwindigkeit gefahren sind, eine Rechtsgrundlage erforderlich ist oder ob die Speicherung noch als derart kurzfristig angesehen werden kann, dass bei einer anschließenden Löschung der Schutzbereich nicht

tangiert wäre. Im Fall eines Verfahrens zur Messung von Reisezeiten über die Erhebung der Bluetooth-Adressen von verbindungsbereiten Geräten, die in an den Sensoren des Systems vorbeifahrenden Kraftfahrzeugen mitgeführt werden, habe ich eine solche Rechtsgrundlage für erforderlich gehalten, auch wenn die Daten nach Berechnung der jeweiligen Reisezeit wieder gelöscht werden sollten (vgl. meinen 31. Tätigkeitsbericht 2012/2013, S. 90 f.). Hinzuweisen ist auch auf den von der Bundesregierung eingebrachten Entwurf eines Gesetzes zur Einführung einer Infrastrukturabgabe für die Benutzung von Bundesfernstraßen, dem zufolge die Kraftfahrzeugkennzeichen auch von inländischen Kfz automatisiert erhoben und im Hinblick auf die Zahlung der Infrastrukturabgabe abgeglichen werden sollen, obwohl zugleich eine Kontrolle über den Eingang der Zahlung im Zuge der Anmeldung eines Kraftfahrzeugs in Deutschland erfolgt und daher die Erhebung der Kennzeichen insoweit dem Grundsatz der Erforderlichkeit nicht entspricht, was der Verkehrsausschuss des Bundesrats zu Recht monierte (Niederschrift der 655. Ausschusssitzung, Vk 024-Nr. 2/16, vom 21. Januar 2015, Top 7, Rn. 22; ebenso auch schon die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014 „Keine PKW-Maut auf Kosten des Datenschutzes!"). Würde man auch hier nur von einer kurzfristigen, technisch bedingten Erfassung und Speicherung ausgehen, würde eine nicht erforderliche Datenverarbeitung gebilligt, ohne dass dies im Wege der Verfassungsbeschwerde angegriffen werden könnte.

Hinzu kommt, dass im Falle der automatischen Kennzeichenerfassung für den das Kennzeichenlesegerät bedienenden Polizeibeamten der Umstand, dass ein Fahrzeug ohne Anzeigen eines Trefferfalls den Bereich der Erfassung durchfährt, den Rückschluss zulässt, dass – vorbehaltlich eines technischen Fehlers bei der Kennzeichenerkennung – das Kennzeichen des Fahrzeugs nicht in den Dateien enthalten ist, mit denen der Abgleich vorgenommen wurde. Das mag zwar auf viele Millionen von Kraftfahrzeugkennzeichen zutreffen (vgl. die Argumentation zur mangelnden Eingriffsqualität bei der Zielwahlsuche in BVerfGE 107,299 ([328 f.]); auch eine solche Negativerkenntnis stellt aber gleichwohl ein personenbezogenes Datum dar, dessen Erhebung einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt und dessen unbefugte Offenbarung sogar die Verletzung eines Dienstgeheimnisses im Sinne des § 353b des Strafgesetzbuchs sein kann (vgl. BGH Urteil vom 23. März 2001 – 2 StR 488/00, NJW 2001, 2032 f.).

Unabhängig von den vorgenannten Erwägungen kommt es aber auch aus tatsächlichen Gründen im Nichttrefferfall zu einem Eingriff in das informationelle Selbstbe-

stimmungsrecht, wenn der Abgleich nach § 20a Absatz 2 PolG im Wege einer Online-Verbindung zu den Dateien des Bundeskriminalamts (nach § 11 Absatz 2 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten - BKAG) erfolgt. Hierzu ist darauf hinzuweisen, dass nach der Gesetzesbegründung zur Einführung des § 22a PolG (LT-Drs. 14/3165, S. 46 und 52) in technischer Hinsicht zwei Möglichkeiten zur Durchführung des Datenabgleichs in Betracht kommen: Denkbar sei es zwar, dass vor Beginn des Einsatzes eines Kennzeichenlesegerätes der gesamte Fahndungsbestand auf einer CD-ROM gespeichert werde, weil von bestimmten Orten aus eine Online-Abfrage des aktuellen Fahndungsbestand beim Bundeskriminalamt aus technischen Gründen ausscheide (a. a. O., S. 52). Der Normalfall soll es aber offenbar sein, dass jedes Kraftfahrzeugkennzeichen im Wege der Online-Abfrage mit dem Datenbestand des Bundeskriminalamts abgeglichen wird (a. a. O., S. 46). Bei einer solchen – von der Gesetzesbegründung als Normalfall angesehenen – Online-Abfrage aber wird eine Reihe von Datenverarbeitungen vorgenommen: Zunächst wird ein Bild des Kennzeichens aufgenommen (Datenerhebung), aus dem Bild die Buchstaben- und Ziffernfolge ausgelesen (Datennutzung) und das Bild sowie der gewonnene Text gespeichert (Speicherung). Danach erfolgt eine Übermittlung des durch das Gerät aus dem aufgezeichneten Bild herausgelesenen Kennzeichens an das Bundeskriminalamt. Dort wird das Kennzeichen mit den Datenbeständen abgeglichen (Datennutzung; zu allem s. Belz/Mußmann/Kahlert/ Sander, Polizeigesetz für Baden-Württemberg, 8. Auflage 2015, § 22a PolG Rn. 2). Außerdem erfolgt dort für jede einzelne Abfrage eine Protokollierung nach § 11 Absatz 6 BKAG, die für zwölf Monate vorwiegend zum Zwecke der Datenschutzkontrolle, der Datensicherheit und der Aufrechterhaltung des ordnungsgemäßen Betriebs gespeichert bleibt, gegebenenfalls aber auch zur Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person verwendet werden kann. Dem steht das Protokollierungsverbot aus § 22a Absatz 3 Satz 2 PolG nicht entgegen, das sich – schon vor dem Hintergrund der Art. 31, 70 ff. des Grundgesetzes (GG) – nur auf die Protokollierung bei der Landespolizei erstrecken kann.

b) Jedenfalls kommt es aber zu einem Eingriff in das Grundrecht, wenn ein erfasstes Kennzeichen im Fahndungsbestand aufgefunden wird (sog. Trefferfall). Spätestens ab diesem Zeitpunkt steht das erfasste Kennzeichen zur Auswertung durch staatliche Stellen zur Verfügung mit der Folge einer Persönlichkeitsgefährdung für Verhaltensfreiheit und Privatheit (BVerfG, Urt. vom 11. März 2008 – 1 BvR 2074/05 und 1254/07 – Absatz-Nr. 69). Dies ist unzweifelhaft dann der Fall, wenn sich das Kraftfahrzeug-

kennzeichen tatsächlich im überprüften Fahndungsbestand befand (echter Trefferfall) und deswegen Maßnahmen nach § 22a Absatz 4 Satz 1 und 2 PolG ermöglicht werden, und zwar auch dann, wenn sich – bei zutreffender Erkennung des Kennzeichens – der verwendete Fahndungsbestand als unrichtig (z. B. veraltet) erweist und deswegen über die Maßnahmen nach § 22a Absatz 4 Satz 1 und 2 PolG hinaus gemäß Satz 3 dieser Vorschrift keine weiteren Maßnahmen zulässig sind. Aber auch dann, wenn es sich um eine Fehl-Erkennung (unechter Trefferfall) handelte (wobei mit einer Fehlerquote von mindestens 5-8 % zu rechnen sein soll, s. BT-Drs. 18/3581 vom 17. Dezember 2014, S. 2 und 4), liegt entgegen der Entscheidung des Bundesverwaltungsgerichts vom 22. Oktober 2014 – 6 C. 7.13 – Absatz-Nr. 29 ein Eingriff in das informationelle Selbstbestimmungsrecht vor. Denn auch im unechten Trefferfall wird das Kennzeichen des Halters sowie Zeit, Ort und Richtung der Fahrt durch einen Polizeibeamten zielgerichtet zur Kenntnis genommen und mit der Information in Verbindung gebracht, dass es sich dabei um ein polizeilich ausgeschriebenes Fahrzeug handele. Selbst wenn sich nach einer Überprüfung herausstellt, dass ein Lesefehler vorlag, ist nach der Kenntnisnahme durch einen Menschen jedenfalls nicht mehr „rechtlich und technisch gesichert, dass die Daten anonym bleiben und sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden".

2. Ein Eingriff in das informationelle Selbstbestimmungsrecht derjenigen Kraftfahrzeug-Halter, deren Fahrzeuge sich im Fahndungsbestand des Bundeskriminalamts befinden, ist ferner auch dann gegeben, wenn dem Einsatz des Erkennungssystems eine Übermittlung des aktuellen Sachfahndungsbestandes der Verbunddatei und dessen Speicherung auf einem Speichermedium des Lesegeräts vorausgeht (was nach der Gesetzesbegründung zumindest dann zulässig sein soll, wenn vom Einsatzort aus eine Online-Abfrage des aktuellen Fahndungsbestand beim Bundeskriminalamt aus technischen Gründen ausscheidet, s. LT-Drs. 14/3165, S. 52; die Formulierung des § 22a Absatz 4 Satz 3 PolG deutet diese Möglichkeit an). Ob für eine derart umfassende Stapelübermittlung (vgl. hierzu § 10 Absatz 4 Satz 3 BDSG, auf den allerdings in § 11 BKAG nicht explizit Bezug genommen wird) die Ermächtigung der Polizeibehörden der Länder in § 11 Absatz 2 Satz 1 BKAG zu Abrufen, die zur jeweiligen Aufgabenerfüllung erforderlich sind, ausreicht (oder im Hinblick auf eine Umgehung des Prinzips der Vollprotokollierung in § 11 Absatz 6 BKAG) unzulässig ist, kann hier dahinstehen (vgl. zur zulässigen Übermittlung von „Mehrfachtreffern" Graulich in Schenke/Graulich/Ruthe, Sicherheitsrecht des Bundes, 2014, § 11 BKAG Rn. 35).

II. Die gesetzliche Regelung entspricht nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen.

1. Auf die – vom Ersten Senat in der Entscheidung vom 11. März 2008 – 1 BvR 2074/05, Absatz-Nr. 179, offengelassene – Frage der Kompetenz des Landesgesetzgebers zur Regelung der automatisierten Kennzeichenerfassung im Bereich der konkurrierenden Gesetzgebung (s. hierzu ausführlich die Beschwerdeschrift im Verfahren 1 BvR 2795/09, S. 8 ff. unter 2.2.1.3.1) soll hier nicht näher eingegangen werden. Besonderen Bedenken begegnen hier jedenfalls die Einbeziehung der nach § 163e StPO (vgl. hierzu auch Moldenhauer in Karlsruher Kommentar zur StPO, 7. Auflage 2013, § 163e StPO Rn. 2) und § 463a (gemeint dürfte Absatz 2 Satz 2 sein) StPO gespeicherten Daten in den Abgleich durch § 22a PolG, da durch die verwendete Automatisierung bei der Kennzeichenüberprüfung der Wirkungsbereich der Ausschreibungen zur polizeilichen Beobachtung gegenüber herkömmlichen Polizeikontrollen grundlegend verändert wird (vgl. allerdings hierzu BVerfG, Urt. vom 11. März 2008 - 1 BvR 2074/05 - , Absatz-Nr. 136 ff., wonach eine landesgesetzliche Einbeziehung der Ergebnisse des automatischen Kennzeichenleseverfahrens in die polizeiliche Beobachtung nach § 163e StPO wohl für zulässig gehalten wurde).

2. Die Regelung ist in verschiedener Hinsicht bedenklich unbestimmt.

Kaum verständlich ist bereits die Formulierung in § 22a PolG, dass der Einsatz der Kennzeichenerkennungssysteme zulässig sein soll „bei Kontrollen nach § 26 Absatz 1". Die in Bezug genommene Vorschrift des § 26 Absatz 1 PolG spricht nur in Nummer 4 und 5 von einer Kontrollstelle bzw. einem Kontrollbereich. Im Übrigen regelt die Vorschrift des § 26 Absatz 1 PolG die Feststellung der Identität einer Person. Sofern durch die Formulierung „bei Kontrollen nach § 26 Absatz 1" nicht nur auf die Voraussetzungen des § 26 Absatz 1 PolG für eine Identitätsfeststellung verweisen werden, sondern einschränkend die tatsächliche Durchführung einer Kontrolle verlangt werden sollte (so Belz/Mußmann/Kahlert/Sander, § 22a PolG Rn. 12; Stephan/Deger/Wöhrle/Wolf, § 22a Rn. 13; Zeitler/Trurnit, Polizeirecht für Baden-Württemberg, 3. Aufl. 2014, Rn. 681 m. Fn. 103), wäre dieser Versuch einer Einschränkung des Anwendungsbereichs der Norm nicht geglückt (s. allerdings BVerfG, Urt. vom 11. März 2008 – 1 BvR 2074/05 – Absatz-Nr. 144 f.); denn dass ein automatischer Abgleich nur insoweit in Bezug auf die Kraftfahrzeugkennzeichen derjenigen Personen zugelassen werden sollte, deren Identität der Polizeivollzugsdienst konkret feststellt, lässt sich kaum annehmen.

Die Vorschrift ist aber auch insoweit nicht bestimmt genug, als sie die zulässige Dauer, Häufigkeit und räumliche Dichte des Einsatzes von Kennzeichenlesegeräten nicht hinreichend nachvollziehbar regelt. Die Formulierungen, der Einsatz dürfe „nicht flächendeckend" (§ 22a Absatz 1 Satz 3 Nr. 1 PolG; s. hierzu auch schon BVerfG, Urteil vom 11. März 2008, Absätze Nr. 92, 144, 146 und 174), bzw. „nicht dauerhaft" (Nr. 2) oder „nicht längerfristig" erfolgen, sind – ohne dass die Regelungsmaterie eine konkretere Festlegung ausschließen würde – derart unbestimmt, dass sie kaum justiziabel erscheinen und ihre Anwendung nicht vorhersehbar ist. Der Gesetzgeber hat es hier versäumt, die wesentlichen Entscheidungen zur höchsten zulässigen Dichte und Dauer der Kontrollen selbst zu regeln. Auch aus der Gesetzesbegründung (LT-Drs. 14/3165, S. 48) ergibt sich keine wesentliche Hilfestellung bei der Auslegung, wenn dort insbesondere ausgeführt wird: „Bezogen auf größere Straßenabschnitte muss sichergestellt sein, dass Fahrzeuge einen größeren Straßenabschnitt in der ganz überwiegenden Zeit durchfahren können, ohne ein im Betrieb befindliches AKLS zu passieren".

3. Die Regelung entspricht auch nicht umfassend dem Grundsatz der Verhältnismäßigkeit.

a) Grundsätzliche Bedenken gegen die Erforderlichkeit der Regelung bestehen deswegen, weil die nunmehr seit über sechs Jahren in Kraft befindliche Vorschrift in Baden-Württemberg kein einziges Mal angewandt wurde (s. zuletzt die Stellungnahme der Landesregierung vom 16. April 2014 zu meinem 31. Tätigkeitsbericht, LT-Drs. 15/5302, S. 17), ohne dass dies daran liegen würde, dass die Tatbestandsvoraussetzungen des § 22a PolG bislang nicht erfüllt gewesen wären. Auch die in aller Regel geringen Fahndungserfolge der anderen Länder lassen Zweifel an der Erforderlichkeit, zumindest aber an der Verhältnismäßigkeit der Maßnahme aufkommen.

b) Darüber hinaus beschränkt sich die Regelung in § 22a PolG nicht auf das zur Zweckerreichung Erforderliche:

- Die Regelung, dass die Insassen der Fahrzeuge von der Bildaufzeichnung erfasst werden dürften, sofern dies unvermeidbar sei (§ 22a Absatz 1 Satz 2 PolG), ist nicht erforderlich (Belz/Mußmann/Kahlert/Sander, § 22a PolG, Rn. 8; a. A. noch zum damaligen Stand der Technik BVerfG, Urt. vom 11. März 2008 – 1 BvR 2074/05 – Absatz-Nr. 159) und läuft bestenfalls leer.

- Die Regelung enthält in § 22a Absatz 1 PolG die Ermächtigung zur Datenerhebung, ohne hinreichend einzuschränken, dass die Datenerhebung zu den in Absatz 1 genannten Zwecken nur zur Durchführung des Datenabgleichs nach § 22a Absatz 2 PolG erfolgen darf (anders die dem Urteil des BVerfG vom 11. März 2008 – 1 BvR 2074/05 –, zugrunde liegenden Regelungen, s. dazu Absatz-Nr. 99). Die Ermächtigung zum Datenabgleich nach § 22a Absatz 2 PolG ist vielmehr als eigenständige – nicht notwendig auf die Erhebung nach Absatz 1 folgende – Eingriffsbefugnis formuliert.
- Die Regelung bestimmt auch keine Frist für die Durchführung des Datenabgleichs. In Absatz 3 der Vorschrift ist lediglich festgelegt, dass nach Durchführung des Datenabgleichs die Löschung unverzüglich zu erfolgen habe, sofern das erkannte Kraftfahrzeugkennzeichen nicht im Fahndungsbestand enthalten war. Diese Regelung ermöglicht die Anlegung eines Datenvorrats bis zur tatsächlichen Durchführung des Abgleichs.
- Die Vorschriften in Absatz 2 bestimmen abstrakt-generell den Umfang der in den Abgleich mit einzubeziehenden Dateien, ohne dass auf den jeweiligen in § 22a Absatz 1 PolG genannten Zweck der Maßnahme abgestellt würde. Erforderlich kann aber nur der Abgleich mit solchen Dateien sein, der dem Zweck der konkreten Maßnahme (also insbesondere der Abwehr der jeweiligen Gefahr) dienlich ist (zur Vielfalt der Zwecke, zu denen allein die INPOL-Verbunddateien „Sachfahndung" und „NSIS-Sachfahndung" geführt werden, s. schon BVerfG, Urt. vom 11. März 2008 – 1 BvR 2074/05 –, Absatz-Nr. 132 ff. sowie außerdem Absatz-Nr. 145 und 174 zur notwendigen Beschränkung auf den spezifischen Bezug zum Anlass der Kontrolle).
- Hinsichtlich der technisch-organisatorischen Maßnahmen zum Datenschutz wird zwar in der Gesetzesbegründung erwähnt, dass bei einem Kennzeichenlesesystem die Kontrollkräfte bis zum Datenabgleich keine Kenntnis vom ausgelesenen Kraftfahrzeugkennzeichen nehmen könnten (LT-Drs. 14/3165, S. 46); als verbindliche organisatorische Maßnahme wird dies aber nicht festgeschrieben (obwohl die Erfüllung dieser Anforderung nicht selbstverständlich ist, s. den Bericht des Hessischen Datenschutzbeauftragten über die von ihm durchgeführte Kontrolle im 40. Tätigkeitsbericht 2011, S. 193 f.).
- In der Regelung wird kein Vorrang der offenen Erhebung normiert, von der nur bei Gefährdung des Zwecks der Maßnahme abgesehen werden kann. Nach der Gesetzesbegründung (LT-Drs. 14/3165, S. 46) soll allerdings die

Möglichkeit der offenen Erhebung im Wege des Erst-Recht-Schlusses in die Vorschrift hineingelesen werden.

Inwieweit diese Mängel des Gesetzestextes durch Auslegung korrigiert werden können oder die Verfassungswidrigkeit der Norm begründen, wird das Bundesverfassungsgericht zu entscheiden haben.

c) Wegen der umfassenden Prüfung der Verhältnismäßigkeit im engeren Sinne der Norm verweise ich auf die detaillierte Darstellung der Beschwerdeführer. Insgesamt scheint mir der vom Ersten Senat geforderte Stichprobencharakter der automatischen Kennzeichenerfassung (vgl. Urt. vom 11. März 2008 – 1 BvR 1254/07 – Absatz-Nr. 174) nicht hinreichend sichergestellt. Vor allem die Möglichkeit der Kontrolle bei jeder einfachen Gefahr für die öffentliche Sicherheit oder Ordnung (§ 26 Absatz 1 Nr. 1 PolG), die Kontrolle an „gefährlichen" Orten i. S. d. § 26 Absatz 1 Nr. 2 PolG – beides sogar ohne Beschränkung der Maßnahme auf öffentliche Straßen oder Plätze (hierzu BVerfG, Urt. vom 11. März 2008 – 1 BvR 1254/07 – Absatz-Nr. 83) – ohne konkrete Gefahrenprognose auch zur vorbeugenden Bekämpfung von Straftaten und mit der einzigen Einschränkung, dass die Kontrolle „nicht dauerhaft" erfolgen dürfe, und die (entgegen BVerfG Urt. vom 11. März 2008 – 1 BvR 1254/07 – Absatz-Nr. 175) nicht auf einen definierten Grenzbereich beschränkte anlasslose Kontrolle in Ergänzung zur sogenannten Schleierfahndung (§ 26 Absatz 1 Nr. 6 PolG) halte ich für bedenklich.

Mit vorzüglicher Hochachtung

[redacted]

Jörg Klingbeil

Abdruck

Der Bayerische Landesbeauftragte für den Datenschutz

Bayer. Datenschutzbeauftragter • PF 22 12 19 • 80502 München

Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen	München, den 23.09.2014
1 BvR 1782/09 31.07.2014	DSB/1-622-163-3	Durchwahl: 089 212672 - 0

Verfassungsbeschwerde des Herrn Benjamin E r h a r t (1 BvR 1782/09); Stellungnahme gem. § 27a BVerfGG

Anlagen: Zehn Kopien dieses Schreibens
Auszug aus dem 23. Tätigkeitsbericht 2008/2009 - BayLT Drs. 16/2100 Nr. 4.1.1)

In vorbezeichneter Angelegenheit nehme ich zu der Verfassungsbeschwerde des Herrn Erhart gegen Art. 33 Abs. 2 Satz 2 und 3 sowie Art. 38 Abs. 3 BayPAG aus datenschutzrechtlicher Sicht wie folgt Stellung:

Ich habe mich bereits in meinem 23. Tätigkeitsbericht für das Jahr 2008/2009 (LT-Drs. 16/2100 Nr. 4.1.1) mit der Problematik der automatisierten Kennzeichenerfassung auseinandergesetzt. Wie ich dort bereits kritisiert habe, wurde die automatisierte Kennzeichenerfassung nicht ausdrücklich auf Stichprobenkontrollen beschränkt, was aus meiner Sicht vorzugswürdig gewesen wäre. Ebenso ist nicht vorgesehen, dass Lageerkenntnisse, auf die sich die Maßnahme stützt, dokumentiert sein müssen. Im Gegensatz zur Begrenzung der Fahndungsbestände ist die Umschreibung der in Art. 33 Abs. 2 Satz 4 BayPAG genannten weiteren polizeilichen Dateien, mit denen ein Abgleich der Kfz-Kennzeichen möglich ist, m.E. zu weitreichend. Dadurch wird faktisch ein Abgleich mit nahezu allen polizeilichen Dateien ermöglicht.

./.

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München

Telefon: 089 212672-0
Telefax: 089 212672-50
https://www.datenschutz-bayern.de
E-Mail: poststelle@datenschutz-bayern.de

Verkehrsverbindungen:
U4/U5, Haltestelle Lehel
Bus Linie 100, Straßenbahn Linie 18
Haltestelle Nationalmuseum / Haus der Kunst

Im Rahmen der mündlichen Verhandlung vor dem Bayerischen Verwaltungsgerichtshof am 10.12.2012 (Az.: 10 BV 09.2641) wurde ich als sachkundige Person zum Einsatz automatisierter Kennzeichenerfassungssysteme in Bayern befragt, wobei ich insbesondere auf die folgenden Aspekte hingewiesen habe:

1 Anwendungspraxis in Bayern

Hinsichtlich der Anwendungspraxis in Bayern haben sich mir zunächst zwei datenschutzrechtliche Kernthemen gestellt: Die Frage der Unverzüglichkeit des Löschens und der Spurenlosigkeit der Speicherung.

Bezüglich der Problematik des unverzüglichen Löschens i.S.v. Art. 38 Abs. 3 Satz 1 BayPAG ist sowohl hinsichtlich eines sog. Nichttrefferfalls als auch im Fall eines sog. unechten Treffers grundsätzlich nicht auszuschließen, dass bei Abgleichungsfragen mit den lokal gespeicherten bzw. vorgehaltenen Fahndungsbeständen sog. Transaktionslog-Dateien geführt werden. Nach Kenntnis der Dokumentation der Systeme gibt es allerdings plausible Argumente dafür, dass auch aufgrund der begrenzten Speicherkapazität dieser Systeme entsprechende Log-Dateien entweder gar nicht oder jedenfalls nur für einen vorübergehenden Zeitraum geführt werden.

Hinsichtlich der Problematik der Spurenlosigkeit der Speicherung stellt sich die Frage nach der Möglichkeit der Rückverfolgung des sog. MD5-Codes (anonymisierte Quersumme der digitalisierten Zeichen). Diesbezüglich möchte ich darauf hinweisen, dass eine sichere Feststellung der Identität durch Rückverfolgung des MD5-Codes zwar gegenwärtig nicht möglich ist. Dies bedeutet, dass weder durch Rückrechnung eines MD5-Codes noch durch „Ausprobieren" eine zuverlässige und eindeutige Reidentifizierung eines Kfz-Kennzeichens möglich ist. Allerdings lässt das Datenschutzrecht als Ausgangspunkt die *Bestimmbarkeit* der Identität ausreichen. Sofern in Einzelfällen die Reidentifizierung mit zumutbarem Aufwand möglich ist, kann insoweit ein Datenschutzverstoß vorliegen. Bei der gegenwärtig verwendeten Technik ist hiervon nicht auszugehen.

Betreffend der gesetzlich normierten Lageerkenntnisse i.S.d. Art. 33 Abs. 2 Satz 2 BayPAG kann ich mitteilen, dass ich diese mindestens einmal jährlich vom Bayeri-

./.

schen Staatsministerium des Innern, für Bau und Verkehr, zur Vorlage anfordere. Derartige Lageerkenntnisse zu entsprechenden Gefahrensituationen i.S.d. Art. 13 Abs. 1 BayPAG existieren in schriftlich dokumentierter Form. In diesen Lageerkenntnissen werden Kriminalitäts- oder Strafbarkeitsphänomene mit Bezug auf bestimmte Örtlichkeiten und die hieraus resultierenden Gefahrensituationen beschrieben. Beispielsweise wird dargelegt, wie bei der sog. Schleuserkriminalität oder der Verschiebung gestohlener Fahrzeuge durch entsprechende Kontrollen an bestimmten Örtlichkeiten etwaig andauernde Straftaten unterbunden oder beendet werden können. Die mir vorgelegten Lageerkenntnisse sind nach meiner Einschätzung schlüssig bzw. nachvollziehbar.

2 Die Heimlichkeit der Maßnahme

Bei der Bewertung der bayerischen Regelung ist in jedem Fall als besonders eingriffserhöhend zu bewerten, dass die Kennzeichenerfassung als gesetzliche Ausnahme vom Grundsatz der offenen Datenerhebung normiert ist und eine Prüfung der Erforderlichkeit einer verdeckten, d.h. heimlichen, Erfassung ausdrücklich nicht vorgesehen ist.

Die heimliche Vornahme einer Maßnahme kann ihre Eingriffsintensität erheblich erhöhen (vgl. BVerfGE 120, 378 (406 f.)). Die Heimlichkeit einer in Grundrechte eingreifenden staatlichen Ermittlungsmaßnahme führt zur Erhöhung des Gewichts der gesetzgeberischen Freiheitsbeeinträchtigung (vgl. BVerfGE 107, 299 [321]; 115, 166 [194]; 115, 320 [353]). Dem Betroffenen wird durch die Heimlichkeit des Eingriffs vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz kann zumindest erschwert werden (vgl. BVerfGE 113, 348 [383 f.]; 118, 168). Er kann also nicht selbst darauf hinwirken, die Eingriffsintensität durch erfolgreichen Rechtsschutz zu verringern, etwa für die Zukunft zu beseitigen. Die Heimlichkeit staatlicher Informationseingriffe betrifft darüber hinaus die Gesellschaft insgesamt (vgl. BVerfGE 93, 181 [188]; 100, 313 [381]; 107, 299 [328]; 109, 279 [354 f.]).

Mit der Ausgestaltung als verdeckte Maßnahme unterscheidet sich die bayerische Regelung auch von anderen vergleichbaren Regelungen, wie beispielsweise

§ 14a, 13 Abs. 7 Satz 2 HSOG oder § 32 Abs. 5 Satz 6 Nds.SOG. Nach diesen Vorschriften

ist eine verdeckte Datenerhebung nur zulässig, wenn durch eine offene Datenerhebung der Zweck der Maßnahme gefährdet würde. Der hessische und der niedersächsische Gesetzgeber konkretisieren mit dieser Einschränkung den Grundsatz der Verhältnismäßigkeit. Demgegenüber gestattet Art. 33 Abs. 2 Satz 2 BayPAG eine Erhebung personenbezogener Daten durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme unter den für die Vornahme einer Identitätsfeststellung geltenden Voraussetzungen des Art. 13 Abs. 1 Nrn. 1 bis 5 BayPAG. Gem. Art. 30 Abs. 3 Satz 1 BayPAG sind personenbezogene Daten von der Polizei grundsätzlich offen zu erheben (sog. Prinzip des „offenen Visiers"). Auch dieser Grundsatz fußt auf dem Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar sein soll, ist zulässig, wenn die Erfüllung polizeilicher Aufgaben auf andere Weise gefährdet oder erheblich erschwert würde oder wenn anzunehmen ist, dass dies den überwiegenden Interessen des Betroffenen entspricht (vgl. Art. 30 Abs. 3 Satz 2 BayPAG). Diese einschränkende Regelung gilt nach dem historischen Willen des bayerischen Gesetzgebers ausdrücklich nicht (vgl. BayLT-Drs. 15/2096, S. 15). Der bayerische Gesetzgeber fingiert damit, dass die Heimlichkeit der Maßnahme pauschal in jedem Fall erforderlich ist. An der Erforderlichkeit dieser Regelung habe ich erhebliche Zweifel.

Eine solche Regelung wäre m.E. nur dann nicht verfassungswidrig, wenn eine offen durchgeführte automatisierte Kennzeichenerfassung typischerweise die polizeilichen Ziele der Maßnahme gefährden würde. Nachdem außerbayerische Regelungen zur automatisierten Kennzeichenerfassung vorrangig von einer offenen Datenerhebung ausgehen, scheint die grundsätzlich offene Kennzeichenerfassung für die polizeilichen Zwecke der Maßnahme durchaus geeignet zu sein.

Zu berücksichtigen ist weiterhin, dass der Schwerpunkt der Maßnahme aus kompetenzrechtlichen Gesichtspunkten auf der Gefahrenabwehr liegen muss. Handelt es sich jedoch im Schwerpunkt um eine präventive Maßnahme, ist es m.E. widersprüchlich eine solche Maßnahme pauschal verdeckt zu regeln, ohne als milderes Mittel

zusätzlich auch eine offene automatisierte Kennzeichenerkennung vorzusehen. Denn verdeckte Maßnahmen sind typischerweise dem repressiven Bereich zuzuordnen und damit dem Bereich der Strafverfolgung.

Aufgrund des eindeutigen Wortlauts der bayerischen Regelung sowie dem historischen Willen des bayerischen Gesetzgebers halte ich auch eine verfassungskonforme Auslegung nicht für möglich.

Vereinzelt wird in der bayerischen polizeirechtlichen Literatur zwar vertreten, dass die Polizei vor dem konkreten Einsatz der automatisierten Kennzeichenerfassung eine Einzelfallabwägung vornehmen müsse (Fundstelle Berner/Köhler/Käß, BayPAG, Art. 33, Rn. 22). Nach dieser Ansicht soll vor einem konkreten Einsatz zu ermitteln sein, ob der verdeckte Einsatz aufgrund der konkreten Umstände erforderlich und angemessen ist oder ob auch ein offener Einsatz ausreichend wäre, um die jeweils konkret verfolgte Zielsetzung zu erreichen.

Der so unternommende Versuch einer verfassungskonformen Auslegung des Art. 33 BayPAG scheitert jedoch an dem eindeutigen Wortlaut der Vorschrift. Im Übrigen liegen mir keine belastbaren Erkenntnisse vor, ob und inwieweit die Bayerische Polizei in der Praxis überhaupt einen offenen Einsatz der Maßnahme in Betracht zieht.

Mit freundlichen Grüßen

gez.

Dr. Thomas Petri

polizeiliche Eingriffsmaßnahmen daten- form auszugestalten, nicht aufgegriffen

Fraktion hat im Rahmen des o.g. Gesetzge- fahrens mehrere Änderungsanträge in den eingebracht. Damit sollten die Befugnis zur sierten Kennzeichenerfassung an die Anfor- des Urteils des Bundesverfassungsgerichts .03.2008 angepasst (vgl. Nr. 4.1.1) und die mit neuen, tiefgreifenden und z.T. verfas- rechtlich bedenklichen Befugnissen (Online- suchung, heimliche Wohnungsdurchsuchung, rn. 4.1.2 und 4.1.3) ausgestattet werden.

dem Gesetzentwurf und den Änderungsanträgen ich gegenüber dem Staatsministerium des In- und den zuständigen Ausschüssen des Landtags führlich Stellung genommen. Der Landtag hat das etz am 03.07.2008 beschlossen. Es ist am .08.2008 in Kraft getreten.

4.1.1 Automatisierte Kennzeichenerkennung

Im Rahmen des Gesetzgebungsverfahrens zur Änderung der Befugnis zur polizeilichen Rasterfahndung (Art. 44 PAG) hat die CSU-Fraktion einen Änderungsantrag eingebracht mit dem Ziel, die Befugnis zur automatisierten Kennzeichenerfassung an das Urteil des Bundesverfassungsgerichts vom 11.03.2008 anzupassen. Zuvor hatte ich das Staatsministerium des Innern auf eine Reihe verfassungs- und datenschutzrechtlich problematischer Punkte der bisherigen Regelung hingewiesen (vgl. Nr. 4.1).

Die Neufassung der Befugnis berücksichtigt meine Forderungen zum Teil:

- Art. 33 Abs. 2 Satz 3 PAG enthält nunmehr eine nähere Bestimmung der polizeilichen Fahndungsbestände, mit denen ein Abgleich der erfassten Kennzeichen erfolgen darf.

- Die Befugnis, die erhobenen Daten zur Verfolgung von Ordnungswidrigkeiten zu verwenden, wurde in Art. 38 Abs. 3 Satz 2 PAG gestrichen.

Leider wurde die automatisierte Kennzeichenerfassung nicht ausdrücklich auf Stichprobenkontrollen beschränkt. Darüber hinaus ist nicht vorgesehen, dass Lageerkenntnisse, auf die sich die Maßnahme stützt, gemäß dem Urteil des Bundesverfassungsgerichts dokumentiert sein müssen. Im Gegensatz zur Begrenzung der Fahndungsbestände ist die Umschreibung der „anderen polizeilichen Dateien", mit denen ein Abgleich der Kfz-Kennzeichen möglich ist, wenig präzise. Sie ermöglicht einen Abgleich mit nahezu allen polizeilichen Dateien.

4.1.2 Online-Durchsuchung

Das Bundesverfassungsgericht hat sich in seinem Urteil vom 27.02.2008 erstmals zur verfassungsrechtlichen Zulässigkeit der sog. Online-Durchsuchung und zu den Anforderungen an diese Maßnahme geäußert sowie deren Grenzen aufgezeigt. Das Gericht ist dabei davon ausgegangen, dass die Nutzung der Informationstechnik für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt hat. Die moderne Informationstechnik eröffne dem Einzelnen neue Möglichkeiten, begründe aber auch neuartige Gefährdungen der Persönlichkeit.

Zum Schutz der Nutzer informationstechnischer Systeme vor diesen neuartigen Gefährdungen hat das Bundesverfassungsgericht aus dem Grundgesetz erstmals ein „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme" hergeleitet. Einen heimlichen Eingriff in dieses Grundrecht, wie er durch die sog. Online-Durchsuchung erfolgt, hat es nur unter besonderen, eng begrenzten Voraussetzungen zugelassen. Das Bundesverfassungsgericht hebt die besondere Schwere des Grundrechtseingriffs der Online-Durchsuchung hervor, die durch einen heimlichen Zugriff auf ein fremdes informationstechnisches System („technische Infiltration") die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht.

Wegen der besonderen Schwere des Eingriffs fordert das Gericht tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut. Überragend wichtig sind nach der Entscheidung Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Es müssen bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für ein solch wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dabei den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen. Der heimliche Zugriff auf informationstechnische Systeme muss grundsätzlich von einem Richter angeordnet werden.

Darüber hinaus fordert das Gericht, dass eine gesetzliche Regelung, die zur Online-Durchsuchung ermächtigt, den verfassungsrechtlich gebotenen Schutz des Kernbereichs privater Lebensgestaltung sicherstellen muss. Erforderlich sei ein zweistufiges Schutzkonzept, wonach in einer ersten Stufe die Erfassung kernbereichsrelevanter Daten soweit möglich unterbleibt. Ergibt die Durchsicht (Zweite Stufe), dass kernbereichsrelevante Daten erhoben wurden, sind diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung ist auszuschließen.

DER HESSISCHE DATENSCHUTZBEAUFTRAGTE

28.01.2015

Stellungnahme zur Verfassungsbeschwerde 1 BvR 3187/10

1. Vorbemerkung

Die Regelung zur Kennzeichenerkennung muss an den Maßstäben gemessen werden, die das BVerfG im Urteil vom 11.03.2008 – 1 BvR 2074/05 u.a. – BverfGE 120, 378 ff – formuliert hat.

Allerdings gebieten nicht zuletzt die neuen technischen Entwicklungen, auch die dort formulierten Rahmenbedingungen nochmals einer kritischen Würdigung zu unterziehen. Dies gilt insbesondere für den dort im Leitsatz 1 formulierten Grundsatz:

> „Eine automatisierte Erfassung von Kraftfahrzeugkennzeichen zwecks Abgleich mit dem Fahndungsbestand greift dann, wenn der Abgleich nicht unverzüglich erfolgt und das Kennzeichen nicht ohne weitere Auswertung sofort und spurenlos gelöscht wird, in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) ein."

Dies wird in der Zwischenzeit allgemein so interpretiert, dass eine Datenerhebung nur dann vorliegt, wenn mehr als eine rein technische Verarbeitung von Informationen erfolgt.

In dieser Allgemeinheit ist jedoch nach meiner Ansicht eine solche technische Festlegung im Interesse des Schutzes des Rechts auf informationelle Selbstbestimmung nicht mehr sachdienlich. Ob im Einzelfall eine kurzzeitige „rein technische" Verarbeitung von Informationen keinen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, hängt sowohl von der konkreten technischen Ausgestaltung als aber auch wesentlich von dem Zweck und den besonderen Umständen der Informationsverarbeitung ab.

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telefon (06 11) 14 08-0 · Telefax (06 11) 14 08-9 00 oder -9 01
E-Mail poststelle@datenschutz.hessen.de · Internet http://www.datenschutz.hessen.de

So halte ich etwa das sog. Pre-Recording im Rahmen der Videoüberwachung nicht mit dem Recht auf informationelle Selbstbestimmung für vereinbar, soweit die Rechtsgrundlage für den Einsatz dieser Maßnahme eine konkrete Gefahr voraussetzt. Durch die permanente Ablage von Daten in einem internen Speicher stünden diese auch für einen Zeitraum zur Verfügung, in dem noch keine konkrete Gefahr vorgelegen hat bzw. durch die Einsatzkräfte eine solche noch nicht festgestellt worden ist. Damit würde eine Erhebung für die Vergangenheit erfolgen oder auch anders formuliert – eine grundsätzlich unzulässige anlasslose Vorratsdatenspeicherung.

Die Problematik zeigt sich erst recht in der Fortentwicklung im Rahmen der Entscheidung des Bundesverwaltungsgerichts vom 22.10.2014 – BVerwG 6 C 7.13 – zu § 33 Abs. 2 PAG-Bayern. Dort heißt es im Leitsatz:

> „Ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung liegt nicht vor, wenn bei Einsatz einer Einrichtung der automatisierten Erfassung von Kraftfahrzeugkennzeichen und deren Abgleich mit Fahndungsdatenbeständen zwar eine Übereinstimmung des tatsächlich erfassten Kennzeichens mit einem im Fahndungsbestand vorhandenen Kennzeichen angezeigt wird, ein visueller Abgleich durch den damit betrauten Polizeibeamten aber eine mangelnde Übereinstimmung ergibt und das erfasste Kennzeichen sofort gelöscht wird, ohne dass die Anonymität des Inhabers aufgehoben wird."

Dies geht ersichtlich weit über eine rein technische Verarbeitung einer Information hinaus. Das Bundesverwaltungsgericht verlangt noch nicht einmal eine unverzügliche Verarbeitung dieser Information durch einen Polizeibeamten. Hinzu kommt, dass schon der Ansatz, „die Anonymität wäre nicht aufgehoben" nicht den datenschutzrechtlichen Standards entspricht. Das Kennzeichen ist nicht anonymisiert sondern auf jeden Fall ein personenbeziehbares Datum, es ist immer mit dem Halter des Kraftfahrzeuges verbunden.

Das „unverzügliche Verwerfen" des fehlerhaft als Treffer erkannten Kennzeichens ist auch nicht durch die Ausgestaltung des technischen Verfahrens zu steuern, sondern beruht lediglich auf der Anweisung so zu verfahren und dem Vertrauen darauf, dass dies auch in jedem Falle so geschieht.

2. Zu § 14a HSOG

Schon im Gesetzgebungsverfahren im Juni 2009 habe ich Bedenken dahingehend geäußert, ob die neugefasste Regelung in vollem Umfang von der Gesetzgebungskompetenz des Landesgesetzgebers umfasst ist. Dies gilt sowohl für die Festlegung, in welchen Fällen diese Maßnahme zum Einsatz kommen darf als auch für die Definition des Datenbestandes, mit dem die erfassten Kennzeichen abgeglichen werden dürfen.

So erscheint mir der Grundsatz der Verhältnismäßigkeit gerade auch im Vergleich zu anderen Regelungen, die den Einsatz technischer Mittel erlauben, nicht gewahrt. Die Eingriffsschwelle – Abwehr einer Gefahr – ist zu niedrig, insbesondere soweit die Kennzeichenerkennung als verdeckte Maßnahme eingesetzt wird.

Nicht wirklich bestimmt bzw. im Sinne der Verhältnismäßigkeit ausreichend beschränkt ist die Regelung zudem, soweit sie auch im Zusammenhang des Schutzes privater Rechte bzw. für „durch Rechtsvorschriften zugewiesene andere Aufgaben" erfolgen darf. Eine echte Abwägung der Grundrechtseingriffe erscheint offensichtlich nicht erfolgt zu sein.

Durch den relativ weit gefassten Katalog der Orte bzw. Anlässe, für die ein Einsatz der Kennzeichenerkennung zulässig ist, sowie die nicht ausreichende Differenzierung der bei dem jeweiligen Einsatz zu verwendenden Abgleich-Datenbestände, ist keine hinreichend normenklare Bestimmung als geeignetes Mittel für den Grundrechtseingriff erfolgt.

Warum z.B. das Erkennen eines Fahrzeuges, dass nicht über einen Versicherungsschutz verfügt und deshalb stillgelegt werden soll, ein geeignetes Mittel zur Gefahrenabwehr im Kontext von Maßnahmen der grenzüberschreitenden Kriminalität (Bekämpfung von Drogenhandel, Zoll- oder Steuervergehen) im Sinne des § 18 Abs. 2 Ziff. 6 HSOG sein soll, erschließt sich nicht.

Im Einzelnen gebe ich folgendes zu Bedenken:

- Zwar ist jetzt – im Gegensatz zu der Vorgängerregelung des § 14 Abs. 6 HSOG – der Datenbestand, mit dem der Abgleich erfolgen darf, näher bestimmt und auch eingegrenzt. Der nunmehr zugelassene Datenbestand enthält aber weiterhin auch in nicht unerheblicher Menge Daten, die im Zusammenhang mit strafprozessualen Maßnahmen in die Datei eingestellt worden sind.

  So benennt § 14a Abs. 2 Satz 3 HSOG ausdrücklich auch Speicherungen von Fahrzeugen, die zum Zwecke der Strafverfolgung oder im Rahmen von polizeilichen Beobachtungen im Zusammenhang mit einem Strafverfahren ausgeschrieben sind.

  Schon im Rahmen des Verfassungsbeschwerdeverfahrens zur Vorgängerregelung des § 14 Abs. 5 HSOG (1 BvR 2074/05 u.a) wurde deutlich, dass die Selektion des Datenbestandes, der jeweils für den Abgleich verwendet werden sollte, mit zum Teil nicht unerheblichem Aufwand verbunden ist. Das beruht anscheinend sowohl auf der großen Anzahl der in den entsprechenden Dateien enthaltenen Datensätze, als auch möglicherweise auf einer nicht differenziert genug ausgeprägten Differenzierung bei der Darstellung der jeweiligen rechtlichen Grundlage der Speicherung, die Grundlage einer Selektierung sein könnte.

Solche Schwierigkeiten können jedoch die Verwendung von Datenbeständen – die aus der polizeilichen Maßnahme eine Maßnahme zur Strafverfolgung machen, die nicht in der Gesetzgebungskompetenz des Landesgesetzgebers liegt – nicht rechtfertigen.

- § 14a Abs. 1 S. 3 HSOG versucht den möglichen Einsatz des technischen Mittels räumlich bzw. zeitlich zu begrenzen. Die gewählten Definitionen – nicht flächendeckend, nicht dauerhaft – bleiben jedoch vage. So lassen sich insbesondere die zeitlichen Beschränkungen durch kurze Unterbrechungen im Einsatz faktisch ignorieren.

- Der Wortlaut der Norm lässt nicht klar erkennen, ob dieses Mittel offen oder verdeckt zum Einsatz kommen soll. Nach der Definition des § 13 Abs. 6 HSOG ist eine verdeckte Maßnahme eine, die nicht als solche erkennbar sein soll. Zumindest die Begründung des Entwurfs zeigt, dass die Absicht des Gesetzgebers nicht eindeutig zu bestimmen ist:

  > „Der Einsatz des AKLS darf verdeckt erfolgen, da es ansonsten leicht möglich wäre, den Kontrollbereich zu umgehen. Ein offener Einsatz des AKLS ist dadurch aber nicht ausgeschlossen." (LT-Drucksache 18/861 S. 12).

  Zumindest soweit die Kennzeichenerkennung bei Kontrollen im Rahmen des § 18 HSOG erfolgen soll, ist nicht ersichtlich, weshalb dies eine verdeckte Maßnahme sein soll.

  Die heimliche Vornahme einer Maßnahme führt im Regelfall dazu, dass ihre Eingriffsintensität erheblich erhöht ist. Dies nicht zuletzt, weil ein voriger Rechtsschutz faktisch nicht möglich und ein nachträglicher Rechtsschutz zumindest erschwert ist (vgl. BVerfGE 113, 348 ff).

Zudem ist zu fragen, ob im tatsächlichen Einsatz auch eine offene Maßnahme als solche erkennbar ist. Dazu müssten die Betroffenen zumindest in der Lage sein, den Einsatz der Geräte als solches wahrzunehmen. Dies ist in der Praxis häufig jedoch nicht oder nur schwer realisierbar, nicht nur weil die Geräte nur begrenzt als solche – auch im Unterschied zu Messgeräten für Geschwindigkeitskontrollen – erkennbar sind. Hinzu kommt, dass es den Fahrzeugführern nicht ohne weiteres möglich ist, im fließenden Verkehr sämtliche Personen und Anlagen am Straßenrand oder auf einer Brücke so exakt wahrzunehmen, dass Kontrollgeräte auffallen und somit die Datenerhebung bewusst wird.

Durch die offene Formulierung des Gesetzes können die Fahrzeugführer nicht ausschließen, dass jederzeit eine Erfassung ihres Kennzeichens erfolgen kann, unabhängig davon ob sie selbst keinerlei Anlass für eine polizeiliche Maßnahme setzen.

- Zur Frage, ob die derzeit eingesetzten Geräte geeignet sind, die Maßnahme der Kennzeichenerkennung in einem verhältnismäßigen Rahmen zu erfüllen, kann ich keine konkreten Angaben machen. Aufgrund der Auslastung meiner Dienststelle konnte in letzter Zeit keine konkrete Überprüfung von Einsätzen erfolgen. Eine im Juni 2006 erfolgte Prüfung hat ergeben, dass die Vorgaben des Urteiles vom 11.03.2008 - Nicht-Treffer-Fälle spurenlos schon im Erfassungsgerät zu löschen - erfüllt werden. Auch war im Vergleich zu früheren Überprüfungen die Möglichkeit der Erkennbarkeit auch ausländischer oder außergewöhnlicher Kennzeichen deutlich verbessert. Eine belastbare Aussage zur Fehlerquote ist mir auf dieser Grundlage jedoch nicht möglich.

3. zu § 22 Abs. 1 Satz 2 HSOG

Grundsätzlich gibt es aus meiner Sicht keine Bedenken, dass der Landesgesetzgeber den möglichen Kreis der Polizeibehörden, an die Daten übermittelt werden dürfen, im Sinne der Vorgaben des Rahmenbeschlusses 2006/960/JI des Rates erweitert hat.

Dabei ist diese Regelung im Kontext der weiteren Regelungen zur Datenverarbeitung und insbesondere -übermittlung im HSOG zu sehen. Dazu gehören zunächst die Allgemeinen Regelungen zur Datenübermittlung in § 21 HSOG. Darüber hinaus weist § 22 Abs. 1 S. 3 HSOG ausdrücklich darauf hin, dass auch die Zweckbindungsregelung des § 20 Abs. 3 HSOG zu beachten ist.

Da für jede Datenübermittlung – unabhängig von den weiteren Bedingungen, die ausdrücklich gesetzlich normiert sind – immer überprüft werden muss, ob diese auch im Einzelfall erforderlich ist, um den Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen, lässt sich diese Norm im Prinzip verfassungskonform so auslegen, dass vorab auch Überlegungen in die Entscheidung mit einfließen können, wie sie in Art. 8 des Rahmenbeschlusses 2006/960/JI des Rates als mögliche Beschränkungen ausdrücklich zugelassen sind.

Allerdings gehe ich davon aus, dass es in der Praxis schwierig sicherzustellen ist, dass entsprechende Überlegungen vor jeder Entscheidung zur Datenübermittlung erfolgen.

Im Sinne der Normenklarheit hätte der Landesgesetzgeber die Übermittlungsbefugnis allerdings auch modifizieren können, wie dies zum Beispiel in § 32a BPolG erfolgt ist.

DER SÄCHSISCHE DATENSCHUTZBEAUFTRAGTE

Bundesverfassungsgericht
Erster Senat
- Der Vorsitzende -
Richter am Bundesverfassungsgericht
Herrn Prof. Dr. Ferdinand Kirchhof
Schlossbezirk 3
76131 Karlsruhe

Dresden, 28. Januar 2015

Az: 4-2801/14/10
(Bitte bei Antwort angeben)

Telefon: Durchwahl 4935-[redacted]

Stellungnahme nach § 27a BVerfGG zu den Verfassungsbeschwerden
1 BvR 1782/09;
1 BvR 2795/09;
1 BvR 3187/10
wegen automatisierter Kennzeichenerfassung

Ihre Schreiben vom 31. Juli und vom 7. Oktober 2014

Sehr geehrter Herr Vorsitzender,

zu den drei Verfassungsbeschwerden wegen Kfz-Massenabgleichs nehme ich wie folgt Stellung:

1. Rechtliche Grundlagen im Freistaat Sachsen:

Im Freistaat Sachsen wird die automatisierte Kennzeichenerfassung durch § 19a SächsPolG geregelt. Die Vorschrift wurde im Rahmen des „Gesetzes zur Änderung des Polizeigesetzes des Freistaates Sachsen und anderer Gesetze" am 14. September 2011 beschlossen und ist am 4. Oktober 2011 in Kraft getreten (SächsGVBl 2011 Nr. 10 S. 370 – Gesetz vom 04.10.2011).
In einer am 12. Mai 2011 erfolgten öffentlichen Anhörung im Sächsischen Landtag stieß der Gesetzentwurf auf Kritik bei den geladenen Sachverständigen. Diese zielte insbesondere auf den Teil ab, der die Kennzeichenerfassung regelte. Auch ich habe damals in meiner Stellungnahme Bedenken geäußert. Diese betrafen unter anderem die Gesetzgebungskompetenz,

Postanschrift: Postfach 120705
01008 Dresden
Hausanschrift: Bernhard-von-Lindenau-Platz 1
01067 Dresden
Besucherverkehr: Devrientstraße 1
01067 Dresden
Telefon: (0351) 49 35 401
Telefax: (0351) 49 35 490
Internet: www.datenschutz.sachsen.de
E-Mail : saechsdsb@slt.sachsen.de

die ich mit Blick auf die Teile der Vorschrift, die m. E. schwerpunktmäßig repressiven Zwecken dienen, beim Bund sah. Weiterhin hatte ich unter Heranziehung der Zahlen aus Hessen, welche eine Trefferquote von lediglich 0.03% auswiesen, Zweifel an der Geeignetheit der Maßnahme geäußert. Darüber hinaus hielt ich den Teil, der die flächige Ausdehnung auf einen 30 Kilometer breiten Streifen entlang der Außengrenzen des Freistaats Sachsen zur Tschechischen Republik und zu Polen beschränkt, nicht für vereinbar mit den vom Bundesverfassungsgericht in seiner Entscheidung vom 11. März 2008 (1 BvR 2074/06 und 1 BvR 1254/07) gesetzten Voraussetzungen, da aufgrund der geographischen Gegebenheiten Sachsens damit sämtliche wesentlichen Fernstraßen – insbesondere die von Chemnitz nach Görlitz und damit parallel zur Grenze verlaufende Autobahn A4 – und Städte flächendeckend erfasst werden. Trotz der geäußerten Bedenken wurde das Gesetz – nur unwesentlich verändert – beschlossen.

2. Einsatzmittel im Freistaat Sachsen

Die sächsische Polizei verwendet ausschließlich mobile automatisierte Kennzeichenerfassungssysteme (AKES) des Typs „CatchKen" der Firma Vidit Systems GmbH. Dabei handelt es sich nach Angaben der Polizei um ein eigens für den polizeilichen Einsatz entwickeltes und für die sächsische Polizei modifiziertes System.

Dieses System wird mittels Stativ oder alternativer Halterung außerhalb des Kraftfahrzeuges oder am bzw. aus dem stehenden Fahrzeug heraus zur Anwendung gebracht. Das System ist kompakt und besteht im Wesentlichen aus einer Kameraeinheit mit integrierter IR-Beleuchtung und einer Auswerteeinheit. Für den Betrieb im geschlossenen Fahrzeug steht eine zweite Kamera zur Verfügung. Die Auswerteeinheit befindet sich in einem Koffersystem, in welchem die erforderliche Analyse-, Auswerte-, Steuerungs- und Stromversorgungstechnik verbaut ist. Die Steuerung des AKES erfolgt über einen mobilen Computer, der im Bedarfsfall auch einige Meter abgesetzt betrieben werden kann.

Der Einsatz der Kamera außerhalb des Fahrzeuges kann in einer Entfernung von bis zu 55 Metern vom Koffersystem erfolgen.

Das Kamerasystem kann bis zu drei Fahrspuren gleichzeitig erfassen. Dabei werden die gelesenen Zeichen mit dem zur Verfügung stehenden Fahndungsbestand abgeglichen und im

Trefferfall akustisch und optisch angezeigt. Nur in diesen Fällen erfolgt eine Speicherung der Aufnahme, wodurch diese für weitere Handlungen zur Verfügung steht. Im Nichttrefferfall wird die Aufnahme sowie das ausgelesene Kennzeichen nur kurzzeitig angezeigt und anschließend sofort gelöscht.

3. Informationsbesuch im Fortbildungszentrum der Polizei in Bautzen zur Vorstellung des „Mobilen automatisierten Kennzeichenerfassungssystems – AKES"

Um die datenschutzrechtliche Zulässigkeit der in Sachsen eingesetzten AKES zu beurteilen, haben meine Mitarbeiter am 4. März 2013 das Fortbildungszentrum der Polizei in Bautzen zur Vorstellung und Vorführung der Funktionsweise der AKES-Geräte besucht.

Bei der Verfahrensbeschreibung erklärte der zuständige Schulungsleiter, dass die Geräte vor allem ein Fahndungshilfsmittel seien. Auf dem Bildschirm des Laptops seien die Umrisse der durch die Kamera aufgenommenen Kraftfahrzeuge sichtbar. Aufgezeichnet würden im Trefferfall jedoch nur das Kfz-Kennzeichen sowie Ort und Zeit der Aufnahme. Die Treffer würden auf der Dienststelle aus dem Gerät ausgelesen. Im Freistaat seien landesweit fünf Geräte im Einsatz (ein Gerät je Polizeidirektion), welche ab dem 15. Februar 2013 eingesetzt würden.
Zum Abruf der Vergleichsdaten (INPOL, NSIS) und zur Einspeisung dieser Daten in die Geräte (als CSF-Datei) mittels USB-Stick seien jeweils nur bestimmte Mitarbeiter der Polizeidirektionen berechtigt. Diese Dateien stelle der Staatsbetrieb Sächsische Informatik Dienste (SID) einmal (geplant seien zukünftig viermal) je Tag zur Verfügung. Der SID ziehe (so zum Zeitpunkt des Besuches) morgens um 6 Uhr aus INPOL und Schengen den aktuellen Kfz-Fahndungsbestand. Auf Nachfrage, warum nicht die Polizei Sachsen dies selbst tue, wurde mitgeteilt, dass nur der SID auf das entsprechende Laufwerk zugreifen könne. Diese Vorgehensweise sei vom LKA Sachsen entwickelt worden. Trefferfälle würden für ein eventuell folgendes Gerichtsverfahren eigens ausgelesen und als PDF-Datei gespeichert. Nach dem Einsatz würden sie mittels USB-Stick (in der Dienststelle) übertragen und ausgedruckt. Auf Nachfrage, ob der Zeitstempel gerichtssicher sei, erklärte die Polizei, dass ein Zeitstempel vom System erstellt würde und später dann zur Dokumentation der Maßnahme ein Bericht geschrieben würde, in dem die Beamten zusätzlich den Zeitpunkt festhielten. Geplant sei die künftige Einbindung von GPS-Technik. Auf Nachfrage, wie lange der Fahn-

dungsbestand zu einem bestimmten Zeitpunkt nachvollziehbar sei, wurde darauf verwiesen, dass für die Datenhaltung in INPOL der Bund zuständig ist.

Anschließend wurde das System zunächst im Schulungsraum und nachfolgend auf dem Gelände vorgeführt. Hierzu fuhren zwei Kraftfahrzeuge der Polizei, deren Kennzeichen vorher manuell in das System eingegeben worden waren, an den aufgestellten Kameras vorbei (zwei unterschiedliche Kameras, eine mittels Stativ, die andere am Fahrzeug angebracht, kamen zum Einsatz). Trotz guter Lichtverhältnisse wurden die Kennzeichen in weniger als 40% der Fahrten als Trefferfälle erkannt. Man erklärte hierzu, dass der hier eingesetzte Rechner bereits als „problembehaftet" bekannt sei und alle ordnungsgemäß funktionierenden Geräte aktuell in den Polizeidirektionen im Einsatz seien. So habe etwa das Gerät der Polizeidirektion Görlitz in einem Einsatz zuverlässig funktioniert und vier Treffer angezeigt. Auf Nachfrage teilte die Polizeidirektion Görlitz mit, dass bisher (Stand: Oktober 2014) 7.900 Kfz gescannt worden seien. Dabei habe es sieben Treffer, davon zwei fehlerhafte wegen litauischer Kennzeichen, gegeben. Die restlichen fünf hätten alle Verstöße gegen die Pflichtversicherung („Zwangsentstempelung") betroffen. Tatsächlich angehalten werden konnten nur zwei Kfz.

Am 30. Oktober 2013 gab das Sächsische Staatsministerium des Innern zudem Informationen über den statistisch erfassten Zeitraum zwischen dem 15. Februar 2013 und dem 29. August 2013 heraus (Anlage 1). Danach habe es insgesamt 88 Einsätze des AKES gegeben. 82 Einsätze seien auf der Grundlage von § 19a Abs. 1 Satz 1 Nr. 2 und Nr. 3 SächsPolG (Sicherstellung gestohlener oder sonst abhanden gekommener Kraftfahrzeuge oder Kraftfahrzeugkennzeichen, Verhinderung der Weiterfahrt von Kraftfahrzeugen ohne ausreichenden Pflichtversicherungsschutz) und 88 Einsätze nach § 19a Abs. 1 Satz 1 Nr. 5 SächsPolG (vorbeugende Bekämpfung der grenzüberschreitenden Kriminalität) erfolgt. Die AKES-Geräte seien auf den BAB 4, 9, 14 und 72 sowie auf den Bundesstraße 2, 87 und 95 wie folgt zum Einsatz gekommen:

Anzahl	Ort	Monat des Jahres 2014	Anzahl je Monat	Einsatzstunden	Grund der Maßnahme § 19a Abs. 1 Satz 1 Nr. ... SächsPolG
68	BAB 4	Februar	5	130	2, 3, 5
		März	15	361	2, 3, 5
		April	14	281	2, 3, 5
		Mai	9	197	2, 3, 5
		Juni	17	378	2, 3, 5
		Juli	8	162	2, 3, 5
6	BAB 72	April	1	3,5	5
		Mai	3	11	5
		Juni	1	4	5
	BAB 9, BAB 14,	April	8	11,25	2, 3, 5
	B 2, B 87, B 95	Mai	2	3	2, 3, 5

Wie viele Kfz dabei gescannt wurden, sei statistisch nicht erfasst worden.

Insgesamt sei es zu 464 Treffermeldungen gekommen, wovon 72 „Echttreffer" gewesen seien. System- bzw. umweltbedingt, bspw. aufgrund schlechter Lichtverhältnisse oder verschmutzter Kennzeichentafeln, könne die von der Kamerakomponente erkannte Zeichenkette von der auf der Kennzeichentafel tatsächlich befindlichen abweichen und demzufolge zu Scheintreffern führen. Weitere Scheintreffer könnten z. B. entstehen, wenn nur die Kennzeichentafel selbst (wegen Verlusts) zur Fahndung ausgeschrieben worden sei. In diesem Fall löse die noch am Fahrzeug befindliche zweite Kennzeichentafel eine Treffermeldung aus. Die 72 „Echttreffer" unterteilten sich wie folgt: 31 Verstöße gegen das Pflichtversicherungsgesetz, 3 Unterschlagungen von Kfz, 27 Diebstähle von Kfz, 5 Diebstähle von Kennzeichen, 4 Diebstähle/Tankbetrug, 2 Feststellungen vermisster Personen. Bei diesen 72 Echttreffern seien alle Kfz angehalten und die Identität der Insassen festgestellt worden.

Eine nach dem Besuch des Fortbildungszentrums veranlasste Prüfung der übergebenen Unterlagen (IuK-Sicherheitskonzept vom 7. Februar 2013; Technisches Betriebskonzept;

CatchKen Handbuch für Polizei Sachsen vom 20. Februar 2013) ergab keine durchgreifenden datenschutzrechtliche Bedenken. Gleiches gilt für die mir vorliegende Errichtungsanordnung zum IT-Verfahren „Mobiles automatisiertes Kennzeichenerfassungssystem – AKES".

Mit freundlichen Grüßen

[redacted]

Schurig

ULD

www.datenschutzzentrum.de

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
[redacted]
Aktenzeichen:
LD5-74.03/99.123

Bundesverfassungsgericht
Erster Senat
- Der Vorsitzende -
Schloßbezirk 3
76131 Karlsruhe

Kiel, 4. Februar 2015

Verfassungsbeschwerden des Herrn Benjamin E r h a r d t, 1 BvR 1782/09 u.a.
Ihre Schreiben vom 31. Juli und 7. Oktober 2014

Sehr geehrter Herr Vorsitzender,

ich bedanke mich für die Gelegenheit zur Stellungnahme zu den im Betreff genannten Verfassungsbeschwerden und bitte, die Verzögerung zu entschuldigen. Da die Verfassungsbeschwerden Vorschriften des Landesrechts anderer Bundesländer betreffen, beschränke ich meine Stellungnahme auf die grundlegende Frage, inwieweit in der automatisierten Kennzeichenerfassung ein Grundrechtseingriff zu sehen ist.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung ist für echte sowie unechte Nichttreffer durch das Bundesverwaltungsgericht verneint worden (BVerwG, Urteil vom 22. Oktober 2014, BVerwG 6 C 7.13, Rn. 27 ff.). Das Urteil des Bundesverwaltungsgericht stützt sich auf Maßstäbe des Bundesverfassungsgerichts aus dem Urteil vom 11. März 2008, 1 BvR 2074/05, 1 BvR 1254/07 (BVerfGE 120, 378 ff.).

Nach den angewandten Maßstäben kann zwar grundsätzlich in der Erhebung von Informationen ein Grundrechtseingriff liegen, wenn dadurch Informationen für Behörden verfügbar gemacht werden und diese die Basis für einen nachfolgenden Abgleich mit Suchkriterien bilden. Maßgeblich ist nach der Rechtsprechung des Bundesverfassungsgerichts, ob sich bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet hat, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist (BVerfGE 115, 320 [343]). Ein solcher Gefährdungstatbestand für die Persönlichkeit bestehe nicht, soweit Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden (BVerfGE 120, 378 [399], BVerfGE 100, 313 [366]; 107, 299 [328]; 115, 320 [343]).

Für das Verfahren der Kfz-Kennzeichenerfassung und des anschließenden Abgleichs mit dem Fahndungsbestand geht das Bundesverwaltungsgericht nach diesen Maßstäben nicht von einem Grundrechtseingriff aus, soweit es nicht zu einer echten Übereinstimmung kommt. Ausschlaggebend hierfür ist die Ausgestaltung des Verfahrens. Bei einem echten Nichttreffer erfolge eine ausschließlich automatisierte Auswertung ohne zeitlichen Verzug und es sei gesichert, dass die Daten einer menschlichen Kenntnisnahme unzugänglich bleiben (BVerwG, a.a.O. Rn. 28). Bei einem unechten Nichttreffer erhalte ein Polizeibeamter zwar Kenntnis von dem Kfz-Kennzeichen. Da dieses aber nur zum Abgleich verwendet werde, beschränke sich das polizeiliche Interesse auf ein systembezogenes Korrekturinteresse. Darin liege noch keine Interessensverdichtung, die zu einem Grundrechtseingriff führe (BVerwG, a.a.O. Rn. 29).

Angesichts der zunehmenden Möglichkeiten der automatisierten Auswertung von Daten bedarf es meines Erachtens einer erneuten Prüfung, ob diese Maßstäbe zutreffend und ausreichend sind, um dem im Volkszählungsurteil des Bundesverfassungsgerichts formulierten Schutzgedanken des Rechts auf informationelle Selbstbestimmung Rechnung zu tragen. Die Zielrichtung des Rechts auf informationelle Selbstbestimmung besteht gerade darin, eine Gesellschaftsordnung zu vermeiden, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß" (BVerfGE 65, 1, [43]). Einer Unsicherheit der Bürger darüber, ob „abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden" (BVerfGE 65, 1 [43]), soll durch klare und begrenzende Befugnisse zur Erhebung und Verwendung personenbezogener Daten begegnet werden.

Die Datenverarbeitung durch nicht öffentliche Stellen und – wenngleich noch in geringerem Umfang durch öffentliche Stellen – ist zunehmend durch Automatisierung, insbesondere in der Auswertung von Daten, geprägt. Gleichzeitig sind zahlreiche und vielfältige Informationen über Bürgerinnen und Bürger für die Allgemeinheit verfügbar, so dass es für Behörden oftmals nicht mehr notwendig ist, personenbezogene Daten gezielt zu erheben und für eigene Aufgaben zu speichern. Vor diesem Hintergrund gewinnen Verfahren der Auswertung von Daten mit dem Ziel, auffälliges Verhalten oder Verdachtsmomente zu erkennen, zunehmend an Bedeutung. Zu nennen sind hier etwa Verfahren zur Verhaltensmustererkennung mittels Videoüberwachung und Auswertung der Bilddaten oder Verfahren zur Auswertung von öffentlich zugänglichen Daten in sozialen Netzwerken zur Erkennung von Anhaltspunkten für Gefahren oder Straftaten. Solche Verfahren sind seit einigen Jahren Gegenstand der Forschung (siehe zu Forschungsprojekten zur Verhaltensmustererkennung im öffentlichen Raum die Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. März 2012). Sie können, gerade durch ihren hohen Automatisierungsgrad, in der Regel in pseudonymisierter Weise durchgeführt werden. Wird eine große Menge von Informationen ausgewertet, um daraus relevante Daten für die Behörden herauszufiltern, wird sich das Interesse der Behörde in der Regel auf diejenigen Personen beschränken, die nach abgeschlossener Auswertung als Treffer erkannt worden sind. Gleichwohl werden alle in die Auswertung einbezogenen Daten gezielt darauf untersucht, ob sie relevante Informationen für die behördliche Aufgabenwahrnehmung enthalten. Diejenigen Personen, deren Identität nicht festgestellt wird, sind dadurch ebenfalls einem Überwachungsdruck sowie der Gefahr ausgesetzt, als echter oder unechter Treffer weiteren Maßnahmen unterzogen zu werden. Die Intensität von möglichen Einschüchterungswirkungen oder Verunsicherungen ist dabei umso höher, je ungenauer und unvorhersehbarer die Selektionskriterien sind.

Angesichts dessen stellt sich die Frage, ob das Kriterium der Interessensverdichtung der Behörde, das für die Beobachtung durch natürliche Personen sicherlich ein hinreichendes Unterscheidungs-

kriterium ist, für die Bestimmung eines Grundrechtseingriffs bei ausschließlich automatisierter Auswertung von Daten angemessen ist. Die automatisierte Datenverarbeitung unterliegt weitaus weniger Kapazitätsbeschränkungen als dies bei der Datenverarbeitung durch Polizeibeamte der Fall ist. Bei entsprechenden technischen Kapazitäten wäre praktisch eine allumfassende automatisierte Beobachtung und Auswertung vorstellbar. Hinzu kommt, dass gerade automatisierte Datenverarbeitung häufig intransparent ist. Es stellt sich die Frage, ob dies auch in rechtlicher Hinsicht zu einer anderen Bewertung bzw. zu anderen Bewertungsmaßstäben führen muss.

Führt man den Gedanken fort, der dem Eingriffskriterium der Interessensverdichtung zu Grunde liegt, wäre die Auswertung von allgemein zugänglichen Daten, z.B. aus sozialen Netzwerken, auf bestimmte Verhaltensweisen, die auf geplante Straftaten wie Amokläufe oder terroristische Anschläge hindeuten, in weitem Umfang kein Grundrechtseingriff. Diese Auswertungen können vollständig automatisiert und sicherlich weitgehend pseudonymisiert durchgeführt werden. Wendet man hierauf maßgeblich das Kriterium der Interessensverdichtung an, würde die Schwelle zum Grundrechtseingriff erst dann erreicht, wenn die Auswertung personenbeziehbare Ergebnisse hervorbringt. Dies würde in der Konsequenz den Polizei- und Ordnungsbehörden, aber auch den Strafverfolgungsbehörden ermöglichen, anlasslos sämtliches Verhalten der Bürgerinnen und Bürger im Vorfeld von Gefahren oder Straftaten automatisiert zu erfassen und auf bestimmte gefahren- oder verdachtsbegründende Kriterien auszuwerten. Die Interessen der Bürgerinnen und Bürger können hierdurch erheblich beeinträchtigt werden. Wie oben beschrieben, wäre bei entsprechenden technischen Kapazitäten eine umfassende Registrierung und Auswertung des menschlichen Verhaltens praktisch möglich. Denn gleichzeitig zu den Auswertekapazitäten steigt auch das Volumen der vorhandenen Informationen über Bürgerinnen und Bürger rasant an.

Vor diesem Hintergrund ist zu überlegen, ob eine Vorverlegung der Schwelle zum Grundrechtseingriff durch die Festlegung anderer Kriterien, wie etwa der Zielgerichtetheit der Datenabgleiche und Datenauswertungen (so BVerfGE 100, 313 [366]), zu einem angemesseneren Grundrechtsschutz für die Betroffenen führen kann.

Mit freundlichen Grüßen

[redacted]

Dr. Thilo Weichert