10 BV 09.2641
M 7 K 08.3052

NIEDERSCHRIFT

über die mündliche Verhandlung
des 10. Senats des Bayer. Verwaltungsgerichtshofs

in der Verwaltungsstreitsache Benjamin **Erhart**
gegen Freistaat Bayern
wegen automatisierter Kennzeichenerfassung

Beginn: 10.00 Uhr
Ende: 17.12 Uhr

am 10. Dezember 2012

Gegenwärtig sind die Mitglieder des Senats:
Vorsitzender Richter am VGH Senftl,
Richterin am VGH Eich,
Richter am VGH Dr. Martini
und
die stellvertretende Urkundsbeamtin Graiss.

Zur Verhandlung haben sich eingefunden:

1. Der Kläger persönlich mit
   Rechtsanwalt Dr. Kauß sowie
   Herrn Wolfgang Killinger (als technischer Beistand)
2. für den Beklagten:
   Landesanwalt Dr. Unterreitmeier
   von der Landesanwaltschaft Bayern mit
   Ministerialrat Hauser und Ltd. Polizeidirektor Feiler vom
   Bayer. Staatsministerium des Innern,
   Polizeidirektor Schmelzer und Kriminalhauptkommissarin Traßl
   vom Polizeipräsidium Oberfranken,
   Kriminaloberrat Baumann und Erster Kriminalhauptkommissar Kreil
   vom Bayer. Landeskriminalamt,
   Herrn Preußer, Technischer Leiter der Firme Vitronic (Hersteller der Kennzeichenerfassungsanlagen)

3. als sachverständiger Zeuge:
   Der Bayer. Landesbeauftragte für den Datenschutz Dr. Thomas Petri

Es wird öffentlich verhandelt.

Der Vorsitzende erklärt, der Senat beabsichtige, den Landesbeauftragten für den Datenschutz Dr. Petri nicht wie ursprünglich in der Ladung aufgeführt als sachverständigen Zeugen, sondern vielmehr aufgrund seines besonderen Fachwissens über die streitige Materie in seiner Funktion als Bayerischer Landesbeauftragter für den Datenschutz als sachkundige Person zu befragen.

Herr Dr. Petri und die Parteien sind mit dieser Vorgehensweise einverstanden.

Es ergeht folgender

Beschluss:

Zum Einsatz automatisierter Kennzeichenerfassungssysteme in Bayern wird der Bayer. Landesbeauftragte für den Datenschutz, Dr. Thomas Petri, als sachkundige Person befragt.

Die Beteiligten verzichten auf den Vortrag des Sachberichts.

Die Sach- und Rechtslage wird mit den Parteien eingehend erörtert.

Erörtert wird zunächst die Frage, ob es sich bei der vorliegenden Streitigkeit um eine solche verfassungsrechtlicher Natur i.S.d. § 40 Abs. 1 Satz 1 VwGO handelt. Der Beklagtenvertreter verweist nochmals auf den seiner Auffassung nach allein im Verfassungsrecht wurzelnden Streit, da der vom Kläger geltend gemachte Unterlassungsanspruch unmittelbar auf die Grundrechte gestützt und materiell ausschließlich die Verfassungswidrigkeit der Rechtsgrundlagen geltend gemacht werde. Der Klägerbevollmächtigte verweist demgegenüber auf das dem Rechtsstreit zugrunde liegende Rechtsverhältnis des einfachen Rechts zwischen dem Kläger als Bürger einerseits und der hier handelnden Polizei als Sicherheitsbehörde andererseits. Sich im Rahmen dieses Rechtsverhältnisses ergebende und inzident zu prüfende Verfassungsfragen machten den Rechtsstreit noch nicht zum verfassungsrechtlichen Rechtsstreit.

Auf Frage des Gerichts erklärt Herr Baumann, der Kläger sei aktuell mit keinem Kfz-Kennzeichen eines derzeit von ihm benutzten Kfz in einem polizeilichen Fahndungsbestand erfasst.

Der Klägerbevollmächtigte erklärt, ein Rechtsschutzbedürfnis des Klägers für seine Klage ergebe sich schon aus der massenhaften Erfassung u.a. auch seiner personenbezogenen Daten durch die automatisierte Kennzeichenerfassung, da insoweit völlig unverdächtige Personen anlasslos betroffen seien. Im Hinblick auf die Entscheidung des Bundesverfassungsgerichts vom 11. März 2008 (Az. 1 BvR 2074/05 u.a.) bezweifle der Kläger gerade die völlige Spurenlosigkeit dieser Erfassung; nur beispielhaft werde die Möglichkeit einer Decodierung entsprechender Spuren genannt.

Der Beklagtenvertreter verweist demgegenüber auf RdNr. 68 der betreffenden Entscheidung des Bundesverfassungsgerichts. Entscheidend für die dort verlangte sofortige spurenlose Löschung sei, dass durch die unverzügliche automatische Löschung der erfassten Kennzeichendaten ein Personenbezug nachträglich nicht hergestellt werden könne.

Der Vorsitzende weist darauf hin, dass auf diese Frage im Rahmen der Erörterung der Begründetheit der Klage nochmals im Detail eingegangen werde.

Zur Problematik eines möglichen Eingriffs in das Grundrecht auf informationelle Selbstbestimmung werden die gesetzliche Regelung und die Anwendungspraxis in Bayern anhand von drei Varianten erörtert.

Zur Variante 1 (sog. Nichttreffer):

Der Klägerbevollmächtigte verweist darauf, dass die Formulierung in Art. 38 Abs. 3 Satz 1 PAG seiner Auffassung nach hinter den Anforderungen des Bundesverfassungsgerichts in der bereits mehrfach zitierten Entscheidung zurückbleibe, weil „unverzüglich" nicht „sofort spurenlos" gleichgesetzt werden könne.

Der Beklagtenvertreter verweist auf den Umstand, dass die Löschung ohnehin automatisiert in der Datenverarbeitungsanlage (Computer) erfolge und schon deshalb ein schuldhaftes Zögern hier nicht der Fall sein könne.

Der Landesbeauftragte für den Datenschutz Dr. Petri weist darauf hin, dass die Formulierung des Gesetzgebers auch vor dem Hintergrund beurteilt werden müsse, dass darunter nicht nur der sog. Nichttrefferfall, sondern auch der Fall eines sog. unechten Treffers subsumiert werden müsse. Somit könne die vom Gesetzgeber gewählte Formulierung auch im Nichttrefferfall jedenfalls bei verfassungskonformer restriktiver Auslegung als mit den Anforderungen des Bundesverfassungsgerichts vereinbar angesehen werden.

Der Klägerbevollmächtigte verweist in diesem Zusammenhang auf die Möglichkeit der Wiederherstellung des konkreten Personenbezugs auch bei der Erfassung und dem Datenabgleich im sog. Nichttrefferfall. Der Beklagtenvertreter erklärt, eine Rückverfolgung über sog. Log-Dateien sei im Nichttrefferfall gerade nicht möglich.

Auf Frage des Gerichts erläutert Herr Preußer von der Herstellerfirma der Erfassungsanlage: Von der Kennzeichenerfassungsanlage werde an den lokalen Rechner vor Ort eine Anfrage bezüglich des jeweils erfassten Kennzeichens gemacht und im lokalen Rechner ein Abgleich mit den dort lokal gespeicherten bzw. vorgehaltenen Fahndungsbeständen vorgenommen. Seiner Kenntnis nach werde weder in der Erfassungsanlage, die im Übrigen keine Festplatte aufweise, noch im lokalen Rechner mit den dort verwendeten Datenbanksystemen ein rückverfolgbarer Log gespeichert.

Der Kläger verweist darauf, dass alle gängigen Datenbanksysteme sog. Transaktionslogs abspeicherten.

Herr Preußer führt ergänzend aus, bei dem Zugriff auf die Fahndungsdateibestände und damit die Datenbanksysteme im lokalen Rechner erfolge ein rein lesender Zugriff, bei dem Sicherheitsmechanismen wie auch Transaktionslog-Dateien grundsätzlich nicht erforderlich seien. Nach Rückfrage beim Datenbankexperten seiner Firma erklärt er, die Select-Abfrage werde nicht in einer Log-Datei gespeichert und sei damit auch nicht mehr nachvollziehbar.

Auf Frage erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Nachdem die Rechensysteme von meinen Mitarbeitern noch nicht vollständig untersucht worden sind, kann ich derzeit nicht ausschließen, dass bezüglich der Abgleichsabfrage 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."

Der Kläger erklärt, soweit solche Transaktionslog-Dateien auch nur für kurze Zeit oder wenige Tage verfügbar seien, werde dem Anspruch des Bundesverfassungsgerichts einer sofortigen spurenlosen Beseitigung nicht genügt.

Auf Frage erklärt der Bayer. Landesbeauftragte für den Datenschutz Dr. Petri: „Die Unverzüglichkeit des durchzuführenden Datenabgleichs ist nicht in Art. 38 Abs. 3 Satz 1 PAG geregelt. Diese Frage bzw. Problematik ist vielmehr nach der für die Erfassung und den Datenabgleich einschlägigen Regelung des Art. 33 Abs. 2 PAG zu beurteilen. Diesbezüglich habe ich bisher allerdings keine verfassungsrechtlichen Probleme bei der Durchführung des Datenabgleichs gesehen."

Der Beklagtenvertreter verweist zu dieser Problematik auf die Formulierung „automatisiert" in Art. 33 Abs. 2 PAG.

Zur Variante 2 (sog. unechter Treffer oder Syntaxfehler):

Auf Frage des Gerichts, ob bei den abgefragten Kfz-Kennzeichen in den polizeilichen Fahndungsbeständen auch Kennzeichen fragmentarisch im Fahndungsbestand erfasst seien, erklärt Herr Baumann vom LKA: „Der Abgleich mit nur fragmentarisch erfassten Kennzeichen im Wege der automatisierten Kennzeichenerfassung macht schon ermittlungstechnisch keinen Sinn."

Auf Frage bestätigt Herr Preußer von der Herstellerfirma, dass nur komplette Kennzeichen in den abgeglichenen Datenbanken erfasst seien.

Auf Frage erklären die Vertreter des Beklagten, wie bereits im Verfahren ausgeführt würden zum Abgleich vor Ort bei der automatisierten Kennzeichenerfassung ausschließlich vollständige Kennzeichen aus den verschiedenen Fahndungsbeständen in entsprechenden Datenbanken vorgehalten. Ein Abgleich mit sonstigen Fahndungsdaten oder auch unvollständigen Kennzeichen sei schon deshalb nicht möglich.

Zur Frage des Zustandekommens sog. unechter Treffer oder Syntaxfehler erläutert Herr Preußer anhand einer vorgefertigten Übersicht: „Sog. unechte Treffer kommen zum einen durch Lesefehler des Erfassungssystems zustande, weil in fünf bis acht Prozent der Fälle das vorbeifahrende Kennzeichen vom Lesegerät falsch ausgelesen wird. In diesem Fall ist allerdings die Herstellung eines Personenbezugs schon aufgrund des falsch gelesenen Kennzeichens und des darauf beruhenden ebenfalls falschen MD5-Codes nicht herstellbar. Zu fehlerhaften Treffern kommt es darüber hinaus bei Verwechslungsfehlern, z.B. wenn das Gerät eine "0" mit dem Buchstaben "O" oder das Kennzeichen M-AN ... mit dem Kennzeichen MA-N ... verwechselt. Solche Verwechslungen als systematische Fehler sind vom System gewollt."

Herr Preußer erläutert weiter: „Wird nach dem Abgleich mit den Fahndungsbeständen auf dem Computer vor Ort ein Treffer festgestellt, wird dieser Treffer sogleich über VPN an den zentralen Z-Server übermittelt, wo es dann zu der weiteren Überprüfung kommt. Auf dem Rechner vor Ort bleibt in diesem Fall als „Übertragungsspur" lediglich ein sog. MD5-Code und vorübergehend in einem Pufferspeicher eine entsprechende Transaktionslog-Datei übrig. Den MD5-Code kann man sich dabei als anonymisierte Quersumme der digitalisierten Zeichen vorstellen. Die Rückverfolgung oder Reproduzierbarkeit ausgehend von dieser Quersumme zurück zum ursprünglichen Kennzeichen ist aufgrund weiterer bei dieser Methode verwendeter Parameter nach meiner Auffassung mit sehr hoher Sicherheit nicht möglich."

Der Kläger erklärt dazu, richtig sei zwar, dass man aus der MD5-Quersumme nicht im umgekehrten Weg das ursprüngliche Kennzeichen ermitteln könne. Es sei jedoch mit vergleichsweise geringem Aufwand sowohl bezüglich Hard- als auch Software möglich, durch Eingabe aller möglichen Kennzeichenkombinationen herauszubekommen, bei welchen Kennzeichen es zur konkreten MD5-Quersumme komme. Eine Deanonymisierung eines solchen MD5-Codes sei mit einer zumindest 90 bis 95%igen Sicherheit möglich.

Herr Preußer von der Herstellerfirma bestreitet dies und erklärt, auch das Bundesamt für Sicherheit in der Informationstechnik gehe davon aus, dass eine Authentifizierung im Umkehrweg nicht sicher erfolgen könne.

Auf Frage erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Richtig ist, dass eine sichere Feststellung der Identität durch Rückverfolgung des MD5-Codes

nicht möglich ist, aber auch, dass das Datenschutzrecht als Ausgangspunkt die Bestimmbarkeit der Identität ausreichen lässt. Wenn man mit einem zumutbaren Aufwand von der Bestimmbarkeit ausgehen kann, wäre aus meiner Sicht jedenfalls ein Verstoß gegen Datenschutzrecht gegeben. Davon ist bei der verwendeten Technik derzeit meines Erachtens aber wohl noch nicht auszugehen. Ein anderes Problem ist jedoch die Frage der Spurenlosigkeit, da diese MD5-Codes eben dauerhaft im System bestehen bleiben."

Der Beklagtenvertreter wendet ein, selbst im Fall einer Rückverfolgbarkeit komme als Ergebnis bestenfalls ein falsches INPOL-Kennzeichen als Ergebnis heraus.

Auf Frage zum weiteren Ablauf im Falle eines unechten Treffers erklärt Herr Schmelzer: „Vom lokalen Rechner vor Ort wird der unechte Treffer (ebenso wie der echte Treffer) zunächst auf den Zentralrechner der Einsatzzentrale übermittelt. Dort wird vom zuständigen Beamten der Einsatzzentrale eine visuelle Kontrolle der Übereinstimmung des erfassten Kennzeichens mit dem vermeintlichen Treffer der Datenbank durchgeführt. Stellt der Beamte fest, dass die beiden Kennzeichen nicht übereinstimmen, wird der gesamte Vorgang durch die Eingabe eines Löschbefehls gelöscht. In diesem Fall verbleibt auch auf dem Rechner in der Einsatzzentrale als Spur dieser Treffermeldung nur die MD5-Quersumme (wie auf dem Rechner vor Ort) zurück."

Herr Preußer erläutert, durch den Befehl „Entfernen" werde der Datenbank-Delete-Befehl ausgelöst. Insoweit unterscheide sich seines Wissens der Vorgang auch nicht, wenn die Überprüfung in einem mobilen Erfassungssystem durch den Beamten vor Ort auf seinem Laptop erfolge.

Die Beteiligten diskutieren die Frage, ob die durch den Entfernen-Befehl gelöschten Daten in der Datenbank später ohne größeren Aufwand als solche wieder ausgelesen werden können. Der Kläger ist der Auffassung, dies sei ohne Weiteres möglich. Herr Preußer von der Herstellerfirma verweist darauf, dass auf der Datenbank sog. kryptische Daten verwendet würden, die auch nur für einen bestimmten Zeitraum noch als solche zur Verfügung stünden.

Der Beklagtenvertreter erklärt, durch Dienstvorschriften für die betreffenden Beamten sei rechtlich gesichert, dass hier ein denkbarer Missbrauch ausgeschlossen werde.

Auf Frage erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Wenn vom System ein Treffer festgestellt und an den Zentralrechner der Einsatzzentrale weitergeleitet wird, ist nach meiner fachlichen Einschätzung die Grenze der Aufhebung der Anonymität und damit auch die Grenze zum Eingriff in das Grundrecht auf informationelle Selbstbestimmung überschritten und zwar unabhängig davon, ob es sich um einen echten oder unechten Treffer handelt. Entscheidend ist, dass allein durch diese Falleingrenzung entsprechend der Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung die Personenbeziehbarkeit, d.h. Bestimmbarkeit der Person nach objektiven Kriterien, hergestellt und damit die Anonymität aufgehoben werden kann. Nicht ausschlaggebend ist insoweit, ob diese Personenbeziehbarkeit im konkreten Fall tatsächlich verfolgt wird."

Herr Hauser verweist auf die entgegengesetzte Bewertung in dem im Verfahren bereits zitierten Gutachten des Max-Planck-Instituts zur Brandenburgischen Regelung über die automatisierte Kennzeichenerfassung (dort S. 100).

Zur Variante 3 (sog. Trefferfall):

Auf Frage erklären die Beklagtenvertreter: „Im sog. Trefferfall werden die Daten grundsätzlich immer gespeichert, weil sie für weitere polizeiliche Maßnahmen benötigt werden. Ab diesem Zeitpunkt erfolgt dann auch ein entsprechender Eintrag mit Aktenzeichen in der polizeilichen Vorgangsverwaltung. Zu einer Verwerfung bzw. Löschung entsprechender Daten kam es hier vor allem im Zusammenhang mit Verstößen gegen das Pflichtversicherungsgesetz, die sich bei der Überprüfung als nicht mehr aktuell herausstellten. Die Speicherung dieses Vorgangs erfolgt in der Praxis dadurch, dass ein Bild der Bildschirmtreffermaske als PDF-Dokument gespeichert und an die zuständige Einheit weitergeleitet wird. Auf dem Rechner der Einsatzzentrale wird der Vorgang als solcher durch den Beamten dann gelöscht. Sollte der Beamte die Löschung ausnahmsweise vergessen, findet die Löschung automatisiert nach 30 Tagen statt."

Auf Frage erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Bei einem echten Treffer bestehen nach meiner Einschätzung keine rechtlichen Bedenken, wenn in diesem Fall die Polizei gemäß Art. 38 Abs. 1 und 2 PAG weiter verfährt. Alles andere wäre im Übrigen nach meiner Auffassung auch systemwidrig."

Die Verhandlung wird um 13:05 Uhr unterbrochen und um 13.46 Uhr fortgesetzt.

Zur Frage der Gesetzgebungskompetenz des Beklagten für die Maßnahmen der automatisierten Kennzeichenerfassung erklärt der Klägerbevollmächtigte, sowohl der Wortlaut der gesetzlichen Bestimmungen (Art. 33 Abs. 2 insbesondere Satz 3, Art. 38 Abs. 3 Satz 2 PAG) als auch die tatsächlich festzustellenden Erfolge dieser Maßnahme sprächen eindeutig für die repressive Zielsetzung und Ausrichtung dieser Maßnahme. Gerade der vorliegende Fall zeige aber die Notwendigkeit, die Regelungsbereiche der Strafverfolgung (StPO) und der polizeilichen Gefahrenabwehr eindeutig und unmissverständlich abzugrenzen.

Der Beklagtenvertreter entgegnet, Schwerpunkt der Erfassung dieser Daten bei der Kennzeichenerfassung sei eindeutig die Prävention; der Wortlaut von Art. 33 Abs. 2 und Art. 38 Abs. 3 PAG stehe dem auch nicht entgegen. Eine dogmatisch saubere und strenge Trennung zwischen Prävention und Strafverfolgung sei auch gar nicht möglich. Im Übrigen stellten die Regelungen der StPO insoweit keine abschließende bundesgesetzliche Regelung mit Ausschlusswirkung für ergänzende landesrechtliche Regelungen dar. Die präventive Informationsgewinnung aus Anlass der in Art. 13 Abs. 1 Nrn. 1 bis 5 PAG beschriebenen Situationen stehe eindeutig im Vordergrund.

Der Landesbeauftragte für den Datenschutz Dr. Petri erklärt, zur Bestimmung der Zweckrichtung dieser Maßnahme müsse Art. 33 Abs. 2, insbesondere Abs. 2 Satz 3 Nr. 2 b, im Zusammenhang mit den Regelungen in Art. 13 Abs. 1 Nrn. 2 und 3 PAG gesehen werden. Letztere stellten gerade nicht auf eine besondere Gefahrensituation ab, die es abzuwehren gelte. Einen Rückschluss aus Art. 38 Abs. 3 Satz 2 PAG hinsichtlich des gesetzlichen Regelungszwecks der automatischen Kennzeichenerfassung halte er nicht für zwingend bzw. möglich. Vielmehr könne man die Regelung in Art. 38 Abs. 3 Satz 2 PAG möglicherweise als Zweckänderung einordnen. Seiner Kenntnis nach habe zuletzt der Thüringische Verfassungsgerichtshof in einer Entscheidung im November dieses Jahres den Versuch einer sauberen Abgrenzung zwischen präventiven und repressiven Handlungszwecken bei einer möglicherweise vergleichbaren Ausgangssituation unternommen. Nach seiner Auffassung gebe es gute Argumente dafür, dass der Bundesgesetzgeber insbesondere auch im Bereich der Strafverfolgungsvorsorge eine Regelung zur automatisierten Kennzeichenerfassung bewusst nicht in den Befugniskatalog mit aufgenommen habe. So sei bei-

spielsweise bei der letzten Novellierung des Bundeskriminalamtgesetzes eine solche Befugnis nicht in das Gesetz mit aufgenommen worden.

Der Beklagtenvertreter weist noch auf die Regelung des Art. 43 Abs. 1 Satz 3 PAG hin. Die Regelung zur Speicherung und Nutzung der bei der automatisierten Kennzeichenerfassung gewonnenen Daten in Art. 38 Abs. 3 Satz 2 PAG sei nur eine entsprechende Bestimmung für diesen speziellen Fall (lex specialis). Weiter verweist er auf die Richtlinie 2002/90/EG vom 28. November 2002 und führt diese beispielhaft für ein gemeinschaftsrechtliches Optimierungsgebot bezüglich der Verfolgung der Straftat einer unerlaubten Einreise an. Auch für andere Bereiche gebe es entsprechende gemeinschaftsrechtliche Bestimmungen, denen man insgesamt die Pflicht der Bundesrepublik zu einem wirksamen Einschreiten entnehmen könne.

Zur Problematik der hinreichenden Normklarheit und Normbestimmtheit:

Auf Frage zu den in Art. 33 Abs. 2 Satz 2 PAG verlangten Lageerkenntnissen erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Die gesetzlich verlangten Lageerkenntnisse fordere ich mindestens einmal jährlich vom Freisstaat Bayern zur Vorlage an. Derartige Lageerkenntnisse zu entsprechenden Gefahrensituationen i.S.d. Art. 13 Abs. 1 PAG existieren in schriftlich dokumentierter Form. Durch die mir vorgelegten Lageerkenntnisse werden entsprechende Gefahrensituationen nach meiner Einschätzung schlüssig bzw. nachvollziehbar umschrieben."

Auf Nachfrage des Klägerbevollmächtigten ergänzt Herr Dr. Petri: „In diesen Lageerkenntnissen werden schwerpunktmäßig Kriminalitäts- oder Strafbarkeitsphänomene mit Bezug auf bestimmte Örtlichkeiten beschrieben, aus denen sich nach meiner Einschätzung zwangsläufig entsprechende Gefahrenlagen (im untechnischen Sinn) ergeben. Als Beispiel möchte ich dafür anführen, dass bei der sog. Schleuserkriminalität oder der Verschiebung gestohlener Kfz durch entsprechende Kontrollen an bestimmten Örtlichkeiten auch die andauernde Straftat unterbunden oder beendet werden kann."

Der Beklagtenvertreter verweist aktuell z.B. auf eine besondere Gefahrenlage hinsichtlich Schleusungen afghanischer Staatsangehöriger in die Bundesrepublik. Er verweist ergänzend dazu auf eine Entscheidung des EuGH vom 10. April 2012

(Rs. C-83/12 RdNrn. 45 ff.), wonach die Mitgliedstaaten zur effektiven Bekämpfung dieser Schleuserkriminalität verpflichtet seien.

Die Parteien diskutieren kontrovers die hinreichende Präzisierung und Konkretisierung der abgleichbaren Fahndungsbestände i.S.d. Art. 33 Abs. 2 Satz 3 PAG. Der Klägerbevollmächtigte kritisiert insoweit nochmals, dass es sich dabei nach wie vor um Fahndungsbestände handle, die sowohl repressiven wie gefahrenabwehrenden Zwecken dienten. Eine Trennung sei insoweit nicht erkennbar. Die Beklagtenvertreter verweisen auf die nach der Rechtsprechung zulässigen Mischdateien und die schwierige bzw. kaum mögliche saubere Abgrenzung zwischen präventivem und repressivem polizeilichen Handeln. Auch das Unionsrecht kenne eine solche Unterscheidung nicht.

Auf Frage erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Nach meiner Auffassung hat der bayerische Gesetzgeber in der aktuellen Regelung in Art. 33 Abs. 2 PAG die Anforderungen des Bundesverfassungsgerichts insoweit weitestgehend erfüllt, als diese hinreichende Kontrollmöglichkeiten gewährleisten."

Auf Frage zu den in der Praxis abgeglichenen Verbunddateien erklären die Beklagtenvertreter: „Es handelt sich hier um in jedem Bundesland voll parallel geführte Verbunddateien des Bundeskriminalamts nach §§ 11 ff., 13 BKAG. Betreiber dieser Verbunddateien ist das Bundeskriminalamt. Die Länder dürfen die vorgehaltenen Daten abfragen. Jeder Polizeibeamte ist im Rahmen seiner Zuständigkeit dann für diese Verbunddateien auch bearbeitungsberechtigt und kann Veränderungen bzw. Ergänzungen der Dateien vornehmen, die ab einer bestimmten Erheblichkeitsschwelle dann für alle Länder sichtbar sind."

Auf Frage des Gerichts erklären die Beklagtenvertreter: „Bei der Speicherung und Nutzung der durch die automatisierte Kennzeichenerfassung gewonnenen Daten für bestimmte Zwecke (auch repressiver Natur) erfolgt im System eine entsprechende Kennung mittels Schlagwort. Dadurch kann die Art der Gewinnung dieser Daten rückverfolgt werden."
Auf Nachfrage: „Eine gesetzliche diesbezügliche Regelung besteht nicht. In den Dienstvorschriften ist allerdings eine solche Kennung vorgesehen."

Auf Frage erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Eine Regelung der Kennzeichnung der Daten, um deren Kumulation für Überwachungszwecke entgegenzuwirken, ist im Bereich der Gefahrenabwehr, wo ich niedrigere Anforderungen sehen würde, sicher im Hinblick auf die Regelungen des Art. 33 Abs. 2 Satz 5 und Art. 38 Abs. 3 Satz 3 PAG hilfreich. Strengere Maßstäbe sind nach meiner Meinung aber im Bereich der Strafverfolgung anzusetzen. Dann müsste aber auch eine korrespondierende Regelung in die StPO aufgenommen werden."

Der Beklagtenvertreter ergänzt, einer Kumulierung durch die automatisierte Kennzeichenerfassung gewonnener Daten stehe schon die Regelung in Art. 38 Abs. 3 Satz 3 PAG entgegen. Im Übrigen griffen die die Rasterfahndung betreffenden Bestimmungen.

Der Beklagtenvertreter verweist zur erforderlichen Güterabwägung im Rahmen des Grundsatzes der Verhältnismäßigkeit auf die nach Auffassung des Beklagten geringere Schutzbedürftigkeit der betroffenen Autofahrer hinsichtlich der Erfassung der Kennzeichen im öffentlichen Straßenverkehr und die hinter den entsprechenden Fahndungsbeständen stehenden gewichtigen Schutzgüter, die mögliche Grundrechtsbeeinträchtigungen rechtfertigten.

Der Klägerbevollmächtigte verweist zusammenfassend nochmals auf die seiner Meinung nach ganz offensichtlich fehlende Mittel-Zweck-Relation dieser Maßnahme.

Die Beklagtenvertreter verweisen auf die Notwendigkeit einer effektiven Bekämpfung z.B. auch der Bandenkriminalität durch diese Maßnahme.

Auf Frage erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „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 und eine Prüfung der Erforderlichkeit einer verdeckten, d.h. heimlichen, Erfassung ausdrücklich nicht vorgesehen ist. Damit unterscheidet sich auch die bayerische Regelung von allen anderen mir bekannten derartigen Regelungen. Im Übrigen bestehen aus meiner Sicht keine signifikanten Unterschiede der bayerischen Regelung zu den Regelungen anderer Bundesländer."

Der Beklagtenvertreter verweist auf Feststellungen in der vergleichenden Untersuchung des Max-Planck-Instituts zu den entsprechenden Regelungen anderer Bundesländer. Danach sehe auch die Regelung in Baden-Württemberg eine verdeckte Kennzeichenerfassung vor, in vier anderen Bundesländern sei eine grundsätzlich offene Datenerhebung vorgesehen, eine verdeckte darüber hinaus aber möglich. Weiter verweisen die Beklagtenvertreter auf Art. 99 SDÜ, worin ausdrücklich die verdeckte Datenerhebung vorgesehen sei. Weiter erklären die Beklagtenvertreter, dass in Bayern die mobilen Anlagen zur Kennzeichenerfassung anlässlich der Fußball-WM 2006 offen eingesetzt worden seien.

Mit den Beteiligten wird die Frage diskutiert, ob Art. 33 Abs. 2 PAG als minus auch die offene Kennzeichenerfassung erlaubt und wie - dies vorausgesetzt - dann die Formulierung „unbeschadet des Art. 30 Abs. 3 Satz 2 PAG" zu verstehen sei.

Nach Auffassung der Beklagtenvertreter verbietet die bayerische Regelung jedenfalls die offene Kennzeichenerfassung nicht.

Auf Frage des Klägerbevollmächtigten erklärt der Landesbeauftragte für den Datenschutz Dr. Petri, bisher sei es nur in einem einzigen Fall zu einer Beschwerde eines Bürgers wegen der automatisierten Kennzeichenerfassung gekommen. Für ihn sei dies deshalb nicht verwunderlich, weil sie für den Bürger eine verdeckte Maßnahme darstelle, die er als solche nicht erkennen könne.

Der Beklagtenvertreter erwidert, aus der Sicht der Parallelwertung in der Laiensphäre verbinde der Bürger mit entsprechenden Kameras an öffentlichen Straßen sehr wohl eine staatliche Beobachtung.

Auf Frage des Gerichts erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Zur Frage der Bedeutung der Streubreite der Maßnahme ist aus meiner Sicht anzumerken, dass sich eine solche Maßnahme in punktueller Anwendung noch im Rahmen des Verhältnismäßigen bewegt. Die Erfolgsquote der Maßnahme als solche hat nach meiner Erinnerung im Verfahren vor dem Bundesverfassungsgericht keine entscheidende Rolle in der Diskussion gespielt. Bei der Beurteilung der Verhältnismäßigkeit ist grundsätzlich nach der Rechtsprechung die Gesamtmaßnahme mit ihren Auswirkungen auf die Bevölkerung insgesamt in den Blick zu nehmen und in die Bewertung mit einzustellen. Dazu kann ich lediglich bemerken, dass diesbezügliche

Beschwerden aus der Bevölkerung gerade im Hinblick auf die massenhafte Erfassung und mögliche Einschüchterungseffekte in letzter Zeit nicht festzustellen sind."

Auf Frage des Klägerbevollmächtigten erklärt der Landesbeauftragte für den Datenschutz Dr. Petri: „Das Auskunftsrecht beispielsweise nach Art. 48 PAG ist nach meiner Auffassung nicht als Kompensation der verdeckten Maßnahme zu sehen. Eine solche Kompensation wäre vielmehr die Benachrichtigung des betroffenen Bürgers."

Auf Frage des Gerichts ergänzt Dr. Petri: „Die Verhältnismäßigkeit einer Maßnahme wie der automatisierten Kennzeichenerfassung ist je nach dem konkreten Einsatzzweck der Maßnahme differenziert zu beurteilen. Die Festlegung des Gesetzgebers der Schwelle einer Gefahr im Bereich der Gefahrenabwehr ist nach meiner Einschätzung wohl ausreichend. Eine weitergehende Differenzierung nach Gefahrenschwellen kann aber bei anderen Zwecken der Maßnahme geboten sein. Nicht unproblematisch erscheint mir in diesem Zusammenhang die in Bezug genommene Bestimmung des Art. 13 Abs. 1 Nr. 4 PAG mit dem dortigen Verweis auf § 100a StPO."

Der Beklagtenvertreter verweist in diesem Zusammenhang auf die Bestimmung des § 99 SDÜ, die auch für die Ausschreibung von Kfz erhebliche Gefahren voraussetze.

Auf Nachfrage ergänzt Dr. Petri: „Der Rund-um-die-Uhr-Betrieb der Kennzeichenerfassung ist bezogen auf die Einzelmaßnahme und einen punktuellen Betrieb als weniger problematisch zu beurteilen. Bezogen auf die objektive Gesamtbetrachtung der Maßnahme als solche ist ein Rund-um-die-Uhr-Betrieb sicher als gravierender zu beurteilen als eine nur zeitlich begrenzte Erfassung."

Auf Frage des Klägerbevollmächtigten bestätigt der Landesbeauftragte für den Datenschutz Dr. Petri, dass er in seinem 23. Tätigkeitsbericht für das Jahr 2008 (LT-Drs. 16/2100 Nr. 4.1.1) ausgeführt habe, dass aus seiner Sicht eine stichprobenartige Kontrolle vorzugswürdig sei.

Die Beteiligten sehen bezüglich der Verhältnismäßigkeit der Maßnahme keinen weiteren Erörterungsbedarf.

Der Klägerbevollmächtigte erklärt zusammenfassend, die Grundrechtsbetroffenheit des Klägers sei deshalb gegeben, weil auch der Kläger damit rechnen müsse, künftig in den Fahndungsbestand der Polizei auch ohne seine Kenntnis und ohne eigenes Verschulden aufgenommen zu werden. Bei dieser Betroffenheit sei vor allem die absolute Breitenwirkung und Flächenabdeckung dieser Kennzeichenerfassung zu berücksichtigen. Die bayerische Regelung erweise sich auch nach dem Ergebnis der mündlichen Verhandlung als unverhältnismäßig.

Der Beklagtenvertreter erklärt, in der mündlichen Verhandlung sei nochmals deutlich geworden, dass der Kläger eine besondere Betroffenheit durch die streitige Maßnahme nicht geltend machen könne. Vielmehr handle es sich bei seiner Klage - wie bereits eingangs ausgeführt - um eine verkappte verfassungsrechtliche Klage. Im Hinblick auf die begrenzte Anzahl der Erfassungsanlagen könne im Übrigen von einem flächendeckenden Einsatz und einer Rundumüberwachung nicht gesprochen werden.

Ergänzend verweist der Beklagtenvertreter für den Fall, dass der Senat Bedenken bezüglich der Vereinbarkeit der bayerischen Regelung mit höherrangigem Recht habe, im Hinblick auf den grenzüberschreitenden Bezug dieser Fragestellung auf das nach der Rechtsprechung des EuGH vorrangige Vorabentscheidungsverfahren (Entscheidung vom 22.6.2010 Rs. C-188/10).

Der Kläger beantragt,

> den Beklagten in Abänderung des Urteils des Verwaltungsgerichts München vom 23. September 2009 zu verurteilen, es zu unterlassen, durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme Kennzeichen von Kraftfahrzeugen, die auf den Kläger zugelassen sind, zu erfassen und mit polizeilichen Dateien abzugleichen.

Der Beklagte beantragt,

> die Berufung als unzulässig zu verwerfen,
> hilfsweise:
> die Berufung als unbegründet zurückzuweisen.

Es ergeht folgender

Beschluss:

Eine Entscheidung wird den Beteiligten zugestellt.

Nachdem niemand mehr das Wort wünscht, schließt der Vorsitzende um 17.12 Uhr die mündliche Verhandlung.

Senftl
Vorsitzender

Graiss
Schriftführerin