2639 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP

Bericht

des Ausschusses für innere Angelegenheiten

über den Antrag 4132/A der Abgeordneten Dr. Christian Stocker, Mag. Georg Bürstmayr, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert wird

Die Abgeordneten Dr. Christian **Stocker**, Mag. Georg **Bürstmayr**, Kolleginnen und Kollegen haben den gegenständlichen Initiativantrag am 13. Juni 2024 im Nationalrat eingebracht und wie folgt begründet:

„Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs:

Mit dieser Novelle des Sicherheitspolizeigesetzes (SPG) soll insbesondere sowohl der behördeninterne als auch der -externe Informationsaustausch im Rahmen der Strafrechtspflege an moderne Kommunikationsmöglichkeiten angepasst werden. So soll einerseits eine Rechtsgrundlage für einen gemeinsamen Aktenindex der Sicherheitsbehörden im Dienste der Strafrechtspflege geschaffen werden. Andererseits sollen die rechtlichen Voraussetzungen für die elektronische Kommunikation im Bereich der Strafrechtspflege für die Sicherheitsbehörden als Kriminalpolizei implementiert werden. Dadurch soll in Zukunft auch in diesem Bereich eine sichere elektronische Kommunikation zwischen den Sicherheitsbehörden und den Gerichten, Staatsanwaltschaften, Vollzugsbehörden sowie bestimmten sonstigen Teilnehmern am Strafverfahren stattfinden können.

Des Weiteren soll § 41 ergänzt und die Möglichkeit der Erlassung einer besonderen Durchsuchungsanordnung auch für Einrichtungen und Anlagen, die für gefährliche Angriffe gegen Leben oder Gesundheit einer größeren Zahl von Menschen als besonders anfällig zu erachten sind, geschaffen werden.

Außerdem wurden die Ausführungen des Verfassungsgerichtshofs in seinem Erkenntnis zu G72-74/2019, G181-182/2019 vom 11.12.2019 aufgegriffen, um – in Umsetzung der im aktuellen Regierungsprogramm vorgesehenen ‚Weiterentwicklung von Maßnahmen gegen Gewalt, Einbruch, Raub und Diebstahlsdelikte' – den polizeilichen Einsatz von bildverarbeitenden technischen Einrichtungen zum Kennzeichenabgleich für sicherheits- und kriminalpolizeiliche Fahndungszwecke im bestehenden verfassungsrechtlichen Rahmen wieder zu ermöglichen.

Um den Informationsfluss zu verbessern, soll es künftig möglich sein, zur Unterstützung bei der Koordination von Einsätzen Bild- und Tonmaterial in Echtzeit in die Landesleitzentralen bzw. das Lagezentrum des BMI zu übertragen.

Neben einer nach dem Vorbild der Strafprozessordnung vorgenommenen Anpassung von Auskunftsverlangen an die seit Inkrafttreten des neuen europäischen Datenschutzregimes bestehenden Erfordernisse und einer Verbesserung zur Klärung der Identität von Hilflosen soll zur Verwaltungsvereinfachung die Regelung hinsichtlich der örtlichen Zuständigkeit für die Kostenersatzpflicht bei sicherheitspolizeilichen Einsätzen präzisiert werden.

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich auf Art. 10 Abs. 1 Z 6 (‚Strafrechtswesen') und Z 7 (‚Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit') des Bundes-Verfassungsgesetzes – B-VG, BGBl. Nr. 1/1930.

Besonderer Teil

Änderung des Sicherheitspolizeigesetzes

Zu Z 1 und 2 (Inhaltsverzeichnis):

Es handelt sich um die erforderlichen Ergänzungen des Inhaltsverzeichnisses.

Zu Z 3 und 4 (§ 13a Abs. 2a und 4):

§ 13a ist jene Vorschrift, die für die Protokollierung und Dokumentation sämtlicher Tätigkeiten der Sicherheitsexekutive (‚Wahrnehmung gesetzlich übertragener Aufgaben') zur Anwendung gelangt, wobei durch § 13a Abs. 2 festgelegt ist, dass kriminalpolizeiliche Akten getrennt von Akten nach sonstigen Materiengesetzen geführt werden.

Die polizeiliche Protokollierung und Dokumentation ist nicht als gemeinsame Datenverarbeitung aller Sicherheitsbehörden ausgestaltet, sondern als lokal geführte Aktenverwaltung. Datenschutzrechtlich verantwortlich für die Datenverarbeitung ist stets die nach dem jeweiligen Materiengesetz zur Vollziehung örtlich zuständige Sicherheitsbehörde. Jede Sicherheitsbehörde hat somit grundsätzlich nur Einblick in die dem eigenen Zuständigkeitsbereich entspringenden Akten und Dokumentationen.

Diese lokale Form der Datenverarbeitung hat jedoch zur Folge, dass die Sicherheitsexekutive keinen gesamthaften Zugang zu Dokumentationsvorgängen zu einer bestimmten Person hat bzw. ein solcher – etwa aufgrund unterschiedlicher Schreibweisen von Namen – mangels ausreichender Datenrichtigkeit nicht mit der notwendigen Verlässlichkeit gegeben ist. Insbesondere im Bereich der Strafrechtspflege kann diese fehlende Verlässlichkeit nicht nur die Tätigkeit der Sicherheitsbehörden als Kriminalpolizei wesentlich erschweren, sondern etwa aufgrund von Verwechslungsgefahren die Rechte von Betroffenen beeinträchtigen.

Durch die gegenständliche Änderung soll nunmehr eine von den Sicherheitsbehörden als gemeinsam Verantwortliche geführte Datenverarbeitung (‚Aktenindex') geschaffen werden, um zu Zwecken der Datenrichtigkeit im Dienste der Strafrechtspflege die eindeutige Zuordnung von Aktenvorgängen zu einer bestimmten Person sicherzustellen. Dazu soll es zulässig sein, ausgewählte Daten zu Verdächtigen (§ 48 Abs. 1 Z 1 StPO), Beschuldigten (§ 48 Abs. 1 Z 2 StPO) und Verurteilten (§ 1 Z 2 StVG) im Rahmen eines Index verfügbar zu haben.

Mit der Einführung des Abs. 2a wird weder eine eigenständige Ermittlungsermächtigung geschaffen noch der direkte Zugriff auf den gesamten Akten- und Dokumentationsbestand der Sicherheitsbehörden ermöglicht. Vielmehr werden taxativ genannte Daten, die nach Abs. 2 bereits im Rahmen der Protokollierung und Dokumentation der Tätigkeiten der Sicherheitsexekutive als Kriminalpolizei verarbeitet werden, in einer als Aktenindex generierten Datenverarbeitung angezeigt. In diesem Sinne dürfen ausschließlich Namen, Geschlecht, frühere Namen, Aliasdaten, Staatsangehörigkeit, Geburtsdatum, Geburtsort, Wohnanschrift, bPK (§ 9 E-Government-Gesetz – E-GovG, BGBl. I Nr. 10/2004), Namen der Eltern, Grund des Einschreitens, Verwaltungsdaten sowie ein Hinweis auf bereits vorhandene, gemäß § 75 Abs. 1 verarbeitete erkennungsdienstliche Daten zu den abschließend genannten Betroffenenkreisen aus dem Aktenbestand in den Aktenindex übernommen werden. Durch die Verarbeitung des bPK ist eine eindeutige personenbezogene Zuordnung sichergestellt.

Der Bundesminister für Inneres übt die Funktion des Auftragsverarbeiters gemäß § 36 Abs. 2 Z 9 in Verbindung mit § 48 DSG aus. Rechten von Betroffenen (§§ 42 bis 45 DSG) ist im Sinne des § 51 Abs. 4 nachzukommen. Für Aktualisierungen gilt § 59 Abs. 1 zweiter und dritter Satz. Die Daten sind zu löschen, wenn der bezughabende Akt im Dienste der Strafrechtspflege (Abs. 2) zu löschen ist. Die Protokollierung der Verarbeitungsschritte im Aktenindex richtet sich gemäß Abs. 4 nach § 50 DSG. In Anbetracht der entsprechenden Anwendbarkeit von § 51 sowie des Datenschutzgesetzes gilt, dass bei der Verarbeitung nach § 13a Abs. 2a die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten sind (vgl. § 38 DSG) und besondere Kategorien personenbezogener Daten gemäß § 39 DSG nur verarbeitet werden dürfen, wenn dies zur Erfüllung der Aufgaben im Dienste der Strafrechtspflege unbedingt erforderlich ist.

Zu Z 5 (§ 13b samt Überschrift):

Nicht zuletzt die Corona-Pandemie hat im Bereich der sicherheitsbehördlichen Tätigkeiten den Bedarf eines verstärkten Einsatzes von elektronischen Kommunikationswegen aufgezeigt. Vor diesem Hintergrund bekannte sich die Bundesregierung im Rahmen des ‚Digital Austria Act für mehr Wohlstand, Sicherheit und neue Chancen durch Innovation' im Juni 2023 zur Notwendigkeit der Implementierung näherer Bestimmungen zur elektronischen Kommunikation der Sicherheitsbehörden als Kriminalpolizei im SPG (vgl. Vortrag an den Ministerrat 61/10 vom 1. Juni 2023). Zur Umsetzung dieser Maßnahme soll durch § 13b – nach dem Vorbild des für Gerichte und Staatsanwaltschaften eingerichteten justiziellen elektronischen Rechtsverkehrs gemäß Gerichtsorganisationsgesetz (GOG) – auch für die Sicherheitsbehörden als Kriminalpolizei eine Rechtsgrundlage für die sichere elektronische Kommunikation im Bereich der Strafrechtspflege geschaffen werden. Die §§ 89a Abs. 2 und 3, 89c Abs. 1 und 89d GOG sind dabei sinngemäß anzuwenden.

Gemäß Abs. 1 soll die elektronische Kommunikation im Bereich der Strafrechtspflege zwischen den Sicherheitsbehörden und den Gerichten, Staatsanwaltschaften, Vollzugsbehörden (§§ 11 und 13 StVG) sowie den in § 89c Abs. 5 GOG genannten Teilnehmern – etwa Rechtsanwältinnen und Rechtsanwälte sowie Verteidigerinnen und Verteidiger in Strafsachen – künftig im Wege des elektronischen Rechtsverkehrs erfolgen, sofern die technischen Möglichkeiten dafür bestehen.

Indem die elektronische Kommunikation nach Maßgabe der technischen Möglichkeiten erfolgen soll, ist es im Einzelfall auch zulässig, sonstige Übermittlungswege zuzulassen (vgl. in diesem Zusammenhang § 100 Abs. 2 StPO, wonach der Kriminalpolizei in der Berichterstattung derzeit die Wahl zwischen Schriftlichkeit oder automationsunterstützter Datenverarbeitung offensteht). Zudem gelten auch bei Ausübung von Rechten im elektronischen Rechtsverkehr einfachgesetzlich verankerte Beschränkungen, wie etwa für die Akteneinsicht nach der StPO (§§ 49 Abs. 2, 51 Abs. 2, 52 und 68 Abs. 1 StPO).

Im Übrigen gelten die §§ 1a und 25 Abs. 1 E-GovG sowie § 28 Abs. 3 ZustellG für den elektronischen Rechtsverkehr mit den Sicherheitsbehörden nach Maßgabe deren technischer Möglichkeiten.

Zu Z 6 (§ 41 samt Überschrift):

Im Zusammenhang mit der erhöhten Gefährdungslage um den Jahreswechsel hat sich zuletzt gezeigt, dass die bestehende Befugnis der Sicherheitsbehörden nach § 41 in der Praxis zu kurz greift. So verhindert die derzeitige Einschränkung der Geltungsdauer auf den Zeitraum der Abhaltung einer Großveranstaltung eine unter sicherheitspolizeilichen Gesichtspunkten unter Umständen angezeigte Absicherung der Veranstaltungsstätte vor und nach Abhaltung der Veranstaltung. Für andere Einrichtungen und Anlagen, die aufgrund gewisser Eigenschaften, wie etwa ihrer Lage oder Exponiertheit, besonders gefahrengeneigt für die Begehung gefährlicher Angriffe sind, fehlt eine entsprechende Befugnis derzeit gänzlich.

Vor diesem Hintergrund soll § 41 ergänzt und die Möglichkeit der Erlassung einer besonderen Durchsuchungsanordnung nicht nur – wie bislang – für Großveranstaltungen (Abs. 1 Z 1), sondern auch für Einrichtungen und Anlagen, die für gefährliche Angriffe gegen Leben oder Gesundheit einer größeren Zahl von Menschen – mithin etwa zehn (vgl. bspw. OGH RS0127943) – als besonders anfällig zu erachten sind (Abs. 1 Z 2), geschaffen werden. Die hierbei im Einzelfall ex-ante zu erstellende sicherheitspolizeiliche Gefährdungseinschätzung muss aufgrund des Vorliegens bestimmter Tatsachen die Annahme stützen, es werde bei einer Einrichtung oder Anlage zu nicht bloß vereinzelten Gewalttätigkeiten oder zu einer größeren Zahl gefährlicher Angriffe gegen Leben oder Gesundheit von Menschen kommen. Von nicht bloß vereinzelten Gewalttätigkeiten oder einer größeren Zahl gefährlicher Angriffe kann gesprochen werden, wenn Angriffe gegen eine größere Zahl von Menschen zu erwarten sind (vgl. *Huber-Lintner* in Thanner/Vogl [Hrsg.], Sicherheitspolizeigesetz[2] § 41 Anm. 4). In diesem Sinne kann eine Verordnung nach § 41 etwa auch aufgrund der Befürchtung eines einzelnen Bombenanschlags, durch den voraussichtlich etwa zehn Personen gefährdet würden, erlassen werden. In Ermangelung einer Beschränkung auf bestimmte Rechtsgüter rechtfertigen auch solche Gewalttätigkeiten, die sich gegen die Freiheit (z.B. Nötigung oder gefährliche Drohung) oder das Eigentum (z.B. Sachbeschädigung) von ca. zehn Personen richten, die Erlassung einer besonderen Durchsuchungsanordnung (vgl. *Huber-Lintner* in Thanner/Vogl [Hrsg.], Sicherheitspolizeigesetz[2] § 41 Anm. 4).

Die gewählte Formulierung der neuen Z 2 orientiert sich an § 38 Abs. 4 sowie § 39 Abs. 6, sodass insbesondere hinsichtlich der erfassten Schutzobjekte (Einrichtungen und Anlagen) weitgehend an die bestehende Rechtslage und deren Anwendungspraxis angeknüpft werden kann. Als besonders gefahrengeneigt können etwa Flughäfen, Bahnhöfe oder auch U-Bahn-Stationen und sonstige Einrichtungen oder Anlagen kritischer Infrastruktur (vgl. § 22 Abs. 1 Z 6) sowie deren unmittelbares Umfeld eingestuft werden. Ob Baulichkeiten vorhanden sind oder nicht, ist nicht entscheidend (vgl. auch *Keplinger*/*Pühringer*, Sicherheitspolizeigesetz[20] § 41 Anm. 4).

Bei Vorliegen einer entsprechenden Gefährdungseinschätzung ist die Sicherheitsbehörde ermächtigt, zeitlich und örtlich begrenzte Verordnungen zu erlassen, durch die der Zutritt zur erfassten Einrichtung oder Anlage von der Bereitschaft des Einzelnen, seine Kleidung und mitgeführte Behältnisse durchsuchen zu lassen, abhängig gemacht werden kann. Soll der Zutritt zur Einrichtung oder Anlage mit einem Fahrzeug erfolgen, ist der Zutritt auch von der Durchsuchung desselben abhängig zu machen. Mit dieser Durchsuchungsbefugnis ist – wie schon nach geltender Rechtslage – keine Befugnis zur Ermittlung personenbezogener Daten verbunden.

Verordnungen gemäß Abs. 1 dürfen – um die Verhältnismäßigkeit zu wahren – ausschließlich einzelfallbezogen und nur begrenzt auf den erforderlichen örtlichen sowie zeitlichen Umfang erlassen werden. Die Verordnung hat hierzu Tag und Uhrzeit ihres Inkrafttretens sowie den genauen örtlichen Umfang ihrer Geltung zu bestimmen. Sie ist aufzuheben, sobald eine Gefährdung nicht mehr zu befürchten ist, und tritt jedenfalls eine Woche nach ihrem Wirksamwerden außer Kraft. Die Verordnung ist in einer Weise kundzumachen, die sie möglichst allen Betroffenen zur Kenntnis bringt, insbesondere durch mediale Information beispielsweise unter Verwendung sozialer Medien und (mehrfachen) Aushang des Verordnungstextes im Umkreis der Einrichtung oder Anlage. Dabei erscheint auch eine rechtzeitige Information der Betreiber solcher Anlagen oder Einrichtungen über eine bevorstehende Maßnahme sinnvoll, um allenfalls erforderliche Vorkehrungen, etwa zur Lenkung von Besucherströmen oder durch Abstellen besonders geschulten Personals, treffen zu können.

Die Durchsuchung nach § 41 kann auch weiterhin nur bei Einwilligung des Betroffenen erfolgen. Bei Verweigerung der Durchsuchung kann der Zutritt oder die Zufahrt zur Veranstaltungsstätte, Einrichtung oder Anlage jedoch verwehrt werden, wobei dieser Ausschluss auch zwangsweise durchgesetzt werden kann (§ 50). Ein Anspruch auf Erstattung eines allfälligen für den Eintritt oder die Beförderung bezahlten Ticketpreises (etwa bereits erworbene Zutrittskarten, Flug-, Bus- oder Bahntickets) gegenüber dem Bund besteht nicht. Allfällige Amtshaftungsansprüche nach Art. 23 B-VG bleiben davon unberührt.

Zu Z 7 (§ 53 Abs. 3a):

Seit Inkrafttreten des neuen europäischen Datenschutzregimes können sogenannte ‚WHOIS'-Anfragen nicht mehr auf § 53 Abs. 4 gestützt werden, da der Name und die Erreichbarkeitsdaten eines Homepage-Betreibers über die Registrierungsstelle (‚Nic.at') nicht mehr öffentlich (im Internet) zugänglich sind. Für die sicherheitspolizeiliche Aufgabenerfüllung ist es aber erforderlich, im Anlassfall (etwa Ankündigung eines gefährlichen Angriffs oder eines Suizids in einem Online-Forum) die Daten eines Homepage-Betreibers bei der Registrierungsstelle zu erfragen, um in weiterer Folge vom zuständigen Betreiber die IP-Adresse (§ 53 Abs. 3a Z 2) sowie Name und Anschrift des IP-Adressen-Benutzers (§ 53 Abs. 3a Z 3) in Erfahrung zu bringen. Die Bestimmung soll diesbezüglich an die korrespondierende Bestimmung in der StPO (§ 134a Abs. 1a StPO) sowie an die terminologischen Änderungen aufgrund der Neuerlassung des Telekommunikationsgesetzes (Telekommunikationsgesetz 2021 – TKG 2021, BGBl. I Nr. 190/2021) angepasst werden.

Zu Z 8 (§ 53 Abs. 3b):

Mit der Änderung in Abs. 3b soll eine Anpassung an die korrespondierende Bestimmung in der StPO (§ 134 Z 2a StPO) erfolgen, in der mit BGBl. I Nr. 27/2018 eine Legaldefinition zur Lokalisierung einer technischen Einrichtung eingeführt wurde. Durch die Einführung einer Legaldefinition sollte klargestellt werden, dass es sich bei der Lokalisierung einer technischen Einrichtung um den Einsatz technischer Mittel zur Feststellung von geografischen Standorten und der zur internationalen Kennung des Benutzers dienenden Nummer (IMSI) ohne Mitwirkung des Anbieters (oder sonstigen Diensteanbieters) handelt. Diese Klarstellung soll nunmehr auch für den Bereich der Sicherheitspolizei (SPG, SNG) nachgezogen werden, um eine klare Rechtsgrundlage zur – für eine effektive Gefahrenabwehr unabdingbaren – präzisen Ortung innerhalb einer Funkzelle sowie der Feststellung der IMSI-Nummer zu schaffen. So kann etwa im Falle einer Geiselnahme die Ermittlung der IMSI-Nummer weitere Ermittlungsschritte wie insbesondere die Erhebung der Telefonnummer (nach § 53 Abs. 3a Z 1 oder § 11 Abs. 1 Z 5 SNG) ermöglichen.

Zu Z 9 (§ 53a Abs. 5):

§ 53a Abs. 1 stellt die Rechtsgrundlage für die von den Sicherheitsbehörden geführten (lokalen) Datenverarbeitungen (z.B. Einsatzleitsysteme) dar, die der Leitung, Administration und Koordination von Einsätzen dienen. Von mehreren Sicherheitsbehörden als gemeinsam Verantwortliche können solche Datenverarbeitungen gemäß Abs. 5 geführt werden, wenn dies wegen eines sprengelübergreifenden Einsatzes erforderlich ist. Durch die Ausweitung des Zwecks des Abs. 5 auf die Unterstützung bei der Koordination von Einsätzen wird der Umstand berücksichtigt, dass der Zweck des Abs. 1 bzw. des § 58e Abs. 1 auch in § 53a Abs. 5 seinen Niederschlag finden soll und insbesondere das im Bundesministerium

für Inneres eingerichtete Lagezentrum für diese Zwecke Daten gemeinsam mit den lokalen Sicherheitsbehörden verarbeiten darf.

Zu Z 10, 16 und 18 (§ 54 Abs. 4b und § 91c):

Der Einsatz von Kennzeichenerkennungsgeräten als Instrument der Fahndung wurde mit der SPG-Novelle 2005 erstmals ins SPG eingeführt (§ 54 Abs. 4b idF BGBl. I Nr. 151/2004) und die Sicherheitsbehörden ermächtigt, Kennzeichenerkennungsgeräte verdeckt zum Einsatz zu bringen, um Kennzeichen-Daten für Zwecke der Fahndung (§ 24) mit dem Fahndungsdatenbestand abzugleichen. Die Erfahrungen seit der Einführung der Kennzeichenerkennungsgeräte im Jahr 2005 haben gezeigt, dass es für die Anhaltung der Fahrzeuge im Trefferfall unbedingt erforderlich ist, über das Kennzeichen hinausgehende Informationen zum Fahrzeug, insbesondere zur Fahrzeugmarke, Fahrzeugtype und Fahrzeugfarbe, zu erhalten, um eine verlässliche Identifizierung des Fahrzeuges im fließenden Straßenverkehr durch die Organe des öffentlichen Sicherheitsdienstes zu ermöglichen. Die Novellierung des § 54 Abs. 4b im Jahr 2018 durch BGBl. I Nr. 29/2018 führte dazu, dass die Sicherheitsbehörden ermächtigt waren, bildverarbeitende technische Einrichtungen zum Einsatz zu bringen, die in der Lage waren, Daten zur Identifizierung von Fahrzeugen, insbesondere Kennzeichen, Type, Marke sowie Farbe des Fahrzeuges, und von Fahrzeuglenkern für Zwecke der Fahndung zu ermitteln. Zudem erlaubte § 54 Abs. 4b idF BGBl. I Nr. 29/2018 den Sicherheitsbehörden, die mittels bildverarbeitenden technischen Einrichtungen ermittelten Daten für die Dauer von höchstens zwei Wochen ab Ermittlung zu speichern: Wurden davor sämtliche erfassten Kennzeichendaten, die im Zeitpunkt des Abgleichs mit dem Fahndungsdatenbestand keinen Treffer ergaben, unverzüglich gelöscht, ermöglichte § 54 Abs. 4b idF BGBl. I Nr. 29/2018 diese Daten für bis zu zwei Wochen zu speichern, damit die Sicherheitsbehörden bei Bestehen einer der in § 54 Abs. 4b idF BGBl. I Nr. 29/2018 genannten Aufgaben auf diese mittels Abgleich mit einem gesuchten KFZ-Kennzeichen zugreifen konnten.

Mit dem Erkenntnis zu G72-74/2019, G181-182/2019 vom 11.12.2019 hat der VfGH § 54 Abs. 4b idF BGBl. I Nr. 29/2018 aufgehoben. In der Begründung seines Erkenntnisses führte der VfGH aus, dass sich die Ermächtigung zur Datenerfassung und Datenspeicherung im Hinblick auf deren Bedingungen sowie die Art und den Umfang der zu ermittelnden Daten als zu weitgehend erweist.

Die Neuerlassung des § 54 Abs. 4b dient der Umsetzung der im Regierungsprogramm (Regierungsprogramm 2020 – 2024, S 217) vorgesehenen ‚Weiterentwicklung von Maßnahmen gegen Gewalt, Einbruch, Raub und Diebstahlsdelikte'. Die Sicherheitsbehörden sollen in Übereinstimmung mit dem Erkenntnis des VfGH ermächtigt werden, verdeckt mittels Einsatz von bildverarbeitenden technischen Einrichtungen Daten zur Identifizierung von Fahrzeugen, insbesondere das KFZ-Kennzeichen sowie Type, Marke und Farbe des Fahrzeuges, für Zwecke der sicherheits- und kriminalpolizeilichen Fahndung zu verarbeiten. Der Umfang der Datenerfassung ist ausdrücklich auf fahrzeugbezogene Daten eingeschränkt und betrifft ausschließlich die für die Ermittlung erforderlichen Daten. Die demonstrative Aufzählung der – im Hinblick auf die Identifizierung des Fahrzeuges – relevantesten Fahrzeugdaten dient daher lediglich der Konkretisierung der Ermittlungsermächtigung.

Diese Regelung soll es den Sicherheitsbehörden ermöglichen, gesuchte Fahrzeuge zu erkennen, zu identifizieren und als gefahndet zu verifizieren. Bei den bildverarbeitenden technischen Einrichtungen handelt es sich um spezielle Bildverarbeitungsgeräte (Kamera- und Computersysteme), die in der Lage sind, zur Identifizierung von Fahrzeugen, insbesondere das KFZ-Kennzeichen sowie Type, Marke und Farbe von stehenden bzw. sich in Bewegung befindlichen Fahrzeugen für die Zwecke der sicherheits- und kriminalpolizeilichen Fahndung auszulesen. Der automatische und nahezu zeitgleiche Abgleich mit Daten aus nationalen und internationalen Fahndungsevidenzen (vgl. etwa § 53 Abs. 1 Z 5 iVm § 24 Abs. 2 SPG, § 57 Abs. 2 SPG, § 8a PolKG, §§ 33 ff EU-PolKG) ist nur anhand der mittels bildverarbeitender technischer Einrichtungen ausgelesenen KFZ-Kennzeichen zulässig. Abfragekriterium in der Fahndungsevidenz ist somit lediglich das Kennzeichen des Fahrzeuges. Nur im Falle einer Übereinstimmung (‚Treffer') zwischen dem erfassten Kennzeichen und einem in einer nationalen oder internationalen Fahndungsevidenz gespeicherten Kennzeichen dürfen die mittels bildverarbeitenden technischen Einrichtungen ermittelten Daten weiterverarbeitet werden. Andernfalls sind die ermittelten Daten automatisch und sofort zu löschen. Eine von einem Trefferfall losgelöste Erlaubnis, die durch den Einsatz bildverarbeitender technischer Einrichtungen ermittelten Daten für einen bestimmten Zeitraum ab Ermittlung zu speichern, wie sie § 54 Abs. 4b idF BGBl. I Nr. 29/2018 noch enthielt, ist in der Neuregelung nicht vorgesehen.

Anders als § 54 Abs. 4b idF BGBl. I Nr. 29/2018 ermächtigt die Neuregelung nicht zur Ermittlung von Lichtbildern von Personen im Fahrzeug bzw. im Nahbereich des Fahrzeuges. Da die bildgebende Erfassung von Personen beim Einsatz bildverarbeitender Einrichtungen aber technisch nicht ausgeschlossen werden kann, ist technisch dafür Vorsorge zu treffen, dass allenfalls erfasste Personen

ohne unnötigen Verzug in nicht rückführbarer Weise unkenntlich gemacht werden, noch bevor das in Rede stehende Bild den Organen des öffentlichen Sicherheitsdienstes zur Kenntnis gelangt (vgl. zur korrespondierenden Regelung in der StVO § 98a Abs. 3 leg.cit.).

Neben dem ohnehin geltenden Verhältnismäßigkeitsgrundsatz gemäß § 51 Abs. 1 iVm § 29, aus dem sich ergibt, dass der Einsatz bildverarbeitender technischer Einrichtungen zu beenden ist, wenn dieser zur Aufgabenerfüllung nicht mehr erforderlich ist, sieht die Neuregelung in bestimmten Fällen eine zusätzliche Verhältnismäßigkeitsprüfung vor. Findet der Einsatz innerhalb einer Woche insgesamt länger als 72 Stunden an derselben Örtlichkeit statt (stationärer Einsatz), ist dieser ausschließlich entlang der vom internationalen Durchzugsverkehr benützten Verkehrswege (vgl. den Wortlaut des § 35 Abs. 1 Z 7) oder nach Durchführung einer ortsbezogenen Risikoanalyse, die auf sicherheits- und kriminalpolizeilichen Erkenntnissen, wie etwa vermehrte Eigentumskriminalität an einer bestimmten Örtlichkeit, beruht, zulässig. Der Standort bzw. das Ergebnis der durchgeführten Risikoanalyse ist diesfalls dem Rechtsschutzbeauftragten in der Meldung gem. § 91c Abs. 1 mitzuteilen. Die ortsbezogene Risikoanalyse gilt längstens sechs Wochen. Sofern in Anbetracht des fortbestehenden Risikopotentials ein weiterer stationärer Einsatz an derselben Örtlichkeit erforderlich erscheint, ist – auch unter Berücksichtigung der innerhalb des bisherigen Einsatzzeitraumes gewonnenen Erkenntnisse – eine erneute Risikoanalyse durchzuführen und der Rechtsschutzbeauftragte nach § 91c Abs. 1 zu informieren.

Der Einsatz bildverarbeitender technischer Einrichtungen unterliegt als verdeckte Ermittlungsmaßnahme gemäß § 91c der Kontrolle durch den Rechtsschutzbeauftragten beim Bundesminister für Inneres (§ 91a). Grundsätzlich soll der Rechtsschutzbeauftragte im Rahmen des neu zu schaffenden § 91c Abs. 3 von der geplanten erstmaligen Inbetriebnahme bildverarbeitender technischer Einrichtungssyteme gemäß § 54 Abs. 4b verständigt werden. Die Information vor der erstmaligen Inbetriebnahme soll dem Rechtsschutzbeauftragten die Möglichkeit geben, die Datenverarbeitung durch diese Einrichtungen, insbesondere die nicht rückführbare Unkenntlichmachung allenfalls erfasster Personen sowie die umgehende und automatische Löschung iSd § 54 Abs. 4b letzter Satz, vorab zu prüfen. Die erstmalige Inbetriebnahme der technischen Einrichtungssysteme ist erst nach Ablauf der in § 91c Abs. 3 ausdrücklich für den Anwendungsfall des § 54 Abs. 4b vorgesehenen zweiwöchigen Äußerungsfrist oder einer entsprechenden Äußerung des Rechtsschutzbeauftragten zulässig. Bei nicht bloß unerheblichen Änderungen der technischen Funktionsweise der Datenverarbeitung, wie insbesondere der Art der Datenerfassung, ist der Rechtsschutzbeauftragte erneut gemäß § 91c Abs. 3 zu befassen.

Beim stationären Einsatz bildverarbeitender technischer Einrichtungen soll der Rechtsschutzbeauftragte außerdem von den Sicherheitsbehörden in Kenntnis gesetzt werden, sobald feststeht, dass der Einsatz innerhalb einer Woche insgesamt länger als 72 Stunden stattfinden wird (§ 91c Abs. 1). Die Information über den erfolgten stationären Einsatz von bildverarbeitenden Einrichtungen soll es dem Rechtsschutzbeauftragten ermöglichen zu prüfen, ob neben den allgemeinen in § 54 Abs. 4b genannten Voraussetzungen auch die für einen stationären Einsatz dieser Einrichtungen zusätzlichen Voraussetzungen – Einsatz auf vom internationalen Durchzugsverkehr benützten Verkehrswegen bzw. nach Durchführung einer den Einsatz begründenden ortsbezogenen Risikoanalyse – tatsächlich vorlagen.

Davon unberührt bleiben die sonstigen Rechte und Pflichten des Rechtsschutzbeauftragten nach § 91d, insbesondere die jederzeitige Überwachung der Durchführung der in § 91c genannten Maßnahmen und der Einhaltung der Löschungsbestimmungen sowie die Erhebung einer Beschwerde an die Datenschutzbehörde.

Zu Z 11, 12 und 14 (§§ 57 Abs. 3, 58 Abs. 3 und 63 Abs. 3):

Mit dem Erkenntnis zu G72-74/2019, G181-182/2019 vom 11.12.2019 hat der VfGH § 57 Abs. 2a aufgehoben. Die diesbezüglichen Verweise in § 57 Abs. 3, § 63 Abs. 3 sowie § 58 Abs. 3 haben deshalb zu entfallen.

Zu Z 13 (§ 58e Abs. 2a):

Zur Verbesserung des Informationsflusses soll der neu eingefügte § 58e Abs. 2a die Sicherheitsbehörden künftig ermächtigen, Bild- und Tondaten, die diese zulässigerweise im Bereich der Sicherheitsverwaltung bzw. als Kriminalpolizei ermitteln, in Echtzeit an die bei den Landespolizeidirektionen (LPD) angesiedelten Landesleitzentralen und an das Lagezentrum des BMI zu übermitteln.

Durch die Änderung soll es ermöglicht werden, dass die Landesleitzentralen der LPD bzw. das Lagezentrum im BMI unmittelbar Informationen über laufende (Groß-)Einsätze erhalten, wenn dies zur Wahrnehmung ihrer Aufgabe der Unterstützung bei der Koordinierung von Einsätzen erforderlich ist. Dabei sind unter Einsätzen – neben den bereits im Gesetzestext demonstrativ aufgezählten sicherheitspolizeilichen Schwerpunktaktionen (etwa Geisellagen, Großeinsätze im Katastrophenfall oder

bei Staatsbesuchen sowie sonstige Schwerpunktaktionen) und ordnungsdienstlichen Anlässen (vgl. § 53a Abs. 1) – auch sonstige besondere Lagen zu verstehen.

Übermittelt werden nur Bild- und Tondaten, welche die Sicherheitsbehörden zur Aufgabenerfüllung im Rahmen der Sicherheitsverwaltung (z.B. Videoüberwachungen nach § 54 oder § 12 Abs. 2 GrekoG) und der Kriminalpolizei (§ 136 Abs. 1 Z 1 oder § 149 Abs. 1 Z 1 StPO) als datenschutzrechtlich Verantwortliche rechtmäßig ermitteln. Bild- und Tondaten, welche die Sicherheitsbehörden auf Grundlage der StVO (z.B. durch Verkehrskameras) ermitteln, sind daher davon nicht umfasst.

Bild- und Tondaten dürfen ausschließlich in Echtzeit übermittelt werden. Das bedeutet, sie dürfen beim Empfänger nicht aufgezeichnet werden. Diese Einschränkung trägt dem Umstand Rechnung, dass die Echtzeitübertragung im Vergleich zur Datenspeicherung das gelindere Mittel (Grundsatz der Datenminimierung) und damit einen geringeren Eingriff in das Grundrecht auf Datenschutz darstellt.

Zu Z 15 (§ 75 Abs. 1):

Im Falle der Identitätsfeststellung einer hilflosen Person gemäß § 35 Abs. 1 Z 3 kann bei Vorliegen der entsprechenden Voraussetzungen eine erkennungsdienstliche Behandlung gemäß § 65 Abs. 3 durchgeführt werden. Unmittelbar nach Erhebung der Daten ist gemäß § 75 Abs. 2 eine Abfrage dieser Daten in der zentralen erkennungsdienstlichen Evidenz (§ 75 Abs. 1 und 1a) zulässig, um einen Hinweis zur Klärung der Identität zu erhalten. Seit dem Wegfall der (lokalen) erkennungsdienstlichen Evidenzen nach § 70 in der Fassung vor BGBl. I Nr. 29/2018 können erkennungsdienstliche Daten hilfloser Personen – anders als jene von Leichen gemäß § 66 Abs. 1 – nicht mehr (weder lokal noch zentral) gespeichert werden. Die weitere Speicherung dieser Daten ist jedoch erforderlich, um die Identität der hilflosen Person auch im Falle einer erst später erfolgenden Abgängigkeitsanzeige klären zu können. Durch die gegenständliche Änderung soll daher (wieder) die Möglichkeit geschaffen werden, gemäß § 65 Abs. 3 iVm § 35 Abs. 1 Z 3 ermittelte erkennungsdienstliche Daten hilfloser Personen zu speichern, wenn die erstmalige Abfrage nach § 75 Abs. 2 zu einem negativen Ergebnis geführt hat. Die gespeicherten Daten sind wie bisher gemäß § 73 Abs. 1 Z 6 zu löschen, sobald sie ihre Funktion für den Anlassfall erfüllt haben, das heißt, die Identität der hilflosen Person festgestellt werden konnte.

Zu Z 17 (§ 91c Abs. 2):

Um aus Gründen des Datenschutzes dem Rechtsschutzbeauftragten eine eingehende Prüfung von Überwachungen öffentlicher Orte mit Bild- und Tonaufzeichnungsgeräten iSd § 54 Abs. 6 bis 7a sowie von Datenverarbeitungen gemäß § 53a Abs. 2 und 6 zu ermöglichen, soll die dem Rechtsschutzbeauftragten zukommende Gelegenheit zur Äußerung auf drei Werktage festgelegt werden, wobei Samstage nicht als Werktage gelten. Der tatsächliche Einsatz der Bild- und Tonaufzeichnungsgeräte oder die Aufnahme der Datenverarbeitung darf weiterhin erst nach Ablauf dieser Frist oder Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten erfolgen.

Zu Z 19 (§ 92a Abs. 2):

Neben einer redaktionellen Anpassung dient die Änderung der Verwaltungsvereinfachung. Die örtliche Zuständigkeit für Vorschreibungen von Kostenersätzen gemäß § 92a Abs. 1 oder 1a soll sich nach dem Ort des Einschreitens richten. Werden dabei Amtssprengel (§ 14 Abs. 1) überschritten, richtet sich die Zuständigkeit nach dem Ort, an welchem das Einschreiten begonnen hat.

Zu Z 20 (§ 94 Abs. 56):

Es handelt sich um die Inkraft- bzw. Außerkrafttretensbestimmung.“

Der Ausschuss für innere Angelegenheiten hat den gegenständlichen Initiativantrag in seiner Sitzung am 19. Juni 2024 in Verhandlung genommen. An der Debatte beteiligten sich außer dem Berichterstatter Abgeordneten Mag. Georg **Bürstmayr** die Abgeordneten Dr. Stephanie **Krisper**, Christian **Ries** und Ing. Reinhold **Einwallner** sowie der Bundesminister für Inneres Mag. Gerhard **Karner**.

Bei der Abstimmung wurde der Gesetzentwurf mit Stimmenmehrheit (**dafür:** V, G, **dagegen:** S, F, N) beschlossen.

Als Ergebnis seiner Beratungen stellt der Ausschuss für innere Angelegenheiten somit den **Antrag**, der Nationalrat wolle dem **angeschlossenen Gesetzentwurf** die verfassungsmäßige Zustimmung erteilen.

Wien, 2024 06 19

Mag. Georg Bürstmayr	**Dr. Christian Stocker**
Berichterstattung	Obmann

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-06-20T13:18:15+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	