ULD · Postfach 71 16 · 24171 Kiel

Innenministerium
des Landes Schleswig-Holstein
Herrn Wiezorek, IV 411

nur per E-Mail
ronald.wiezorek@im.landsh.de

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Barbara Körffer
Durchwahl: 988-1216

Aktenzeichen:
LD5-74.03/99.118

Kiel, 18. März 2013

Gesetzentwurf zur Änderung des Landesverwaltungsgesetzes und des Landesverfassungsschutzgesetzes - Anpassung des manuellen Abrufs der Bestandsdaten nach dem Telekommunikationsgesetz an die verfassungsrechtlichen Vorgaben

Sehr geehrter Herr Wiezorek,

ich bedanke mich für die Übersendung des oben bezeichneten Gesetzentwurfs und die Gelegenheit zur Stellungnahme.

Zu dem Entwurf ist aus unserer Sicht Folgendes anzumerken:

I. Zu Artikel 1 - Änderung des Landesverwaltungsgesetzes

Insgesamt enthält der Entwurf - im Vergleich zu dem Gesetzentwurf des Bundes zur Änderung der Strafprozessordnung, des Bundeskriminalamtsgesetzes und anderer Gesetze zur Anpassung an die verfassungsrechtlichen Vorgaben - eine Reihe von Grundrechtssicherungen, die aus unserer Sicht zu begrüßen sind. Dazu gehört vor allem die vorgesehene Vorlage der Auskunftsersuchen über den Inhaber einer IP-Adresse sowie über Zugangssicherungscodes beim zuständigen Amtsgericht sowie die Einführung einer Benachrichtigung der Betroffenen über diese Maßnahmen. Beide Vorkehrungen tragen dem Umstand Rechnung, dass es sich bei den zu Grunde liegenden Maßnahmen um gewichtige Grundrechtseingriffe handelt, die wesentlich schwerer wiegen als die bloße Bestandsdatenabfrage. Die Zuordnung dynamischer IP-Adressen zu deren Nutzern setzt eine Analyse der Verkehrsdaten voraus und greift daher in Artikel 10 GG ein, wie das Bundesverfassungsgericht in seiner Entscheidung vom 24. Januar 2012 ausdrücklich klargestellt hat (BVerfG vom 24.1.2012 - 1 BvR 1299/05 - Absatz-Nr. 120). Ähnlich ist die Auskunft über Zugangssicherungscodes wie PIN, PUK oder Passwörter zu bewerten. Diese Angaben selbst mögen zwar Bestandsdaten sein. Sie dienen der Polizei aber dazu, sich Kenntnis von weiteren Daten zu verschaffen.

Diese weiteren Daten sind üblicherweise Verkehrs- und Inhaltsdaten über bereits abgeschlossene Telekommunikationsvorgänge. Als solche unterfallen sie zwar nicht unmittelbar dem Schutz des Artikel 10 GG (BVerfG vom 2.3.2006 - 2 BvR 2099/04 - Absatz-Nr. 72 ff.). Sie sind vom Schutzbereich des Rechts auf informationelle Selbstbestimmung umfasst. Die Erhebung dieser Daten stellt aber regelmäßig einen schwerwiegenden Eingriff in dieses Grundrecht dar. Denn hierdurch können zum einen der Umfang der Kommunikationsbeziehungen sowie die näheren Umstände der Kommunikation, oftmals für einen weitreichenden Zeitraum, erschlossen werden. Zum anderen können Inhalte abgeschlossener Kommunikation erfasst werden, die mit dem Kommunikationspartner in der Annahme der Vertraulichkeit der Kommunikation ausgetauscht wurden und die höchstpersönliche Bereiche betreffen können. Angesichts dieser Eingriffsintensität sind beide Maßnahmen deutlich von der reinen Bestandsdatenabfrage zu unterscheiden. Die vorgesehene gerichtliche Befassung und die Benachrichtigung der Betroffenen sind grundsätzlich geeignete Mittel, um den Schutz für die Betroffenen zu erhöhen.

Zu § 180a Abs. 1 Nr. 2 LVwG-E

Mit der vorgesehenen Ermächtigung, die Bestandsdaten auch für die *Verhütung* zu erwartender Schäden für die genannten Rechtsgüter abzufragen, wird eine neue Kategorie einer Gefahr eingeführt, die es bislang im LVwG nicht gibt. Das LVwG sieht bislang nur die Kategorien „Gefahr“ und „Verhütung von Straftaten“ vor. Während die Bezugnahme auf die Gefahr Maßnahmen der klassischen Gefahrenabwehr beschreibt, erweitern die Vorschriften zur Verhütung von Straftaten das polizeiliche Handeln um Maßnahmen, die bereits im Vorfeld einer Gefahr getroffen werden können. Wie sich die im Entwurf vorgesehene neue Kategorie in dieses Spektrum einordnet, geht aus Gesetzestext und Begründung nicht eindeutig hervor. Insofern bestehen Zweifel an der Bestimmtheit dieser Regelung.

Es bestehen darüber hinaus Zweifel an deren Verhältnismäßigkeit. Dabei ist zu bedenken, dass die neue Befugnis nicht nur für die reinen Bestandsdaten gelten soll. Durch den Verweis in Absatz 3 soll auch die Anfrage nach dem Inhaber einer dynamischen IP-Adresse im Gefahrenvorfeld erlaubt werden. Die Erforderlichkeit für die Vorverlagerung des Eingriffs wird in der Entwurfsbegründung nicht dargelegt. Damit kann die Verhältnismäßigkeit der Maßnahme nicht festgestellt werden. Der bloße Verweis auf den Schutz gewichtiger Rechtsgüter reicht für sich allein nicht aus. Erforderlich wäre der Nachweis eines tatsächlichen Bedarfs für solche Auskünfte. Dies gilt umso mehr als die Bestandsdatenabfrage unter Nutzung dynamischer IP-Adressen kein geringer Grundrechtseingriff ist und damit insoweit nicht von vornherein von einem Übergewicht der zu schützenden Rechtsgüter gegenüber dem beeinträchtigten Rechtsgut ausgegangen werden kann. Hervorzuheben ist vor allem, dass es sich bei der Bestandsdatenabfrage unabhängig von einer Gefahr im klassischen Sinne um eine neue Maßnahme handelt, die es im geltenden Recht nicht gibt. Die bislang für Bestandsdatenabfragen geltende Regelung des § 113 TKG knüpft die Maßnahme an das Vorliegen einer Gefahr für die öffentliche Sicherheit. Das Bundesverfassungsgericht hat seiner Bewertung der Bestandsdatenauskunft nach § 113 Abs. 1 Satz 1 TKG als grundsätzlich verhältnismäßig ausdrücklich zu Grunde gelegt, dass nach dieser Regelung die Bestandsdatenauskunft nur für die Gefahrenabwehr im Sinne einer „konkreten“ Gefahr und nicht für die Gefahrenvorsorge zugelassen ist (so ausdrücklich BVerfG vom 24. Januar 2012 - 1 BvR 1299/05 - Absatz-Nr. 177).

Insgesamt gilt für die Eingriffsschwellen, dass hier eine Differenzierung zwischen der reinen Bestandsdatenabfrage und der Ermittlung des Inhabers einer dynamischen IP-Adresse vor-

genommen werden sollte. Da die letztgenannte Maßnahme von höherer Eingriffsintensität ist, sollte hierfür auch die Eingriffsschwelle höher liegen.

Zu § 180a Abs. 2 LVwG-E

Zu begrüßen ist, dass der Entwurf die Maßnahmen im Einzelnen benennt, für die die mittels PIN, PUK oder Passwörtern zu erschließenden Daten genutzt werden dürfen. Aus welchem Grund der Entwurf diese Maßnahmen allerdings nur beispielhaft („insbesondere“) und nicht abschließend benennt, ist nicht ersichtlich. Aus der Begründung ergibt sich kein Hinweis darauf, dass die gespeicherten Daten auf anderem Wege als über eine Sicherstellung nach § 210 LVwG oder unter den Voraussetzungen der Telekommunikationsüberwachung genutzt werden sollen. Die Erforderlichkeit für eine Öffnung im Gesetzestext für andere Maßnahmen ist daher nicht dargelegt. Im Interesse einer bestimmten Regelung sollte der Gesetzgeber sorgfältig prüfen, unter welchen Voraussetzungen die auf Endgeräten gespeicherten Daten genutzt werden dürfen und diese abschließend im Gesetz benennen. Ggf. reicht es dafür aus, das Wort „insbesondere“ in § 180a Abs. 2 LVwG-E zu streichen.

Zu § 180b Abs. 2 LVwG-E

Die vorgesehene Mitteilung der polizeilichen Anordnung an das zuständige Amtsgericht ist wie oben bereits festgestellt, grundsätzlich zu begrüßen. Hierbei handelt es sich offenbar nicht um eine gerichtliche Anordnung der Maßnahme, sondern um eine nachträgliche Bestätigung oder Verwerfung der vom Behördenleiter angeordneten Maßnahme. Da die Auskunft regelmäßig innerhalb einer kurzfristigen Zeitspanne erlangt werden kann, ist davon auszugehen, dass die Polizei die ersuchten Daten im Regelfall bereits erhoben hat, bevor das Gericht über die Zulässigkeit der Maßnahme entscheidet. Ein vorbeugender Grundrechtsschutz wird durch dieses Verfahren kaum erreicht werden können.

Wir raten daher, die Mitwirkung des Gerichts als echte Anordnung des Gerichts auszugestalten.

Sofern die Regelung unverändert bleibt, ist sie ergänzungsbedürftig. Soll die gerichtliche Befassung überhaupt einen nennenswerten Mehrwert haben, muss sie zwingend durch ein Verwendungsverbot für den Fall der Feststellung der Unzulässigkeit der Maßnahme durch das Gericht flankiert werden. Andernfalls bliebe die gerichtliche Feststellung der Unzulässigkeit in vielen Fällen folgenlos.

Zu § 185a Abs. 2 Nr. 2 LVwG

Wir raten dringend dazu, den Verweis in § 185a Abs. 2 Nr. 2 LVwG auf den seit der Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 nichtigen § 113a TKG zu streichen. Gegenwärtig läuft dieser Verweis lediglich ins Leere. Da es sich um einen dynamischen Verweis handelt, ist er gleichzeitig aber auch ein Blankett-Platzhalter für einen neuen § 113a TKG, der automatisch wirksam wird, sobald eine gültige Neuregelung im TKG in Kraft tritt. Der Inhalt eines künftigen § 113a TKG ist für den schleswig-holsteinischen Gesetzgeber in keiner Weise absehbar, zumal die Vorratsdatenspeicherung seit Jahren Gegenstand politischer und rechtlicher Auseinandersetzungen auf Ebene der Länder, des Bundes und der EU ist. Ob die Bezugnahme auf eine Neuregelung im TKG vom Willen des Landesgesetzgebers getragen ist

und der Verweis auf eine spätere Neuregelung dem Parlamentsvorbehalt genügt, ist daher äußerst fraglich.

II. Zu Artikel 2 - Änderung des Landesverfassungsschutzgesetzes

Der Entwurf differenziert hinsichtlich der einzelnen Maßnahmen lediglich im Hinblick auf die Mitwirkung der G10-Kommission und der Einführung von Benachrichtigungspflichten. Im Übrigen werden die reine Bestandsdatenabfrage und die Abfrage über den Inhaber einer dynamischen IP-Adresse gleich behandelt. Aus den oben genannten Gründen sollte hier eine differenzierte Regelung getroffen werden, die der unterschiedlichen Eingriffsintensität Rechnung trägt.

Die Beteiligung der G10-Kommission bei den Auskunftsersuchen unter Nutzung dynamischer IP-Adressen und über Zugangssicherungscodes ist zu begrüßen. Es sollte geprüft werden, ob hierfür auch eine Änderung des § 26a Abs. 1Nr. 2 LVerfSchG erforderlich ist.

Darüber hinaus sollte über diese Maßnahmen auch das Parlamentarische Kontrollgremium unterrichtet werden. Auskunftsersuchen unter Nutzung von dynamischen IP-Adressen berühren den Schutzbereich des Art. 10 GG. Auskunftsersuchen über Zugangssicherungscodes stellen regelmäßig eine Vorstufe zu Maßnahmen dar, die ihrerseits den Schutzbereich des Art. 10 GG berühren können. Daher ist eine Benachrichtigung des Parlamentarischen Kontrollgremiums auch über diese Maßnahmen angezeigt.

Zu § 8a Abs. 2 LVerfSchG

Auch diese Regelung enthält in Satz 2 einen Verweis auf die nichtige Vorschrift des § 113a TKG über die Vorratsdaten. Aus den oben genannten Gründen sollte dieser Verweis gestrichen werden.

Mit freundlichen Grüßen

Barbara Körffer