Wortprotokoll Ständerat vom 7. Dezember 2015

7. Dezember 2015

Ständerat - Wintersession 2015 - Fünfte Sitzung - 07.12.15-15h15

13.025

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Änderung, Differenzen

Engler Stefan (C, GR), für die Kommission: Wir beraten also die Differenzen zum Überwachungsgesetz und dies in der ersten Bereinigung. Ganz generell ist zu sagen, dass der Nationalrat sich in den meisten Punkten dem Ständerat angeschlossen hat. Ihre vorberatende Kommission hat sich mit den verbliebenen gut ein Dutzend Differenzen vertieft auseinandergesetzt und hierfür auch eine zusätzliche Anhörung der KKJPD durchgeführt. Weil die Beratung im Ständerat jetzt schon eineinhalb Jahre zurückliegt, erlauben Sie mir vielleicht nur noch zwei generelle Überlegungen zu dieser Vorlage.

Die Revision des Überwachungsgesetzes will also die Voraussetzungen dafür schaffen, zum Zwecke der Strafverfolgung und nur dann, wenn ein dringender Verdacht auf Begehung einer schweren Straftat besteht, den Post- und Fernmeldeverkehr im Vergleich zu heute nicht mehr, aber besser überwachen zu können. Es geht im Unterschied zum Nachrichtendienstgesetz also nicht um eine präventive Überwachung der Bürgerinnen und Bürger; das Überwachungsgesetz bezweckt auch nicht eine flächendeckende Überwachung, wie sie offenbar der amerikanische Geheimdienst über Jahre bei Freund und Feind praktiziert. Es geht darum, zur Aufklärung von Straftaten die rechtlichen Voraussetzungen zur Überwachung des Fernmeldeverkehrs den technischen Entwicklungen anzupassen. Es soll damit verhindert werden, dass durch die Verwendung neuer Technologien die Überwachung erschwert, wenn nicht sogar verhindert wird.

Was macht diese Vorlage so umstritten? Wir haben das jetzt im Verlaufe dieser eineinhalb Jahre seit der Erstberatung in unserem Rat immer wieder gehört: Es sind die gegenläufigen Interessen. Der Schutz der Persönlichkeitsrechte und persönlicher Daten steht dem Interesse an einer wirksamen Strafverfolgung gegenüber, und diese wiederum konkurrieren mit den Interessen der Provider, ihr Geschäftsmodell möglichst ungehindert kommerziell anbieten zu können. In diesem mehrfachen Interessenkonflikt sucht sich das Gesetz einen Weg, der im Rahmen des Gesetzmässigkeits- und Verhältnismässigkeitsprinzips gerade so viel wie nötig, aber so wenig wie möglich in Grundrechte eingreift und als dritte Komponente der Rechtsstaatlichkeit den Rechtsschutz garantiert. Das Machbare, das Mögliche und das Notwendige - in diesem Spannungsfeld spielt sich auch die gesellschaftspolitische Debatte um die Überwachung von Post- und Fernmeldeverkehr ab.

Man ist sich darin auch einig: Je ausgefeilter die technischen Möglichkeiten sind, umso mehr haben wir den grundrechtssensiblen Bereich im Auge zu behalten, um den wirksamen Schutz dieser Grundrechte möglichst wahren zu können.

Das sind zwei, drei grundsätzliche Überlegungen, bevor wir jetzt in die Beratung der rund zwölf Differenzen zum Nationalrat treten.

Art. 11 Abs. 6

Antrag der Kommission

Zustimmung zum Beschluss des Nationalrates

Angenommen

Art. 12 Abs. 4-6

Antrag der Kommission

Streichen

Engler Stefan (C, GR), für die Kommission: Die Absicht des Nationalrates lag mit dieser Ergänzung von Artikel 12 darin - im Übrigen hat der Nationalrat diese Bestimmung mit 90 zu 90 Stimmen bei 4 Enthaltungen beschlossen -, die Informatiksicherheit im Überwachungsgesetz selber zu verankern. Die Kommission für Rechtsfragen anerkennt zwar die vom Nationalrat verfolgte Absicht, stellt sich hingegen auf den Standpunkt, dass das Thema der Informatiksicherheit ins Datenschutzrecht, ins Datenschutzgesetz gehört und dort allenfalls infolge des Detaillierungsgrades sogar in eine entsprechende Verordnung. Die Formulierung gemäss Nationalrat lässt durch die Unterscheidung von gewöhnlichen und erheblichen Sicherheitslücken zudem noch viel Interpretationsspielraum offen. Das letzte Argument, weshalb Ihnen die Kommission beantragt, die Absätze 4, 5 und 6 von Artikel 12 zu streichen, liegt in einer europäisch aufgegleisten Reform des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Für die Kommission scheint es richtig und zielführender, die Ergebnisse dieser Reform abzuwarten.

Als zu wenig bestimmt, am falschen Ort und zu früh hat die Kommission also die Ergänzung des Nationalrates in Artikel 12 abgelehnt.

Angenommen

Art. 19 Abs. 4

Antrag der Kommission

Festhalten

Engler Stefan (C, GR), für die Kommission: Es geht bei beiden Bestimmungen, Artikel 19 Absatz 4 und Artikel 26 Absatz 5, um die Aufbewahrungsdauer sogenannter Randdaten. Für solche des Postverkehrs beantragt Ihnen die Kommission, am Beschluss des Ständerates von sechs Monaten festzuhalten. Der Nationalrat ist dem Bundesrat gefolgt und hat die Aufbewahrungsdauer auch für Randdaten des Postverkehrs auf zwölf Monate verlängert. Bezüglich der Aufbewahrungsdauer der Daten aus dem Fernmeldeverkehr gemäss Artikel 26 Absatz 5 hat sich die Kommission dafür ausgesprochen, auch diese wie im geltenden Recht auf sechs Monate zurückzunehmen. Auch hier folgte der Nationalrat zuvor in der Erstberatung dem Bundesrat und dem Ständerat und sah für die Randdaten aus dem Fernmeldeverkehr eine zwölfmonatige Aufbewahrungsfrist vor.

Mit dem Antrag Ihrer Kommission bestünde nun neu für Randdaten des Postverkehrs wie für solche aus dem Fernmeldeverkehr die gleich lange Aufbewahrungsdauer, nämlich sechs Monate. In formeller Hinsicht brauchte die Kommission dafür die Zustimmung der Schwesterkommission, darauf in der Differenzbereinigung zurückkommen zu dürfen. Die Schwesterkommission hat uns die Zustimmung erteilt, obwohl an und für sich keine formelle Differenz mehr in Artikel 26 Absatz 5 besteht, um auf diese Frage zurückzukommen. Warum diese Umkehr? Es handelt sich bekanntlich um das sensible Thema der Vorratsdatenspeicherung, und zwar als Mittel, um bei polizeilichen Ermittlungen belastende wie auch entlastende Beweismittel zu erlangen. In vielen Fällen bilden diese Verbindungsdaten möglicherweise auch nur einen ersten Ermittlungsansatz, um zu weiteren Beweisen zu gelangen. Die Regelung soll sicherstellen, dass Anbieter von Telefondiensten die Verbindungsdaten eines Telefonats, also Rufnummer, Datum und Uhrzeit, für sechs Monate speichern müssen. Wohlgemerkt, es geht dabei nicht um Inhalte, sondern lediglich um die Randdaten der Kommunikation.

Die Kommission erachtet es als vernünftigen und verhältnismässigen Kompromiss zwischen den Freiheitsrechten einerseits und den Erfordernissen einer effektiven Strafverfolgung andererseits, wenn die Aufbewahrungsdauer nicht noch verlängert wird, sondern auf sechs Monate beschränkt bleibt. Nochmals sei betont, dass nicht der Staat Datensammlungen anlegt, sondern dass die Telekommunikationsanbieter verpflichtet werden, solche Verbindungsdaten während sechs Monaten aufzubewahren. Die Beibehaltung der Aufbewahrungsdauer der Randdaten von sechs Monaten entspricht also der Beibehaltung des Status quo.

Die Vorratsdatenspeicherung ist ja per se schon sehr umstritten. In diesem Kontext würde eine Erhöhung auf zwölf Monate die Chance eines Referendums möglicherweise erhöhen und die ganze Vorlage gefährden, was ganz und gar nicht im Interesse der Strafverfolgungsbehörde liegen dürfte. Das war, nebst den in den vergangenen eineinhalb Jahren geführten Diskussionen zu dieser Frage, ein zusätzlicher Grund dafür, dass sich die Kommission entschieden hat, auf einen getroffenen Entscheid zurückzukommen. Mit der Gesetzesrevision soll ja im Grunde genommen nicht mehr überwacht werden können als bisher, sondern die Überwachung soll an die technischen Fortschritte angepasst werden, und die Datensicherheit und der Datenschutz sollen verbessert werden.

Das sind die Gründe, weshalb Ihnen Ihre Kommission beantragt, bei den Randdaten des Postverkehrs beim Beschluss des Ständerates - sechs Monate Aufbewahrungsdauer - zu bleiben und bei Artikel 26 Absatz 5, wo es um die Randdaten des Fernmeldeverkehrs geht, zum geltenden Recht, nämlich zur Aufbewahrungsdauer von maximal sechs Monaten, zurückzukommen.

Janiak Claude (S, BL): Ich spreche zu Artikel 26, ich habe es so verstanden, dass man das zusammennimmt.

Ich bitte Sie, hier dem Entwurf der Kommission zuzustimmen und die Frist bei diesen sechs Monaten zu belassen; das ist im Übrigen das geltende Recht. Wir haben ja jetzt die Behandlung dieses Gesetzes. Parallel dazu ging es aber auch noch um das Nachrichtendienstgesetz. Ich habe immer wieder gestaunt, wie die Debatten gelaufen sind, da wurde kreuz und quer vermischt. Etwa die präventive Überwachung: Kürzlich hat ein Journalist in einer Sonntagszeitung unserem Antrag, hier wieder auf sechs Monate zurückzukommen, eine ganze Seite gewidmet. Er machte Untersuchungen bei den Umfragen, die man im Zusammenhang mit den Wahlen beantworten kann, und kam zum Schluss: Eine Mehrheit ist gegen die präventive Überwachung. Das hat gar nichts miteinander zu tun! Es ist erstaunlich, dass man einen Artikel schreiben kann und immer noch nicht begriffen hat, was der Unterschied ist.

Es gibt noch einen weiteren Grund, hier beim geltenden Recht zu bleiben: Es liegt ein Urteil des Europäischen Gerichtshofes vor, dessen Begründung man noch nicht kennt, aber es ist ein Fall, bei dem Deutschland zurückgepfiffen worden ist, als es diese Frist verlängern wollte. Wenn man daraus Folgerungen zieht, dann muss man zur Erkenntnis kommen, dass diese Ausdehnung auf zwölf Monate auch bei uns schwierig wäre. Man muss damit rechnen, dass allenfalls auch wir in Schwierigkeiten kommen könnten. Mit einer Senkung auf sechs Monate hätten wir dann - darauf hat auch der Präsident schon hingewiesen - in einem allfälligen Abstimmungskampf sicher gute Karten, und wir könnten auch der Rechtsentwicklung in anderen europäischen Ländern Rechnung tragen.

Wir haben in der Kommission ja, das möchte ich auch noch betonen, Herrn Käser, den Direktor der KKJPD, angehört und haben ihm explizit die Frage gestellt, ob die KKJPD damit einverstanden wäre. Er hat das bejaht. Er hat auch gesagt, dass es für sie eigentlich viel wichtiger sei, dass die gesetzliche Grundlage für den Einsatz für Govware für die Strafverfolgungsbehörden endlich möglich wird. Das ist für sie das viel wichtigere Thema. Das bedeutet auch, dass man dieses Geschäft jetzt endlich abschliesst. Für das Büpf brauchen wir viel länger als für das Nachrichtendienstgesetz, obwohl das Nachrichtendienstgesetz in Bezug auf die Grundrechte und die Eingriffe in die persönliche Freiheit ja eigentlich viel weitergehend ist; da läuft ja noch kein Strafverfahren.

Ich bitte Sie, hier Ihrer Kommission zu folgen. Ich habe die Aufgabe gehabt, das der Kommission des Nationalrates schmackhaft zu machen. Sie haben ein bisschen "gewäffelt", aber sie sind am Schluss doch bereit gewesen, uns die Möglichkeit zu geben, diese Differenz noch einmal zu öffnen.

Sommaruga Simonetta, Bundespräsidentin: Es wurde jetzt erwähnt: Sie haben mit Ihrem letzten Entscheid zu diesem Gesetz die Aufbewahrungsdauer von Randdaten unterschiedlich festgelegt, je nachdem, ob sie den Postverkehr oder den Fernmeldeverkehr betraf. Der Nationalrat hat dann für beide Arten eine Aufbewahrungsfrist der Randdaten von 12 Monaten festgelegt. Deshalb stellen sich eigentlich zwei Fragen:

Soll man erstens für den Postverkehr und den Fernmeldeverkehr eine unterschiedlich lange Aufbewahrungsdauer festlegen? Macht es Sinn, für den Fernmeldeverkehr 12 Monate und für den Postverkehr 6 Monate festzulegen? Sollen zweitens insgesamt 6 oder 12 Monate gelten?

Der Bundesrat ist in Bezug auf die erste Frage, also die unterschiedliche Aufbewahrungsdauer, ganz klar der Meinung: Nein, man soll bei beidem, beim Postverkehr und beim Fernmeldeverkehr, eine gleich lange Aufbewahrungsdauer haben. Das hat der Nationalrat auch so beschlossen, 12 Monate für beide.

Nun ist Ihre Kommission nochmals auf die Frage zurückgekommen, ob man diese Ausweitung tatsächlich vornehmen soll oder ob man bei der Aufbewahrungsdauer für die Randdaten, also bei der Vorratsdatenspeicherung, bei den heute geltenden 6 Monaten bleiben soll.

Ich muss Ihnen sagen: Ich bin auch tief beeindruckt über die Schwierigkeit, dieses Gesetz zu erklären und zu vertreten. Eigentlich müsste es klar sein. Ich meine, es geht hier um schwere Straftaten, es geht nicht um irgendwelche Bagatelldelikte. Es geht darum, dass die Strafverfolgungsbehörde eine Überwachung erst nach einem Entscheid des Zwangsmassnahmengerichtes vornehmen kann, und trotzdem ist diese Regelung so umstritten.

Wie Herr Ständerat Janiak jetzt auch in Bezug auf die Strafverfolgungsbehörden gesagt hat - auch wir haben nach diesen kontroversen Diskussionen nochmals das Gespräch mit den

Kantonen, mit den Strafverfolgungsbehörden gesucht -, sind diese einhellig der Meinung, dass es jetzt erstens vorwärtsgehen muss und dass man zweitens auch die Möglichkeit haben muss, die verschlüsselte Kommunikation zu überwachen.

Die Polizei hat mir Folgendes erzählt: Bei Abhörungen hört sie, wie Delinquenten sagen: "Okay, wir werden jetzt in die verschlüsselte Kommunikation wechseln." Das ist nicht etwas wahnsinnig Kompliziertes, das ist einfach, wenn man per Skype telefoniert. Stellen Sie sich einmal vor: Die Strafverfolgungsbehörde ist dann einfach draussen - das ist ja wirklich völlig absurd!

Nun aber, angesichts dieses massiven Widerstandes, angesichts der Schwierigkeit auch, diese Fragen in Ruhe zu diskutieren, ist auch aus Sicht des Bundesrates Folgendes zu sagen: Wir haben es zumindest begrüsst, dass sich Ihre Kommission diese Fragen nochmals gestellt hat. Wie auch erwähnt wurde, gab es dann in der Zwischenzeit das Urteil des Europäischen Gerichtshofes, der die europäische Richtlinie über die Vorratsdatenspeicherung für ungültig erklärt hat.

Das hat doch zu einer beträchtlichen Verunsicherung innerhalb von Europa geführt. Es gab noch ein Verfassungsgericht, dasjenige in Österreich, das dann die dortige Gesetzgebung zur Vorratsdatenspeicherung auch gleich aufheben wollte. In der Zwischenzeit hat man in einzelnen europäischen Staaten wieder legiferiert; das war immer das erste und wichtigste Thema, dass ich mit den Justizministern diskutiert habe. Deutschland liegt jetzt bei 10 Wochen Vorratsdatenspeicherung, Luxemburg hat sich für 6 Monate entschieden. Es gibt aber auch Staaten, die heute weiter gehen und die 12 Monate haben. Unter dem Eindruck der terroristischen Anschläge wird das Pendel wahrscheinlich jetzt wieder ein bisschen in die andere Richtung ausschlagen. Es ist eigentlich schade, dass man so legiferieren muss - ich sage es ganz offen.

Trotzdem ist auch der Bundesrat der Meinung, dass der Entscheid Ihrer Kommission im heutigen Zeitpunkt der richtige ist. Man sollte diese Vorlage vorwärtsbringen. Wir brauchen die Möglichkeit, unter den strengen Voraussetzungen - damit das auch noch ganz klar gesagt ist - eben auch verschlüsselte Kommunikation zu überwachen. Wenn man hier etwas Druck wegnehmen kann, dann sagt auch die Strafverfolgungsbehörde, dass ihr das letztlich diene. Im Prinzip kann man sagen, dass die Strafverfolgungsbehörde immer länger Daten speichern möchte, je länger, desto besser; je mehr Material sie hat, desto besser. Aber sie sagt, dass man mit den heutigen 6 Monaten doch auch gewisse Möglichkeiten hat, vor allem die Möglichkeit, mit den Staatstrojanern auch die verschlüsselte Kommunikation unter strengen Voraussetzungen zu überwachen. Das hat für sie eindeutige Priorität. Deshalb würde sich der Bundesrat einem Rückkommen auch nicht widersetzen. Das ist jetzt, sage ich mal, unter den gegebenen Umständen die politisch richtige Antwort. Es ist ganz klar eine politische Antwort, aber wir werden hier jetzt sicher nicht beharren. Ich denke, in Ihrer Kommission wurde das sorgfältig noch einmal abgewogen und auch mit den Kantonen und den Strafverfolgungsbehörden besprochen. Wenn diese sich dem ebenfalls anschliessen können, dann, denke ich, ist es ein politisch nachvollziehbarer Entscheid.

Angenommen

Art. 21 Abs. 2

Antrag der Kommission

... und während der Dauer der Kundenbeziehung sowie während 6 Monaten nach deren Beendigung geliefert werden können. Der Bundesrat legt fest, dass die

Fernmeldedienstanbieter bestimmte dieser Daten nur zum Zweck der Identifikation während 6 Monaten aufbewahren und liefern müssen.

Art. 22 Abs. 2

Antrag der Kommission

... zum Zweck der Identifikation während der Dauer der Kundenbeziehung sowie während 6 Monaten nach deren Beendigung bereithalten und liefern müssen. Der Bundesrat legt fest, dass die Fernmeldedienstanbieter bestimmte dieser Daten nur zum Zweck der Identifikation während 6 Monaten aufbewahren und liefern müssen. Sie müssen dem Dienst weitergehende Angaben liefern, über die sie verfügen.

Engler Stefan (C, GR), für die Kommission: Beide Bestimmungen betreffen den Grundsatz und den Umfang der Auskunftspflicht von Providern gegenüber der Behörde, einmal ganz generell, in Artikel 21 Absatz 2, und dann im Zusammenhang mit Straftaten, die über das Internet begangen werden. Dabei ist die Anpassung von Artikel 21 Absatz 2 dann die Folge der Anpassung von Artikel 22 Absatz 2. Wir befinden uns also hier bei den Auskünften, nicht etwa bei den Randdaten und schon gar nicht bei inhaltlichen Daten der Überwachung.

Als Auskünfte gelten Daten, die der Identifikation der Teilnehmer der Internetkommunikation dienen sollen. Wie gesagt, es handelt sich also bei dem, was unter Auskünften zu verstehen ist, grundsätzlich weder um Randdaten noch um den Inhalt der Kommunikation. Um jetzt aber sicherzustellen, dass bezüglich Aufbewahrungsdauer und Qualität der Daten, die einzig zur Identifikation dienen dürfen, die Bestimmungen zur Speicherung der Randdaten gemäss Artikel 26 Absatz 5 nicht unterlaufen werden, hat sich die Kommission für Rechtsfragen zu einer Präzisierung und Anpassung von Artikel 22 Absatz 2 und als Folge davon auch von Artikel 21 Absatz 2 entschieden. Damit soll explizit ausgeschlossen werden, dass beispielsweise für Verbindungsdaten und Server-Protokolle, die im Einzelfall auch der Identifikation dienen können, die Aufbewahrungsdauer über die für Randdaten vorgesehene hinaus sogar noch verlängert würde. Der Bundesrat erhält mit der durch die Kommission neu angepassten Bestimmung die Ermächtigung, dann im Rahmen der Verordnung zu regeln, welche der Identifikation dienenden Daten nicht länger als sechs Monate aufbewahrt werden dürfen.

Sommaruga Simonetta, Bundespräsidentin: Diese erläuternde Ergänzung des Kommissionssprechers ist nicht bestritten. Ich möchte Sie deshalb bitten, der Kommission zu folgen.

Die Ergänzung bedarf aber noch einiger Erklärungen; ich möchte diese insbesondere auch zuhanden der Materialien abgeben.

In der ersten Runde haben Sie und der Nationalrat eine Änderung von Artikel 21 Absatz 2 bzw. von Artikel 22 Absatz 2 beschlossen. Demnach müssen die Anbieterinnen von Fernmeldediensten bestimmte Daten während der Dauer der Kundenbeziehung und während einer bestimmten Zeitspanne nach deren Beendigung aufbewahren. Eine Kundenbeziehung besteht sowohl bei Abonnementsverhältnissen als z. B. auch bei der Verwendung einer Prepaid-SIM-Karte. Dabei geht es um Daten, die der Identifikation von Teilnehmerinnen und Teilnehmern dienen.

Solche Daten können nun aber je nach Konstellation gleichzeitig auch Randdaten sein. Wie lange Randdaten aufbewahrt werden müssen, regelt aber Artikel 26. Diese Bestimmung knüpft für die Dauer der Aufbewahrung der Daten an den Zeitpunkt ihres Entstehens an, nicht aber an

die Dauer der Kundenbeziehung. Deshalb besteht die Gefahr, dass für die gleichen Daten unterschiedliche Fristen gelten, je nachdem, ob man Artikel 21 und Artikel 22 oder ob man Artikel 26 anwendet.

Um solche Widersprüche zur Aufbewahrungsdauer der Randdaten des Fernmeldeverkehrs zu vermeiden, beantragt Ihre Kommission eine Ergänzung der Artikel 21 Absatz 2 und 22 Absatz 2. Demnach muss der Bundesrat in der Verordnung festlegen, welche Identifikationsdaten als Randdaten zu betrachten und folglich nur so lange aufzubewahren sind, wie es Artikel 26 vorschreibt.

Das wollte ich hier noch zuhanden der Materialien festhalten.

Angenommen

Art. 24

Antrag der Kommission

Zustimmung zum Beschluss des Nationalrates

Sommaruga Simonetta, Bundespräsidentin: Auch hier möchte ich zuhanden der Materialien - es ist, denke ich, wichtig, dass wir das festhalten - noch etwas beifügen. Der Nationalrat wie auch Ihre Kommission haben beschlossen, die vom Bundesrat vorgeschlagene und von Ihnen beschlossene Regelung in Artikel 24 dahingehend zu präzisieren, dass die zu liefernden Informationen technischer Natur seien. Nun stellt sich die Frage, wie diese Ergänzung zu verstehen ist.

Mit dieser Ergänzung wird noch einmal deutlich, was ohnehin gilt: Diese Informationen dienen nicht dazu, eine Person oder einen Anschluss zu identifizieren, und sie sind auch keine Randdaten. Das geht schon aus dem Kommentar zu Artikel 24 in der Botschaft eindeutig hervor. Dennoch ist es zur Vermeidung aller Missverständnisse richtig, das auch im Gesetz selber zu sagen. Solche Informationen technischer Natur können also insbesondere den Standort einer Mobilfunkantenne betreffen, wie das im Beispiel im Kommentar zu Artikel 24 in der Botschaft erwähnt ist. Diese Informationen können zum Beispiel auch Auskünfte über folgende Fragen geben: Welche Antenne bedient oder deckt gemäss Abdeckungsinformationen der Fernmeldedienstanbieterin einen bestimmten geografischen Punkt ab? Welche Charakteristiken hat eine Antenne - beispielsweise die Art, die Abstrahlungsrichtung, die Technologie, das Frequenzband? Werden ankommende Anrufe eines Anschlusses über eine andere Fernmeldedienstanbieterin als die ausgehenden abgewickelt? Betrifft das zu überwachende Adressierungselement einen ganzen Firmenanschluss mit Hunderten von Benutzern? Und schliesslich: Was ist die genaue Standortadresse des Gebäudes, dessen Anschlüsse überwacht werden sollen?

Dies zuhanden der Materialien.

Angenommen

Art. 26

Antrag der Mehrheit

Abs. 5

... des Fernmeldeverkehrs während 6 Monaten aufbewahren.

Abs. 5bis

Streichen

Zustimmung zum Beschluss des Nationalrates

Engler Stefan (C, GR), für die Kommission: In Artikel 26 Absatz 5bis finden Sie eigentlich die einzige Bestimmung, bei der sich in der Kommission eine Mehrheit und eine Minderheit ergeben haben. Worum geht es? Es geht im Wesentlichen darum, dass der Nationalrat eine Verpflichtung in die Vorlage neu aufgenommen hat, wonach die Randdaten des Fernmeldeverkehrs in der Schweiz aufbewahrt werden müssen. Der Nationalrat verspricht sich davon einen Mehrwert an Datensicherheit. Eine Minderheit der Kommission für Rechtsfragen hat sich dieser Auffassung angeschlossen; die klare Mehrheit lehnt eine solche Pflicht ab. Ich würde es vorziehen, wenn der Vertreter der Minderheit zuerst begründet, weshalb sie an der nationalrätlichen Fassung festhalten möchte. Ich werde Ihnen im Anschluss daran die Überlegungen der Kommissionsmehrheit mitteilen.

Cramer Robert (G, GE): C'est avec plaisir que je vais tenter de vous convaincre que la proposition du Conseil national est une bonne proposition et que nous devons regretter de ne pas l'avoir faite nous-mêmes. Nous devons le regretter, mais nous avons quelques excuses à cela, car le Conseil national a été servi par un arrêt de la Cour de justice de l'Union européenne, du 8 avril 2014, c'est-à-dire postérieurement à la date du 19 mars 2014, à laquelle nous avions examiné ce projet de loi.

Que nous dit la Cour de justice de l'Union européenne? Elle nous dit qu'il faut être très attentif lorsqu'on recherche le "Safe Harbor", c'est-à-dire lorsque l'on recherche le "port sûr". Le port sûr, c'est l'endroit où l'on peut, en toute sécurité, aller déposer des données; le port sûr, c'est l'endroit où l'on est certain que lorsqu'on y a déposé ces données, personne d'autre n'y aura accès. La Cour de justice de l'Union européenne, qui a été saisie par des affaires portées dans deux Etats, l'Irlande et l'Autriche, a constaté que les Etats-Unis ne sont pas un port sûr. Et pourquoi est-ce que les Etats-Unis ne sont pas un port sûr? C'est parce que, aux Etats-Unis, l'autorité peut à tout moment ordonner au détenteur de données de les lui communiquer. En d'autres termes, le contrat qui est passé entre le déposant de données et qui, par hypothèse, se trouverait en Suisse, et le récipiendaire qui, par hypothèse, se trouverait aux Etats-Unis, ne s'impose pas à l'autorité américaine, laquelle peut s'emparer de toutes les données qui se trouvent sur son territoire. Et il va de soi que ce qui se passe aux Etats-Unis - parce que c'est évidemment avec ce pays que l'affaire a été posée, parce que c'est aux Etats-Unis que l'on trouve énormément d'entreprises actives dans le domaine des télécommunications - peut se passer de la même façon dans n'importe quel Etat au monde. Je n'imagine pas que des données déposées en Russie ou en Chine puissent être considérées comme déposées dans un port plus sûr que si elles sont déposées dans un port américain.

Et la réflexion que je vous fais ici n'est pas uniquement celle du Conseil national. Il nous a été confirmé, lors des travaux en commission, par le Préposé fédéral à la protection des données et à la transparence, Monsieur Hanspeter Thür, qu'aujourd'hui on est dans une situation d'incertitude juridique, et que personne ne peut affirmer que des données suisses déposées aux Etats-Unis sont des données dont la confidentialité est garantie.

C'est la raison pour laquelle le Conseil national, fort sagement, a proposé une adjonction à cette loi, sur la base donc de cet arrêt de la Cour de justice de l'Union européenne, qui ne nous était

pas connu à l'époque où nous avons examiné ce projet de loi pour la première fois. Le Conseil national propose que les données secondaires de télécommunication doivent être conservées en Suisse.

C'est certainement une source d'inconvénients pour les fournisseurs, pour lesquels il est beaucoup plus commode - et peut-être même plus économique - de pouvoir trouver un autre endroit pour déposer ces données. Mais on parle là de protection des données, c'est-à-dire de quelque chose d'essentiel! Et je suis persuadé que toutes celles et tous ceux qui, au sein de ce conseil, à juste titre, ont été attentifs à toute la problématique du secret bancaire, qui ont considéré, à juste titre encore, qu'on ne peut pas sans autre avoir accès à un certain nombre de renseignements qui ressortent de la sphère privée, seront encore plus attentifs ici. Il ne s'agit pas ici d'un cadre juridique comme celui de l'échange d'informations ou des procédures d'entraide. Il s'agit véritablement de déposer des données dans un lieu où, à tout moment, l'autorité du pays concerné peut s'en emparer.

C'est la raison pour laquelle le Conseil national a proposé cet amendement. J'y étais déjà favorable après l'avoir lu, parce qu'il me semblait s'imposer. Mais après avoir entendu le Préposé fédéral à la protection des données et à la transparence, j'ai été totalement convaincu que le Conseil national a eu le bon réflexe en modifiant ainsi ce projet de loi.

Engler Stefan (C, GR), für die Kommission: Für eine Mehrheit der Kommission macht es keinen Sinn und ist es auch nicht nötig, den Aufbewahrungsort dieser Randdaten exklusiv in der Schweiz festzulegen. Das ist für das Einhalten des schweizerischen Datenschutzrechts nicht nötig, denn die in der Schweiz aktiven Unternehmungen müssen ja das schweizerische Recht, also auch das Datenschutzrecht, einhalten.

Es wurde das Urteil des Europäischen Gerichtshofes erwähnt, das als "Safe Harbor"-Urteil bekanntgeworden ist. Auch aus diesem Urteil lässt sich nicht ableiten, dass die Daten in der Schweiz aufbewahrt werden müssten. Der Europäische Gerichtshof hat in diesem Urteil nämlich bloss festgestellt - aber immerhin festgestellt -, dass die EU nicht genügend überprüft hat, ob die USA für die personenbezogenen Daten ein angemessenes Schutzniveau aufweisen.

Für die Kommission wäre eine solche Einschränkung nicht verhältnismässig, denn sie würde das Aufbewahren von Daten im Ausland generell verbieten, obschon es durchaus Staaten gibt, die für die personenbezogenen Daten ein angemessenes Schutzniveau kennen. Weiter würde die Wirtschaftsfreiheit eingeschränkt, die Anbieter von Fernmeldediensten könnten sich nämlich nicht mehr so organisieren, wie sie es als wirtschaftlich sinnvoll erachten. Sie könnten gewisse administrative Arbeiten wie zum Beispiel das Aufbereiten der Daten für die Rechnungsstellung nicht mehr im Ausland vornehmen lassen, weil dafür auch die Randdaten nötig sind. Möglicherweise würden auch die betreffenden betrieblichen Prozesse verteuert. Die Aufbewahrungspflicht in der Schweiz hätte somit weitreichende und negative Auswirkungen, vor allem für international tätige Telekommunikationsunternehmungen. Telekommunikationsdienste werden zunehmend von international tätigen Unternehmen bereitgestellt, die dazu notwendigen IT- und Kommunikationssysteme werden dabei in einigen wenigen Ländern zentralisiert, und diese befinden sich häufig auch ausserhalb der Schweiz. Deshalb ist es unvermeidbar, dass Randdaten auch im Sinne unseres Überwachungsgesetzes ausserhalb der Schweiz bereitgestellt und auch heute schon dort gespeichert werden.

Diese Unternehmungen gehen in der Regel sorgsam mit diesen sensitiven Daten um und stellen durch physische und prozessbezogene Massnahmen die Sicherheit und die gesetzeskonforme Verwendung der Randdaten sicher.

Ein zusätzliches Argument, weshalb sich die Mehrheit dagegen ausgesprochen hat, einen exklusiven Aufbewahrungsort im Überwachungsgesetz zu definieren, liegt darin, dass eine solche Regelung im Überwachungsgesetz am falschen Ort wäre. Eine Norm, die eine Pflicht zur Aufbewahrung der Daten an einem bestimmten Ort statuiert, gehört nämlich - wenn schon - eher in das Telekommunikationsgesetz selber oder allenfalls in das Datenschutzgesetz, denn die Frage der Übermittlung der Telekommunikationsdaten in ein bestimmtes Land ist eine generelle Frage, die nicht die Fernmeldeüberwachung alleine betrifft. Man könnte sich fragen, ob beispielsweise Bank- oder andere Daten dann auch davon betroffen wären, Daten von Versicherungen, Daten aus medizinischen Labors usw. Auch hier müsste man sich dann die Frage stellen, weshalb diese und die anderen Daten nicht exklusiv in der Schweiz aufbewahrt werden müssten. Die Kommission betrachtet deshalb die Formulierung des Nationalrates zwar als gutgemeint, allerdings nicht im Interesse der Wirtschaft und auch nicht beitragend zur Erhöhung der Datensicherheit.

Sommaruga Simonetta, Bundespräsidentin: Der Nationalrat und Ihre Kommissionsminderheit möchten hier eigentlich eine Swissness-Regel für Fernmeldedienstanbieterinnen einführen. Aber im Unterschied zum Swissness-Gesetz, bei dem es ja freiwillig ist, ob die Firmen sich dieser Regel unterwerfen wollen oder nicht, wäre das hier natürlich obligatorisch.

Ich möchte Ihnen gerne die Gründe darlegen, weshalb der Bundesrat zusammen mit Ihrer Kommissionsmehrheit der Meinung ist, dass es diese Swissness-Regel, eben diese spezielle Vorschrift, nicht braucht: Die Einschränkung ist für die Einhaltung des schweizerischen Datenschutzrechts nicht nötig; für mich ist das eigentlich das wichtigste Argument. Wenn der Eindruck entstanden wäre, dass das in Bezug auf den Datenschutz nur für die Schweiz gilt und die Schweizer Datenschutzbestimmungen nicht mehr gelten, wenn ein Unternehmen z. B. Daten in einem anderen Land speichert, dann ist das falsch. Das schweizerische Datenschutzrecht gilt eben ungeachtet dessen, wo die Daten effektiv gelagert werden. Ich glaube, das ist wichtig zu wissen.

Jetzt kann man sagen, dass man immer mehr tun kann und dass es in der Schweiz sicherer ist als irgendwo; aber einfach, damit das klar ist: Im Ausland Daten speichern heisst nicht, dass dann das schweizerische Datenschutzrecht nicht mehr gilt. Das hat der Kommissionssprecher gesagt. Natürlich sind das sensible Daten, um die es hier geht, aber denken Sie einmal an die Daten der Privatversicherer oder der Krankenversicherungen. Müssten Sie dann nicht auch sagen, dass diese Daten, wenn schon, nur in der Schweiz gespeichert werden dürfen? Deshalb glaube ich, dass es schon wichtig ist, dass wir bei der heutigen Regelung bleiben, dass wir sagen, dass das Datenschutzrecht eingehalten werden muss, unabhängig davon, wo die Daten effektiv gelagert werden.

Ich will nicht wiederholen, was schon gesagt wurde. Aus dem Urteil des Europäischen Gerichtshofes zu den "Safe Harbor"-Verträgen mit den USA in Europa kann man nicht ableiten, dass die Daten deswegen in der Schweiz aufbewahrt werden müssen. Der Europäische Gerichtshof hat in diesem Urteil bloss festgestellt, dass die EU nicht genügend geprüft hat, ob die USA für die personenbezogenen Daten ein angemessenes Schutzniveau bieten.

Wir sind schon auch der Meinung, dass eine solche Ergänzung, wie Sie der Nationalrat und die Minderheit vorschlagen, zu einer Einschränkung der Wirtschaftsfreiheit führen würde. Denn die Fernmeldedienstanbieterinnen könnten sich nicht mehr so organisieren, wie sie es - noch einmal - unter der heute geltenden Datenschutzgesetzgebung für wirtschaftlich sinnvoll erachten. Es kommt noch hinzu, dass die Aufbereitung der Daten für die Rechnungsstellung nicht mehr im Ausland vorgenommen werden könnte, weil dafür auch die Randdaten nötig sind. Das könnte natürlich schon auch zu einer Verteuerung führen.

Dass die Regelung hier im Büpf nicht am richtigen Ort wäre, hat der Kommissionssprecher schon gesagt: Das müssten Sie wenn schon im Fernmeldegesetz regeln. Aber das ist mehr eine formale Begründung, nicht eine materielle. Wir sind der Meinung, dass mit dem heute geltenden Datenschutzrecht genügend abgesichert ist, dass die Aufbewahrungs- und Datenschutzvorschriften unabhängig davon gelten, wo die Daten gelagert sind.

Deshalb beantragt Ihnen der Bundesrat, die Mehrheit zu unterstützen.

Abstimmung - Vote

Für den Antrag der Mehrheit ... 20 Stimmen

Für den Antrag der Minderheit ... 17 Stimmen

(2 Enthaltungen)

Art. 42 Abs. 2

Antrag der Kommission

Zustimmung zum Beschluss des Nationalrates

Angenommen

Aufhebung und Änderung bisherigen Rechts

Ziff. II Ziff. 1 Art. 269 Abs. 2 Bst. a

Antrag der Kommission

Zustimmung zum Beschluss des Nationalrates

Angenommen

Ziff. II Ziff. 1 Art. 269quater

Antrag der Kommission

Abs. 1-3

Zustimmung zum Beschluss des Nationalrates

Abs. 4, 5

Streichen

Engler Stefan (C, GR), für die Kommission: Bei der Bestimmung von Artikel 269quater geht es um das Thema der Staatstrojaner - die Informatikprogramme, welche die Behörden einsetzen, um Echtzeitüberwachung auch verschlüsselter Kommunikation vornehmen zu können. Hier hat der Nationalrat die Rahmenbedingungen neu definiert, indem er der Sicherheit und der Qualität dieser Informatikprogramme ein stärkeres Gewicht geben wollte.

Ihre Kommission ist der Meinung, dass man die zusätzlichen Sicherheitsvoraussetzungen, wie sie neu in den Absätzen 1, 2 und 3 durch den Nationalrat in dieses Gesetz eingefügt wurden, durchaus übernehmen kann und diese Vorschriften einen Beitrag leisten können, den Umgang mit dieser Software, mit Informatikprogrammen sicherer und verlässlicher zu machen, so dass diese rechtsstaatlich auch weniger beanstandet werden können.

Indessen ist Ihre Kommission der Meinung, dass die Bestimmungen in Absatz 4 und in Absatz 5 von Artikel 269quater zu sehr in die Hoheit der Kantone eingreifen, die nämlich für die Strafverfolgung zuständig bleiben sollen, und dazu gehört auch die Wahl der Instrumente und Massnahmen, mit denen sie die Strafverfolgung ausüben. Eine vorgängige Zertifizierung von Govware, wie sie mit den Absätzen 4 und 5 verlangt wird, beurteilt die Kommission einstimmig als in vielerlei Hinsicht problematisch. Dies zum einen im Wissen darum, dass diese Software laufend - es wurde uns gesagt, sogar in Wochenabständen - an die neuste IT-Entwicklung angepasst werden können muss. Bei jedem neuen Update wäre eine neue Zertifizierung nötig. Das würde dazu führen, dass die Software während der neuen Prüfung nicht eingesetzt werden könnte. Es sind also pragmatische, praktische und auch technische Hindernisse, welche eine vorgängige Zertifizierung von Govware, gemeint durch den Bund, an und für sich gar nicht zulassen könnten. Diese Zertifizierung wäre zum andern mit grossem Aufwand verbunden. Die bekannten Programme würden einen Umfang von mehreren hunderttausend Programmzeilen aufweisen, deren Überprüfung immer einen grossen Aufwand nach sich zöge; es war da von mehreren Wochen die Rede. Entsprechend würden auch die Kosten dieser Programme durch die Zertifizierung um ein Mehrfaches wachsen.

Die KKJPD wurde von unserer Kommission explizit zu dieser neuen Bestimmung in Artikel 269quater angehört, und die Kantone haben uns mit aller Deutlichkeit gesagt, dass eine Lösung, wie sie dem Nationalrat vorschwebt, völlig unpraktikabel wäre. Auch die Frage der zentralen Beschaffung und der zentralen Entwicklung von Govware bei einem Dienst des Bundes lehnen die Kantone ab. Dies, weil sie sich auf den Standpunkt stellen, dass die Bedürfnisse der Kantone sehr unterschiedlich sind und dass die Kantone aufgrund der Strafverfolgungshoheit auch selber in der Lage wären, die für sie geeignete Software zu beschaffen bzw. entwickeln zu lassen. Zum andern scheitert die zentrale Beschaffung der Software aber auch an Haftungs- und Verantwortlichkeitsfragen, beispielsweise mündend in der Frage: Haftet der Bund oder haftet der Kanton gegenüber Dritten, wenn durch den Einsatz von Govware Schäden auf deren Zielsystem entstehen? Könnte der Bund verantwortlich gemacht werden, wenn er die Govware für eine angeordnete Überwachung nicht oder zu spät freigibt und deshalb Beweismittel verloren gegangen sind?

Das sind Überlegungen, die die Kommission dazu geführt haben, eine vorgängige Zertifizierung der Govware zu verweigern und eine zentrale Beschaffung von Govware für die Kantone durch den Bund als unpraktikabel zu bezeichnen. Das hat zur Folge, dass die Kommission Ihnen beantragt, die ersten drei Absätze zu belassen, dann allerdings die Absätze 4 und 5 zu streichen.

Angenommen

Ziff. II Ziff. 1 Art. 273 Abs. 3

Antrag der Kommission

Unverändert

Angenommen

Ziff. II Ziff. 1 Art. 286 Abs. 2 Bst. i

Antrag der Kommission

i. Waffengesetz vom 20. Juni 1997: Artikel 33 Absatz 3.

Angenommen

Ziff. II Ziff. 2 Art. 70ter Abs. 1

Antrag der Kommission

Zustimmung zum Beschluss des Nationalrates

Angenommen

Ziff. II Ziff. 2 Art. 70quater

Antrag der Kommission

Abs. 1-3

Zustimmung zum Beschluss des Nationalrates

Abs. 4, 5

Streichen

Angenommen

Ziff. II Ziff. 2 Art. 70d Abs. 3

Antrag der Kommission

Unverändert

Angenommen