

seine Aufgaben wirksam und – das habe ich gesagt – unter Beachtung des Subsidiaritätsprinzips wahrnehmen kann. Ich danke für die Leseempfehlung und kann nur bestätigen, dass dieser Bericht vielleicht eine gute Lektüre für die Weihnachtsferien sein könnte.

**Le président** (Comte Raphaël, président): La commission propose de prendre acte du rapport.

*Vom Bericht wird Kenntnis genommen  
Il est pris acte du rapport*

13.025

**Bundesgesetz  
betreffend die Überwachung  
des Post- und Fernmeldeverkehrs.  
Änderung  
Loi sur la surveillance  
de la correspondance par poste  
et télécommunication.  
Modification**

*Differenzen – Divergences*

Ständerat/Conseil des Etats 10.03.14 (Erstrat – Premier Conseil)  
Ständerat/Conseil des Etats 19.03.14 (Fortsetzung – Suite)  
Nationalrat/Conseil national 17.06.15 (Zweitrat – Deuxième Conseil)  
Nationalrat/Conseil national 17.06.15 (Fortsetzung – Suite)  
Ständerat/Conseil des Etats 07.12.15 (Differenzen – Divergences)

**Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs  
Loi fédérale sur la surveillance de la correspondance par poste et télécommunication**

**Engler** Stefan (C, GR), für die Kommission: Wir beraten also die Differenzen zum Überwachungsgesetz und dies in der ersten Phase der Differenzbereinigung. 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 stärker, aber besser überwachen zu können. Es geht im Unterschied zum Nachrichtendienstgesetz auch nicht um eine präventive Überwachung der Bürgerinnen und Bürger; das Überwachungsgesetz bezweckt keine flächendeckende Überwachung, wie sie offenbar der amerikanische Geheimdienst über Jahre bei Freund und Feind praktizierte. Es geht darum, zur Aufklärung von Straftaten die rechtlichen Voraussetzungen zur Überwachung des Fernmeldeverkehrs den technischen Entwicklungen anzupassen. Damit soll verhindert werden, dass durch die Verwendung neuer Technologien die Überwachung erschwert, wenn nicht sogar verhindert wird.

Was macht diese Vorlage so umstritten? Es sind die gegenläufigen Interessen. Der Schutz der Persönlichkeitsrechte und persönlicher Daten steht dem Interesse an einer wirksamen Strafverfolgung gegenüber, und diese beiden Faktoren konkurrieren wiederum mit den Interessen der Provider, ihr Geschäftsmodell möglichst ungehindert kommerziell anbie-

ten 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.

Einigkeit besteht darin: Je ausgefeilter die technischen Möglichkeiten sind, umso mehr haben wir in einem grundrechtssensiblen Bereich ein Auge auf den wirksamen Schutz der betroffenen Grundrechte zu richten.

**Art. 11 Abs. 6**

*Antrag der Kommission*  
Zustimmung zum Beschluss des Nationalrates

**Art. 11 al. 6**

*Proposition de la commission*  
Adhérer à la décision du Conseil national

*Angenommen – Adopté*

**Art. 12 Abs. 4–6**

*Antrag der Kommission*  
Streichen

**Art. 12 al. 4–6**

*Proposition de la commission*  
Biffer

**Engler** Stefan (C, GR), für die Kommission: Die Absicht des Nationalrates mit Artikel 12 war – im Übrigen hat der Nationalrat seine Fassung mit 90 zu 90 Stimmen und dem Stimmenscheid des Präsidenten beschlossen –, die Informatik-sicherheit im Überwachungsgesetz selber zu verankern. Die Kommission für Rechtsfragen anerkennt zwar die vom Nationalrat verfolgte Absicht, stellt sich jedoch auf den Standpunkt, dass das Thema der Informatik-sicherheit ins Datenschutzrecht 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 viel Interpretationsspielraum offen. Ein letztes 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 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 – Adopté*

**Art. 19 Abs. 4**

*Antrag der Kommission*  
Festhalten

**Art. 19 al. 4**

*Proposition de la commission*  
Maintenir

**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 diejenigen des Postverkehrs beantragt Ihnen die Kommission, am Beschluss des Ständerates, sie sechs Monate aufzubewahren, 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 entsprechend dem geltenden Recht wieder auf sechs Monate zurückzunehmen. Der Nationalrat war zuvor dem Ständerat gefolgt, der gemäss Entwurf des Bundesrates für die Randdaten aus dem Fernmeldeverkehr eine zwölfmonatige Aufbewahrungsfrist vorsah.

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 Differenzvereinbarung zurückkommen zu dürfen. Die Schwesterkommission hat uns die Zustimmung dafür erteilt. Warum diese Umkehr? Es handelt sich bekanntlich um das sensible Thema der Vorratsdatenspeicherung 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 zur Aufbewahrungsdauer 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 erfolgreichen Referendums möglicherweise erhöhen und die ganze Vorlage gefährden, was ganz und gar nicht im Interesse der Strafverfolgungsbehörde liegen würde. Das war, nebst den in den vergangenen ein- einhalb 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, also bei Artikel 19 Absatz 4, 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 wir Artikel 19 und Artikel 26 zusammen beraten.

Ich bitte Sie, hier dem Beschluss der Kommission zuzustimmen und die Frist bei diesen sechs Monaten zu belassen; das ist im Übrigen das geltende Recht. Wir sind ja gerade bei der 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 Aufbewahrungsfrist verlängern wollte. Wenn man daraus Folgerungen ableitet, 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 der Frist 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 weiter geht; da läuft ja noch kein Strafverfahren.

Ich bitte Sie, hier Ihrer Kommission zu folgen. Ich habe die Aufgabe gehabt, diese sechs Monate 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 zwölf 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 zwölf Monate und für den Postverkehr sechs Monate festzulegen? Sollen zweitens insgesamt sechs oder zwölf 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 – zwölf 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 sechs 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 Möglich-

keit 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, auch angesichts der Schwierigkeit, 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 dazu legiferiert; das war immer das erste und wichtigste Thema, dass ich mit den Justizministern diskutiert habe. In Deutschland liegt die Dauer der Vorratsdatenspeicherung jetzt bei zehn Wochen, Luxemburg hat sich für sechs Monate entschieden. Es gibt aber auch Staaten, die heute weiter gehen und zwölf 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 sechs 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 auf das geltende Recht 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 auf unserem Entwurf 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 – Adopté*

#### **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 Fernmeldediensteanbieter bestimmte dieser Daten nur zum Zweck der Identifikation während sechs Monaten aufbewahren und liefern müssen.

#### **Art. 21 al. 2**

##### *Proposition de la commission*

... durant toute la durée de la relation commerciale ainsi que durant six mois après la fin de celle-ci. Le Conseil fédéral

prévoit que les fournisseurs de services de télécommunication ne doivent conserver et livrer certaines de ces données durant six mois qu'à des fins d'identification.

#### **Art. 22 Abs. 2**

##### *Antrag der Kommission*

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

#### **Art. 22 al. 2**

##### *Proposition de la commission*

... de services de télécommunication doivent, durant toute la durée de la relation commerciale ainsi que six mois après la fin de celle-ci, posséder et livrer aux fins de l'identification. Le Conseil fédéral prévoit que les fournisseurs de services de télécommunication ne doivent conserver et livrer certaines de ces données durant six mois qu'à des fins d'identification. Ils doivent également livrer au service les autres indications dont ils disposent.

**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 im Speziellen 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.

Es geht also um Auskünfte. 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 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 Surf-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, 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 Kommissionsprechers 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 Anbieter 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 aufbe-



wahrt 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 zuhänden der Materialien festhalten.

*Angenommen – Adopté*

#### **Art. 24**

*Antrag der Kommission*

Zustimmung zum Beschluss des Nationalrates

*Proposition de la commission*

Adhérer à la décision du Conseil national

**Sommaruga** Simonetta, Bundespräsidentin: Auch hier möchte ich zuhänden 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 einen bestimmten geografischen Punkt oder deckt ihn gemäss Abdeckungsinformationen der Fernmeldediensteanbieter ab? Welche Charakteristiken hat eine Antenne – beispielsweise hinsichtlich der Art, der Abstrahlungsrichtung, der Technologie, des Frequenzbands? Werden ankommende Anrufe eines Anschlusses über einen anderen Fernmeldediensteanbieter abgewickelt als die ausgehenden Anrufe? 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?

So weit meine Ausführungen zuhänden der Materialien.

*Angenommen – Adopté*

#### **Art. 26**

*Antrag der Mehrheit*

*Abs. 5*

... des Fernmeldeverkehrs während sechs Monaten aufbewahren.

*Abs. 5bis*

Streichen

*Antrag der Minderheit*

(Cramer, Levrat)

*Abs. 5bis*

Zustimmung zum Beschluss des Nationalrates

#### **Art. 26**

*Proposition de la majorité*

*Al. 5*

... de télécommunication durant six mois.

*Al. 5bis*

Biffer

*Proposition de la minorité*

(Cramer, Levrat)

*Al. 5bis*

Adhérer à la décision du Conseil national

**Le président** (Comte Raphaël, président): La discussion sur l'alinéa 5 a déjà eu lieu lors du débat sur l'article 19 alinéa 4.

**Engler** Stefan (C, GR), für die Kommission: Zu Artikel 26 Absatz 5bis finden Sie eine Minderheit vor. 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 begründen würde, weshalb sie auf die nationalrätliche Fassung umschwenken 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 avons examiné ce projet de loi.

Que nous dit la Cour de justice de l'Union européenne? Elle nous indique qu'il faut être très attentif lorsque l'on recherche un «Safe Harbor», c'est-à-dire lorsque l'on recherche un «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 lorsque l'on y a déposé ses données, personne d'autre n'y aura accès. La Cour de justice de l'Union européenne, qui a été saisie par des cas provenant de 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 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 la question s'est 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 sage-ment, 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 de bénéficier 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, müssen in der Schweiz aktive Unternehmungen doch das schweizerische Datenschutzrecht auch 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 bloss 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 Pflicht zur Aufbewahrung in der Schweiz hätte somit weitreichende und negative Auswirkungen, vor allem für international tätige Telekommunikationsunternehmen. 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 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 Unternehmen gehen in der Regel sorgsam mit diesen sensiblen Daten um und stellen durch physische und prozessbezogene Massnahmen die Sicherheit und die gesetzeskonforme Verwendung der Randdaten sicher.

Ein zusätzliches Argument dafür, dass sich die Mehrheit dagegen ausgesprochen hat, einen exklusiven Aufbewah-

rungsort 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 wie von Versicherungen oder medizinischen Labors usw. nicht auch exklusiv in der Schweiz aufbewahrt werden müssten. Die Kommission betrachtet deshalb die Formulierung des Nationalrates zwar als gutgemeint, allerdings nicht im Interesse der Wirtschaft. Die Formulierung trägt auch nicht dazu bei, die Datensicherheit zu erhöhen.

**Sommaruga Simonetta, Bundespräsidentin:** Der Nationalrat und Ihre Kommissionsminderheit möchten hier eigentlich eine Swissness-Regel für Fernmeldediensteanbieter 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: Eine solche 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 Aufbewahren von Daten in Bezug auf den Datenschutz nur in der Schweiz möglich sei und die Schweizer Datenschutzbestimmungen nicht mehr gelten würden, wenn ein Unternehmen z. B. Daten in einem anderen Land speichern würde, dann wäre dieser Eindruck 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 noch 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 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 der Nationalrat und die Minderheit vorschlagen, zu einer Einschränkung der Wirtschaftsfreiheit führen würde. Denn die Fernmeldediensteanbieter 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 Vertauung 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, dem Antrag der Mehrheit zuzustimmen.

#### *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

#### **Art. 42 al. 2**

##### *Proposition de la commission*

Adhérer à la décision du Conseil national

*Angenommen – Adopté*

#### **Art. 45 Abs. 3**

##### *Antrag der Kommission*

Streichen

#### **Art. 45 al. 3**

##### *Proposition de la commission*

Biffer

*Angenommen – Adopté*

### **Aufhebung und Änderung bisherigen Rechts Abrogation et modification du droit en vigueur**

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

##### *Antrag der Kommission*

Zustimmung zum Beschluss des Nationalrates

#### **Ch. II ch. 1 art. 269 al. 2 let. a**

##### *Proposition de la commission*

Adhérer à la décision du Conseil national

*Angenommen – Adopté*

#### **Ziff. II Ziff. 1 Art. 269quater**

##### *Antrag der Kommission*

*Abs. 1–3*

Zustimmung zum Beschluss des Nationalrates

*Abs. 4, 5*

Streichen

#### **Ch. II ch. 1 art. 269quater**

##### *Proposition de la commission*

*Al. 1–3*

Adhérer à la décision du Conseil national

*Al. 4, 5*

Biffer

**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. Der Nationalrat hat die Rahmenbedingungen dafür neu definiert, indem er der Sicherheit und der Qualität solcher 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 dazu leisten können, den Umgang mit solcher Software sicherer und verlässlicher zu machen.

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 Auswahl der Massnahmen dafür. 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 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 ausschliessen. Eine Zertifizierung wäre zudem mit grossem Aufwand verbunden. Die bekannten Programme würden einen Umfang von mehreren hunderttausend Programmzeilen aufweisen, deren Überprüfung einen grossen Aufwand nach sich zöge; es war 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 dazu angehört. Die Kantone haben uns mit aller Deutlichkeit gesagt, dass eine Lösung, wie sie dem Nationalrat vorschwebt, völlig unpraktikabel wäre. Auch das Thema der zentralen Beschaffung und der zentralen Entwicklung von Govware bei einem Dienst des Bundes lehnen die Kantone ab. Sie stellen sich auf den Standpunkt, dass ihre Bedürfnisse sehr unterschiedlich sind und dass sie 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? Kann der Bund verantwortlich gemacht werden, wenn er die Govware für eine angeordnete Überwachung nicht oder zu spät freigibt und deshalb Beweismittel verlorengangen sind?

Mit diesen Überlegungen lehnt die Kommission eine vorgängige Zertifizierung und eine zentrale Beschaffung von Govware für die Kantone durch den Bund ab. Das hat zur Folge, dass die Kommission Ihnen beantragt, die ersten drei Absätze zu belassen, allerdings die Absätze 4 und 5 zu streichen.

*Angenommen – Adopté*

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

##### *Antrag der Kommission*

Unverändert

#### **Ch. II ch. 1 art. 273 al. 3**

##### *Proposition de la commission*

Inchangé

*Angenommen – Adopté*

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

##### *Antrag der Kommission*

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

#### **Ch. II ch. 1 art. 286 al. 2 let. i**

##### *Proposition de la commission*

i. loi du 20 juin 1997 sur les armes: article 33 alinéa 3.

*Angenommen – Adopté*

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

##### *Antrag der Kommission*

Zustimmung zum Beschluss des Nationalrates



**Ch. II ch. 2 art. 70ter al. 1***Proposition de la commission*

Adhérer à la décision du Conseil national

*Angenommen – Adopté***Ziff. II Ziff. 2 Art. 70quater***Antrag der Kommission*

Abs. 1–3

Zustimmung zum Beschluss des Nationalrates

Abs. 4, 5

Streichen

**Ch. II ch. 2 art. 70quater***Proposition de la commission*

Al. 1–3

Adhérer à la décision du Conseil national

Al. 4, 5

Biffer

*Angenommen – Adopté***Ziff. II Ziff. 2 Art. 70d Abs. 3***Antrag der Kommission*

Unverändert

**Ch. II ch. 2 art. 70d al. 3***Proposition de la commission*

Inchangé

*Angenommen – Adopté*

15.3849

**Postulat Stöckli Hans.  
Flexiblere Kollektivverwertung  
im Urheberrecht****Postulat Stöckli Hans.  
Flexibiliser la gestion collective  
en matière de droit d'auteur**

Ständerat/Conseil des Etats 07.12.15

**Le président** (Comte Raphaël, président): Le Conseil fédéral propose de rejeter le postulat.

**Stöckli Hans** (S, BE): Mit meinem Postulat wollte ich erreichen, dass der Bundesrat im Rahmen der jetzt anstehenden Revision des Urheberrechtsgesetzes auch die Möglichkeit eröffnet, die sogenannte erweiterte Kollektivlizenz ins Spiel zu bringen. Denn es ist tatsächlich so, dass die heute vorhandenen rechtlichen Möglichkeiten ungenügend sind, wenn es um Kollektivverwertung geht. Wir haben die freiwillige Kollektivlizenz und die obligatorische Kollektivverwertung. Bei der freiwilligen Kollektivlizenz haben wir das Problem, dass der Rechtserwerb unvollständig ist, da er auf die Mitglieder der Verwertungsgesellschaften beschränkt bleibt. Bei der obligatorischen Kollektivverwertung haben wir das Problem, dass diese Art der Verwertung etwa im Online-Bereich ungenügend ist. Seit über fünfzig Jahren wird vor allem in den skandinavischen Ländern die erweiterte Kollektivlizenz, die «extended collective license», angewandt. Dies mit grossem Erfolg: Sowohl die Nutzer wie auch die Berechtigten unterstützen diese Möglichkeit. Auch in den EU-Richtlinien hat sich diese erweiterte Kollektivlizenz durchgesetzt. Nun bin ich natürlich sehr froh, dass der Bundesrat schneller bereit ist, dieses Projekt anzugehen, als ich es mit einem Bericht erreicht hätte. Ich bin dementsprechend erfreut und bereit, das Postulat zurückzuziehen, wenn mich die Frau Bundespräsidentin noch mit zwei Antworten beehrt. Meine

erste Frage: Wie sieht der Zeitplan aus, um dieses Projekt der Revision der Urheberrechtsgesetzgebung, das noch viele andere Themen beinhaltet, voranzutreiben? Das Zweite: Ich gehe davon aus, dass die Vernehmlassungsvorlage, wenn sie dann im Bundesrat ist, auch die erweiterte Kollektivlizenz enthalten wird und diese nach der Beratung durch den Bundesrat ebenfalls noch im Projekt enthalten ist. Insgesamt: Herzlichen Dank, dass der Bundesrat dieses Anliegen so schnell in den Vernehmlassungsentwurf einbeziehen will.

**Sommaruga Simonetta**, Bundespräsidentin: Ich fand eigentlich nicht, dass wir hier wahnsinnig schnell vorwärtskommen würden. Wenn Sie das so sehen, wird es wohl so sein.

Wir haben im Jahr 2012 eine Arbeitsgruppe zum Urheberrecht eingesetzt, die Agur 12. Diese ist seit 2012 am Arbeiten und hat auch diese Fragen zum Instrument der erweiterten Kollektivlizenz angeschaut. Deshalb kann ich Ihre Fragen jetzt auch sehr kurz beantworten. Der Bundesrat wird noch in diesem Jahr – so lange geht dieses ja nicht mehr – die Vernehmlassung eröffnen. Und er wird im Rahmen der Vernehmlassungsvorlage aufzeigen, wie die erweiterte Kollektivlizenz im Urheberrechtsgesetz verankert werden kann. Insofern haben wir Sie überholt.

Es handelt sich nicht um ein einfaches Geschäft. Es gibt in dieser Vernehmlassung sehr unterschiedliche, divergierende, sich widersprechende und kaum zusammenzubringende Interessen. Das wird also noch etwas dauern. Jedenfalls wird die Vernehmlassung nächstens beginnen. Dann wird man auch diese Frage diskutieren. Auch dieses Thema ist, wie Sie das gewünscht haben, in der Vernehmlassungsvorlage enthalten.

**Le président** (Comte Raphaël, président): L'auteur du postulat est-il prêt à le retirer, suite à la réponse de Madame la conseillère fédérale Sommaruga?

**Stöckli Hans** (S, BE): Ja, ich ziehe mein Postulat zurück.

*Zurückgezogen – Retiré*

15.3876

**Interpellation Stöckli Hans.  
Video-on-Demand-Nutzungen.  
Vergütung für Filmurheber  
und -schauspieler****Interpellation Stöckli Hans.  
Services de vidéo à la demande.  
Rémunération des auteurs de films  
et des acteurs**

Ständerat/Conseil des Etats 07.12.15

**Le président** (Comte Raphaël, président): L'auteur de l'interpellation s'est déclaré non satisfait de la réponse écrite du Conseil fédéral et demande l'ouverture de la discussion. – Ainsi décidé.

**Stöckli Hans** (S, BE): Im Gegensatz zum soeben behandelten Thema bin ich hier beim zweiten Vorstoss nicht sehr glücklich über die Antwort des Bundesrates und muss mich als nicht befriedigt erklären.

Der Bundesrat führt aus, dass tatsächlich ein Ungleichgewicht zwischen den Urhebern und denjenigen, welche die Leistungen dann vermarkten, vorhanden sei. Er sagt zur Video-on-Demand-Verwertung aber: «Wenn die Urheber und Interpreten bei der VoD-Verwertung für ihr Schaffen nicht oder ungenügend entschädigt werden, liegt dies nicht an ei-