



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

CHRONOLOGIE

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)
NATIONALRAT/CONSEIL NATIONAL 03.03.16 (DIFFERENZEN - DIVERGENCES)
STÄNDERAT/CONSEIL DES ETATS 08.03.16 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 14.03.16 (DIFFERENZEN - DIVERGENCES)
STÄNDERAT/CONSEIL DES ETATS 16.03.16 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 16.03.16 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 18.03.16 (SCHLUSSABSTIMMUNG - VOTE FINAL)
STÄNDERAT/CONSEIL DES ETATS 18.03.16 (SCHLUSSABSTIMMUNG - VOTE FINAL)

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

Art. 12 Abs. 4–6

Antrag der Kommission

Zustimmung zum Beschluss des Ständerates

Art. 12 al. 4–6

Proposition de la commission

Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 19 Abs. 4

Antrag der Mehrheit

Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)
Festhalten

Art. 19 al. 4

Proposition de la majorité

Adhérer à la décision du Conseil des Etats





Proposition de la minorité

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

Maintenir

Art. 21 Abs. 2

Antrag der Mehrheit

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

Antrag der Minderheit

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

... und während der Dauer der Kundenbeziehung sowie während zwölf Monaten nach deren Beendigung geliefert werden können. Der Bundesrat legt fest, dass die Fernmeldediensteanbieter bestimmte dieser Daten zum Zweck der Identifikation nur während zwölf Monaten aufbewahren und liefern müssen.

Art. 21 al. 2

Proposition de la majorité

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

Proposition de la minorité

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

... durant toute la durée de la relation commerciale ainsi que durant douze 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 à des fins d'identification que durant douze mois.

Art. 22 Abs. 2

Antrag der Mehrheit

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

Antrag der Minderheit

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

... zum Zweck der Identifikation während der Dauer der Kundenbeziehung sowie während zwölf Monaten nach deren Beendigung bereithalten und liefern müssen. Der Bundesrat legt fest, dass die Fernmeldediensteanbieter bestimmte dieser Daten zum Zweck der Identifikation nur während zwölf Monaten aufbewahren und liefern müssen ...

Art. 22 al. 2

Proposition de la majorité

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

Proposition de la minorité

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

... de services de télécommunication doivent, durant toute la durée de la relation commerciale ainsi que douze 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 à des fins d'identification que durant douze mois ...

Art. 26 Abs. 5

Antrag der Mehrheit

Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)



Festhalten

AB 2016 N 132 / BO 2016 N 132

Art. 26 al. 5*Proposition de la majorité*

Adhérer à la décision du Conseil des Etats

Proposition de la minorité

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

Maintenir

Geissbühler Andrea Martina (V, BE): Mit der Minderheit fordere ich eine zwölfmonatige Aufbewahrungszeit für die Randdaten des Post- und Fernmeldeverkehrs. In den Kommissionen für Rechtsfragen des Nationalrates und des Ständerates waren nach der Beratung die meisten Parlamentarier für zwölf Monate und folgten damit den Empfehlungen des Bundesrates und der Strafverfolgungsbehörden, dies zugunsten der Sicherheit in unserem Land. Dann kam ganz unerwartet ein Rückkommensantrag der Kommission für Rechtsfragen des Ständerates, obwohl keine neuen Fakten bekanntgeworden waren und es keine neuen Begründungen dafür gab, warum sechs Monate ausreichend sein sollten. Daher ist die Minderheit nach wie vor für eine zwölfmonatige Aufbewahrungsfrist.

Bei den hier relevanten Delikten geht es vorwiegend um grenzüberschreitende Kriminalität. Wir sprechen also von schweren Delikten und nicht von Bagatelldelikten. Da die Strafverfolgungsbehörden mit zeitlicher Verzögerung von einem Delikt erfahren und da nochmals Zeit vergeht, bis ein Verfahren eröffnet wird, ist es wichtig, dass die Daten zwölf Monate lang gespeichert werden. Diese Frist von zwölf Monaten ist für die Verfolgung von schweren Delikten entscheidend. Nur so ist eine wirksame Strafverfolgung möglich.

Auch bei der Forderung nach einer zwölfmonatigen Aufbewahrungszeit wird nach den Prinzipien der Gesetzmässigkeit und der Verhältnismässigkeit so wenig wie möglich in die Grundrechte eingegriffen. Die Strafverfolgungsbehörden müssen glaubhaft darlegen, dass für die Aufklärung des Deliktes die Notwendigkeit einer allfälligen Überwachung oder Abhörung gegeben ist. Zudem muss ein Gesuch an den Provider gestellt werden, und die Einwilligung der Staatsanwaltschaft muss vorliegen. Erst dann können die Daten herausgegeben werden.

Es ist also sicher nicht so, dass jeder Polizist Zugang zu diesen Daten hätte. Auch haben die Strafverfolgungsbehörden weder die finanziellen noch die personellen Ressourcen, um irgendwelchen Kleinkriminellen nachzuspionieren.

Ich habe hier noch einen interessanten Vergleich: Gemäss Artikel 958f des Obligationenrechts muss eine Firma ihre Geschäftsbücher und Buchungsbelege während zehn Jahren aufbewahren. Bei dem zur Diskussion stehenden Gesetz geht es aber um schwere Straftaten, und unser Ziel muss es sein, diese aufzuklären. Dazu brauchen wir eine Aufbewahrungsfrist von zwölf Monaten.

Ich bitte Sie, dem Antrag meiner Minderheit – zwölf Monate Aufbewahrungsfrist für Randdaten – zuzustimmen.

Merlini Giovanni (RL, TI): Bei Artikel 19 Absatz 4 und Artikel 26 Absatz 5 geht es um die Dauer der Randdatenaufbewahrung durch die Anbieter im Zusammenhang mit der Überwachung des Postverkehrs bzw. des Fernmeldeverkehrs. Die Frage der Dauer der Randdatenaufbewahrung sollte aber im Rahmen dieser wichtigen Revision nicht hochstilisiert werden.

Wesentlich ist für die FDP-Liberale Fraktion, dass die Strafverfolgungsbehörden möglichst rasch auf die verschlüsselte Kommunikation Zugriff haben können. Es ist also nicht so wichtig, ob die Aufbewahrungsdauer bei zwölf Monaten belassen oder auf sechs Monate reduziert wird, wie es der Ständerat beschlossen hat. Wichtiger ist unseres Erachtens, dass eine einheitliche Regelung für den Postverkehr sowie für den Fernmeldeverkehr gilt. Diese Randdaten werden ja nicht vom Staat, sondern von privaten Telekommunikationsunternehmen aufbewahrt. Je länger man diese Randdaten bei einer privaten Gesellschaft aufbewahrt, umso grösser ist das Risiko, dass Privatpersonen Zugang zu Daten unserer Bürgerinnen und Bürger erhalten. Es gilt also, dieses Risiko zu minimieren, indem wir die Randdatenspeicherung auf eine Dauer von sechs Monaten reduzieren. Im Übrigen werden dadurch auch die Aufbewahrungskosten für die verpflichteten Unternehmen tiefer gehalten. Ich bitte Sie deshalb, der Mehrheit zu folgen.



Guhl Bernhard (BD, AG): Der BDP ist die Sicherheit sehr wichtig. Die Strafverfolgungsbehörden müssen moderne Mittel und Werkzeuge haben, um organisierte Kriminalität wie Drogenhandel, Menschenhandel, Mafia usw. bekämpfen zu können. Die Vorlage ist diesbezüglich auf einem guten Stand. Kriminelle können sich bei der jetzigen Vorlage nicht mehr mit Verschlüsselungstechnologien verstecken. Damit man verschlüsselte Technologien wie beispielsweise Skype überwachen kann, braucht es diese Govware. Die Vorlage ist also so weit gut.

Ich nehme an, dass von Ihnen niemand mehr mit dem Betriebssystem DOS arbeitet: Sie gehen mit der Zeit und nutzen die neuesten Systeme, sei es Windows 10 oder Apple. Sehen Sie, die Verbrecher nutzen diese auch. Darum ist diese Vorlage enorm wichtig.

Die wesentliche Differenz zum Ständerat ist die Dauer der Aufbewahrung der Randdaten des Postverkehrs und der Fernmeldedienste. In einem Punkt sind wir uns hoffentlich einig: Es macht keinen Sinn, unterschiedliche Fristen für Post- und Fernmeldeverkehr festzulegen. Doch auf welche Dauer wollen wir uns festlegen? Es ist in der Realität leider so, dass die Aufklärung komplexer Kriminalfälle einiges länger dauert als gewünscht. In der echten Welt geht es bei den Ermittlungen um einiges langsamer, als dies z. B. bei der Sendung "CSI: Miami" der Fall ist. Zuerst muss man in Fällen organisierter Kriminalität lange recherchieren. Gewissen Tätern kommt man erst sehr spät auf die Schliche. Dann ist es so – und das sieht man auch bei den Krimis selten –, dass die Fälle über die Landesgrenzen hinausreichen und man Rechtshilfeersuchen stellen muss, und das dauert sehr lange. Es dauert teilweise Monate, bis man Antworten aus dem Ausland kriegt, und dann ist es gegebenenfalls zu spät.

Strafverfolgungsbehörden und Strafrechtsprofessoren votieren denn auch entschieden für die Speicherung dieser Daten während zwölf Monaten. Die Fernmeldediensteanbieter haben ja Bedenken, dass es was weiss ich wie viel kostet, wenn man die Frist bei zwölf statt bei sechs Monaten festlegt. Ich höre immer wieder Berichte darüber, was für einen grossen Wert die Daten haben und wie viele Daten die Fernmeldedienstleister für sich zu Marketingzwecken speichern. Also sind diese Randdaten – nur wenige Zeichen – ein Klacks, gemessen an dem, was die Fernmeldediensteanbieter für ihr Marketing speichern. Dieses Argument kann man also nicht gelten lassen.

Wie gesagt, der BDP ist die Aufklärung von Verbrechen wichtig. Dazu brauchen wir diese Aufbewahrungsfrist von zwölf Monaten.

Ich bitte Sie, bei diesen Artikeln, in denen es um die Dauer der Aufbewahrung geht, dem Antrag auf zwölf Monate zuzustimmen, also der Minderheit zu folgen.

Vogler Karl (C, OW): Namens der CVP-Fraktion ersuche ich Sie, bei Artikel 19 Absatz 4 und Artikel 26 Absatz 5 der jeweiligen Minderheit zu folgen.

Erinnern wir uns: Anlässlich der Debatte vom 17. Juni 2015 hat die Mehrheit dieses Rates noch klar Ja gesagt zu der jetzt nur noch von der Minderheit unterstützten Aufbewahrungsdauer von zwölf Monaten für Randdaten, der Aufbewahrungsdauer notabene, die damals vom Bundesrat vorgeschlagen und im Rat von der Frau Bundesrätin bzw. damals Frau Bundespräsidentin auch engagiert vertreten wurde. Frau Bundesrätin Sommaruga sagte damals: "Warum wollen wir diese Erhöhung von heute sechs auf neu zwölf Monate bei der Randdatenspeicherung? Weil die Erfahrung gezeigt hat, dass es bei der Ermittlung von Straftaten oft eine gewisse Zeit braucht! Damit diese Zeit auch vorhanden ist, zum Beispiel wenn es um Rechtshilfeersuchen, um komplexe Fälle geht, möchten wir eine

AB 2016 N 133 / BO 2016 N 133

Erhöhung" (AB 2015 N 1149) – notabene eine Erhöhung auf zwölf Monate. Weiter sagte sie dann bei der Detailberatung: "Sollten Sie trotzdem beschliessen, dass die Aufbewahrungsfrist für Randdaten verkürzt wird oder dass diese gar nicht mehr benutzt werden dürfen, müssen Sie sich bewusst sein, dass Sie für die Strafverfolgung in verschiedenen Bereichen Erschwerungen einführen oder diese insgesamt sogar verunmöglichen. Gerade bei komplexen Kriminalfällen, und das ist in den Bereichen des organisierten Verbrechens oder des Terrorismus der Fall, sind diese Fristen von sechs Monaten heute häufig einfach zu kurz." (AB 2015 N 1160) So weit das, was die Frau Bundesrätin anlässlich der Debatte vom Juni 2015 gesagt hat.

Jetzt sagt man, es gebe unterschiedliche Diskussionen in verschiedenen europäischen Staaten zu dieser Aufbewahrungsdauer und es rege sich politischer Widerstand gegen das Gesetz. Man könne auch mit sechs Monaten leben; wichtig sei, dass das Gesetz möglichst rasch in Kraft trete, damit man beim Problem der verschlüsselten Kommunikation vorankomme. Da habe nicht nur ich, da hat die Politik als Gesamtes ein Glaubwürdigkeitsproblem! Wie soll man im Hinblick auf die wirksame Bekämpfung von schweren Verbrechen nach aussen glaubhaft erklären, dass sechs Monate nun plötzlich ausreichend sind, wenn auch der Bundesrat bis



vor Kurzem klar und deutlich für zwölf Monate eingetreten ist? Entsprechend wäre es absolut falsch, jetzt einfach zu sagen, wir wollten ein Referendum abwenden und verzichteten darum auf einen wichtigen Punkt in dieser Vorlage.

Die Ausgangslage hat sich nämlich überhaupt nicht geändert – es gibt keinen einzigen sachlichen Grund, die Aufbewahrungsdauer plötzlich um die Hälfte zu verkürzen. Dafür spricht einzig politischer Opportunismus, und diesem sollten wir nicht verfallen. Ich bin überzeugt, eine allfällige Referendumsabstimmung ist zu gewinnen, wenn mit überzeugenden Argumenten auf die Notwendigkeit einer entsprechenden Aufbewahrungsdauer von zwölf Monaten verwiesen werden kann. Diese Notwendigkeit ist im Hinblick auf eine wirksame Aufklärung und Bekämpfung schwerer Verbrechen gegeben. Weichen wir von der notwendigen Dauer ab, hat die Politik, ich habe es gesagt, ein Glaubwürdigkeitsproblem.

Namens der CVP-Fraktion ersuche ich Sie, dem Antrag der Minderheit zuzustimmen. Das gilt auch betreffend Artikel 21 Absatz 2 und Artikel 22 Absatz 2 – es geht hier letztendlich um die gleichen Fragen.

Schwander Pirmin (V, SZ): Hier geht es um eine Gratwanderung zwischen Sicherheit und Freiheit. Deshalb sind die einen unserer Fraktion für dieses Gesetz und die anderen gegen dieses Gesetz.

Es ist jetzt vielfach von Sicherheit gesprochen worden. Ich bin überzeugt: Die grösste Sicherheit in einem Rechtsstaat ist gewährleistet, wenn die Persönlichkeitsrechte nach wie vor geschützt sind. Diese Persönlichkeitsrechte dürfen nicht verwässert werden. Es geht aber hier ja nicht mehr um eine Grundsatzdebatte, sondern um diese Differenzen bei der Aufbewahrungsfrist und bei der Frage, wo die Daten entsprechend aufbewahrt werden. Es ist für uns klar: Wenn wir eine Frist haben, soll diese sowohl für den Postverkehr wie auch für den Fernmeldeverkehr gleich sein. Das ist an und für sich klar.

Nun zum Thema sechs Monate oder zwölf Monate: Bei uns ist eine Mehrheit für sechs Monate, da es eben auch um Persönlichkeitsrechte geht. Wir haben jedoch bis heute eben keine Gründe dafür gehört, dass wir von zwölf auf sechs Monate gehen sollen. Diese möchten wir heute noch hören, weil in der ersten Diskussion ganz klar gesagt wurde, eine Frist von zwölf Monaten sei wichtig, das sei das Kernstück dieser Vorlage; ohne diese zwölf Monate würde die ganze Vorlage verwässert. Deshalb wurden hier, in diesem Saal, diese zwölf Monate vehement vertreten. Ich denke, wir haben tatsächlich aus Sicht der SVP ein Glaubwürdigkeitsproblem, wenn wir jetzt plötzlich von zwölf auf sechs Monate gehen – selbst wenn wir das mehrheitlich unterstützen, das muss ich Ihnen auch sagen. Einige von uns sind aber auch gegen dieses Gesetz.

Grüter Franz (V, LU): Sie haben es gehört, wir haben zwei Differenzen: jene zur Frage, ob die Vorratsdatenspeicherung sechs oder zwölf Monate dauern soll, und die andere zur Frage, ob diese Daten nur in der Schweiz oder auch im Ausland gespeichert werden sollen.

Zur ersten Differenz: Es geht hier nicht darum, Verbrechen aufzuklären; es geht hier darum, ob die Kommunikationsdaten von Millionen von Schweizerinnen und Schweizern – auch Ihre Daten – zwölf oder sechs Monate gespeichert werden sollen. Es handelt sich dabei um E-Mail-, Telefonranddaten und die gesamten Bewegungsdaten, die darüber Auskunft geben, wo wir uns befunden und wie wir uns bewegt haben.

Nein, Herr Kollege Vogler, es ist kein politischer Opportunismus. Es geht hier wirklich um die Frage, ob wir so weit gehen wollen, dass für die Aufklärung einiger weniger Verbrechen von allen Schweizern so grosse, riesige Datenmengen gespeichert werden sollen.

Ich zitiere den Ersten Staatsanwalt des Kantons St. Gallen, Thomas Hansjakob, der vor wenigen Wochen öffentlich gesagt hat, dass in 99 Prozent aller Fälle eine Vorratsdatenspeicherung von sechs Monaten völlig ausreiche. Österreich hat die Vorratsdatenspeicherung sogar vollständig abgeschafft, und in vielen anderen europäischen Ländern umfasst sie lediglich den Zeitraum von drei bis sechs Wochen. Ich plädiere nicht für drei bis sechs Wochen, doch sechs Monate reichen vollends aus.

Der Staat hat zudem neu mit diesem Überwachungssystem Online-Zugriff auf die Telekommunikationsanbieter. Es ist also nicht mehr so, dass die Daten beim Telekommunikationsanbieter gespeichert werden und dann dort angefragt wird. Vielmehr besteht die Möglichkeit, online auf die Daten zuzugreifen.

Sagen Sie deshalb Nein zu einer unverhältnismässigen, überbordenden Massnahme, zu einem Eingriff in die Grundrechte, in die Freiheitsrechte von uns Bürgerinnen und Bürgern! Gewichten Sie das höher als die allfällige Aufklärung einiger weniger Fälle!

Zur zweiten Differenz, zum Standort der Speicherung dieser Daten: Hier plädiere ich dafür, dass sie unbedingt in der Schweiz gespeichert werden. Stellen Sie sich einmal vor, dass alle unsere Daten auf einem Grossrechner irgendwo in den USA oder sonst irgendwo gespeichert würden. Es wäre schon sehr schwer zu verstehen, dass Daten in einem Land gespeichert werden sollen, in dem eine andere Gesetzgebung herrscht, wo wir doch alle wissen, dass Staaten dann ganz andere Zugriffsrechte auf diese Daten haben. Ich erwarte also deshalb



schon, dass diese Daten, wenn überhaupt, dann in der Schweiz gespeichert werden.

Guhl Bernhard (BD, AG): Werter Herr Ratskollege, eine Sache möchte ich gleich richtigstellen: Online-Zugriff haben die Strafverfolgungsbehörden also nicht; sie können nicht direkt auf die Daten zugreifen. Die Anträge der Staatsanwaltschaften und die entsprechenden richterlichen Beschlüsse braucht es dann schon.

Meine Frage an Sie: Sie sagen, in 99 Prozent der Fälle würden die sechs Monate reichen. Aber das eine Prozent an Straffällen wollen Sie nicht aufklären? Ist Ihnen und Ihrer Partei die Aufklärung möglichst vieler Straftaten der organisierten Kriminalität nicht wichtig?

Grüter Franz (V, LU): Ich frage mich natürlich, ob es wirklich immer so lange dauern muss, bis diese Anfragen kommen. Ich erlaube mir den Fall in Emmen zu zitieren, bei dem erst jetzt gerade, nach mehr als zwölf Monaten, diese Daten nachgefragt werden. Es ist mir schleierhaft, weshalb das nicht schneller möglich sein soll, wie gesagt in sechs Monaten. Selbst die Staatsanwälte sind der Meinung, dass das in fast allen Fällen immer ausreicht. Ich gewichte die Freiheit höher.

AB 2016 N 134 / BO 2016 N 134

Allemann Evi (S, BE): Die SP-Fraktion unterstützt in den diversen betroffenen Artikeln die Mehrheit, die für eine sechsmonatige Aufbewahrungsfrist ist. Mitten in die Büpf-Beratungen ist das Urteil des Europäischen Gerichtshofes gefallen. Dieses Urteil hat die Voraussetzungen für die Aufbewahrung von Randdaten massiv verschärft. In Deutschland zum Beispiel ist man in der Folge auf eine zehnwöchige Aufbewahrungsfrist gegangen.

Für die Schweiz ist dieses Urteil nicht verbindlich, das ist richtig. Aber es hat auch bei uns zu einer gewissen Unsicherheit geführt und vor allem zu neuen Gesprächen. Das Fazit daraus war, dass man vorerst beim geltenden Recht bleibt, bei sechs Monaten, und abwartet, wie sich das auf europäischer Ebene weiterentwickelt. Die Frist von sechs Monaten ist also nicht ein Zurückgehen gegenüber heute, es ist schlicht das geltende Recht.

Ein anderes Argument kommt für uns noch dazu: Die Länge der Frist für die Randdatenaufbewahrung ist weniger wesentlich als vielmehr die Tatsache, dass die Strafverfolgungsbehörden überhaupt Zugriff darauf haben und die Möglichkeit erhalten, verschlüsselte Kommunikation zu überwachen, um schwere Verbrechen zu bekämpfen. Die Verlängerung der Aufbewahrungsfrist hat so gesehen zweite Priorität. Angesichts der entstandenen Unsicherheit nach dem Urteil ist es umso vertretbarer, beim geltenden Recht mit sechs Monaten zu bleiben.

Ich bitte Sie im Namen der SP-Fraktion, der Mehrheit zu folgen.

Arslan Sibel (G, BS): Wir, die Grünen, haben immer wieder die lange Dauer der Aufbewahrung der Randdaten kritisiert. Wir haben letztes Jahr hier mit einem Rückweisungsantrag den vollständigen Verzicht auf die Vorratsdatenspeicherung gefordert und alternativ dafür plädiert, dass die Daten höchstens drei Monate aufbewahrt werden sollten.

Die Kommission hat nun immerhin einen Kompromiss gefunden. Die Mehrheit schlägt sowohl beim Postverkehr wie auch beim Fernmeldeverkehr vor, die Vorratsdatenspeicherung nicht von heute sechs auf zwölf Monate zu verdoppeln. Die Fristen beim Postverkehr und beim Fernmeldeverkehr waren im ersten Beschluss des Ständerates unterschiedlich. Doch die Kommission ist sich einig, dass es keinen Sinn macht, dass bei der Gesetzgebung zum Post- und zum Fernmeldeverkehr unterschiedliche Fristen bestehen.

Wir haben es gehört, der Europäische Gerichtshof hat eine Regelung von Deutschland gekippt, welche für die Speicherung von Vorratsdaten eine lange Frist vorgesehen hatte. Nun sind die Fristen in Deutschland neu auf zehn Wochen gesenkt worden. Auch andere Länder haben die Aufbewahrungsfristen nicht ausgedehnt. Lange Aufbewahrungsfristen bringen konsequenterweise auch Verpflichtungen mit sich.

Es ist klar, dass die Grünen den Kompromiss von sechs Monaten der Ausdehnung der Frist vorziehen. Grundsätzlich sind wir aber nach wie vor der Vorratsdatenspeicherung gegenüber kritisch eingestellt.

Sommaruga Simonetta, Bundesrätin: Wir behandeln hier mit Artikel 19 Absatz 4 die lebhaft umstrittene Aufbewahrungsfrist für Randdaten. Umstritten ist aufgrund des Rückkommensentscheides des Ständerates bei Artikel 26 Absatz 5 nicht nur die Aufbewahrungsdauer der Randdaten des Postverkehrs, sondern eben auch jene des Fernmeldeverkehrs. Bei der ersten Beratung dieses Geschäfts wollte Ihr Rat ja sowohl für die Randdaten des Postverkehrs als auch für die Randdaten des Fernmeldeverkehrs eine Aufbewahrungsfrist von zwölf Monaten. Das entspricht auch dem Antrag des Bundesrates in seiner Botschaft. Hingegen haben der Stände-



rat und jetzt die Mehrheit Ihrer Kommission für beide Arten von Randdaten eine Aufbewahrungsfrist von sechs Monaten beschlossen. Das wiederum entspricht dem geltenden Recht.

Es stellen sich jetzt also zwei Fragen: Sollen die Aufbewahrungsdauer der Randdaten des Postverkehrs und die des Fernmeldeverkehrs unterschiedlich lang sein? Das ist die erste Frage. Die zweite Frage lautet: Soll sie sechs oder zwölf Monate betragen?

Die erste Frage lässt sich einfach beantworten. Das ist die Ansicht des Bundesrates, aber ich habe auch hier eigentlich Einigkeit festgestellt: Es macht keinen Sinn, dass die Dauer unterschiedlich lang ist. Dafür gibt es weder sachliche noch politische Gründe. Das spricht also für eine gleich lange Dauer beim Postverkehr und beim Fernmeldeverkehr.

Bei der Frage, ob die richtige Dauer sechs Monate oder zwölf Monate beträgt, ist der Fall aus Sicht der Strafverfolgung natürlich klar. Für die Strafverfolgung ist eine längere Dauer immer besser – lieber zwölf Monate als sechs Monate, lieber vierundzwanzig Monate als zwölf Monate. Wenn die Strafverfolgungsbehörde auf diese Daten zurückgreifen kann, allenfalls auch zu einem späteren Zeitpunkt, dann ist das für sie immer besser.

Was ist seit der Verabschiedung der Botschaft durch den Bundesrat alles passiert? Es ist wichtig, dass wir das noch einmal in Erinnerung rufen. Der Europäische Gerichtshof hat mit seinem Urteil vom April 2014 die europäische Richtlinie über die Vorratsdatenspeicherung für ungültig erklärt. Darauf haben verschiedene europäische Staaten reagiert und die Vorratsdatenspeicherung zum Teil ganz ausgesetzt, zum Teil auch mit kürzeren Fristen versehen. Einige Staaten, etwa Luxemburg, haben jetzt eine Aufbewahrungsdauer von sechs Monaten, andere eine solche von zwölf Monaten. Deutschland, das wurde bereits gesagt, sieht jetzt eine Aufbewahrungsdauer von zehn Wochen vor. Grossbritannien hingegen kennt eine Dauer von zwölf Monaten, und zwar für Briefe, Telefongespräche und E-Mails; dies soll nun auch auf die sozialen Netzwerke und die Internettelefonie ausgeweitet werden.

Eine neue europäische Richtlinie über die Vorratsdatenspeicherung ist zurzeit nicht in Sicht, und zwar aus dem einfachen Grund – ich habe immer wieder nachgefragt –, dass man sich im Moment unter den europäischen Staaten wohl kaum auf eine bestimmte Frist einigen kann. Die Vorstellungen gehen hier zu weit auseinander. Das heisst, es ist im Moment schwierig vorzusagen, wie dereinst eine europäische Richtlinie ausfallen wird. Zurzeit schwingt ja das Pendel, das immer hin und her geht, aufgrund der Terroranschläge eher wieder in Richtung mehr Überwachung.

Der Bundesrat ist in Übereinstimmung mit dem Ständerat zum Schluss gelangt, dass man an der heute geltenden Dauer der Vorratsdatenspeicherung vorerst festhalten soll, das heisst an sechs Monaten für Post- und Fernmeldedienste. Natürlich ist das Urteil des Europäischen Gerichtshofes für uns nicht bindend, deshalb verzichten wir auch nicht auf die Vorratsdatenspeicherung. Aber die Vorteile einer Verlängerung der Dauer wiegen die dadurch ausgelöste politische Unruhe – ich sage das ganz offen – aus Sicht des Bundesrates nicht auf.

Wir haben diese Fragen mit den Kantonen und mit den Strafverfolgungsbehörden noch einmal diskutiert. Wir sind uns hier einig: Wichtig ist den Strafverfolgungsbehörden, dass dieses Gesetz jetzt möglichst rasch verabschiedet und in Kraft gesetzt werden kann. Sie wissen, dass es einen direkten Zusammenhang zwischen dem BÜPF und dem Nachrichtendienstgesetz gibt. Deshalb ist man sich hier einig: Man möchte, dass es vorwärtsgeht, dass man dieses Gesetz so rasch wie möglich in Kraft setzen kann. Es geht hier schliesslich darum, dass wir die Rechtsgrundlage für die Überwachung der verschlüsselten Kommunikation schaffen.

Vorhin wurde gesagt, dass die Aufbewahrungsdauer der Randdaten die Kernfrage dieser Vorlage sei; dem muss ich widersprechen. Ich denke, das Kernelement dieser Vorlage ist, dass wir die Möglichkeit schaffen, für die verschlüsselte Kommunikation ebenfalls Überwachungen anzuordnen, selbstverständlich unter den sehr strengen Bedingungen, wie Sie sie bereits beschlossen haben.

Ich möchte abschliessend noch ein Wort zu denjenigen sagen, die sich jetzt für die längere Aufbewahrungsfrist aussprechen und diese verteidigen, also zur Minderheit. Ich habe Verständnis für jene, die sich für eine längere Frist exponiert haben und deshalb jetzt auch an zwölf Monaten

AB 2016 N 135 / BO 2016 N 135

festhalten wollen. Sie sagen, es sei eine Frage der Glaubwürdigkeit, weil Sie sich für diese längere Frist eingesetzt und exponiert haben. Sie unterstützen dieses Gesetz und möchten an dieser längeren Frist festhalten. Dafür habe ich Verständnis. Ich habe etwas mehr Mühe, jene zu verstehen, die sich jetzt ebenfalls mit der Minderheit für eine längere Aufbewahrungsdauer aussprechen und sich dafür einsetzen, obwohl sie ja das Gesetz in der Gesamtabstimmung abgelehnt haben! Als es also eine längere Frist für den Fernmeldeverkehr gab, haben sie das Gesetz abgelehnt, und jetzt setzen sie sich für die längere Frist ein und werden – davon muss ich ja ausgehen – das Gesetz in der Gesamtabstimmung wieder ablehnen. Da muss ich Ihnen sagen: Das finde ich in Bezug auf die Glaubwürdigkeit doch eher etwas fraglich. Dass man in der Politik neue Ent-



wicklungen einbezieht und aufgrund neuer Entwicklungen dann allenfalls auch für eine Änderung eintritt, das scheint mir aber legitim.

Deshalb beantrage ich Ihnen namens des Bundesrates, dem Ständerat und der Kommissionsmehrheit zu folgen.

Flach Beat (GL, AG), für die Kommission: Wir sind in der Differenzbereinigung zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Es sind nur noch wenige Differenzen offen. Sie haben es gehört: Es geht vor allen Dingen noch um die Frage der Dauer der sogenannten Randdatenspeicherung.

Der Ständerat hatte in der letzten Session ein Rückkommen auf diese Frage beschlossen, und Ihre Kommission für Rechtsfragen hat diesem Rückkommen stattgegeben. In der Kommissionsberatung wurde angeführt, was Sie bereits gehört haben. Die Kommission ist aber in der Mehrheit zum Schluss gelangt, dass der Kerngehalt dieses Gesetzes vor allen Dingen die Möglichkeit ist, die nun geschaffen wird, um die sogenannte verschlüsselte Kommunikation abzuhören. Auf diesem Auge sind die Strafverfolgungsbehörden heute blind. Der wesentlichste Bestandteil dieser Gesetzesänderung ist deshalb der Anschluss unserer gesetzlichen Regelungen an die technische Entwicklung.

Einig ist sich die Kommission darin gewesen, dass es nicht zwei verschiedene Fristen geben soll, betreffend die Aufbewahrung der Randdaten für den Postverkehr einerseits und für die Telekommunikation und die elektronische Kommunikation andererseits. Die Kommission hat bei der Aufbewahrung im Bereich des Postverkehrs mit 11 zu 9 Stimmen bei 1 Enthaltung und im Bereich des Fernmeldeverkehrs mit 11 zu 8 Stimmen bei 2 Enthaltungen für sechs Monate votiert.

Schwaab Jean Christophe (S, VD), pour la commission: Tout d'abord, permettez-moi de vous dire en introduction que pour chacun des articles 19, 21, 22 et 26, mais également pour toutes les dispositions connexes, la majorité et la minorité de la commission proposent des délais identiques, soit de six mois pour la majorité et de douze mois pour la minorité – cela a été rappelé par Madame Arslan. C'est pour cela que je vous recommande de faire preuve d'une certaine cohérence dans vos votes, et de demander soit un délai de six mois pour les fournisseurs de services de télécommunication, pour les données secondaires postales et pour la conservation des données après la fin de la relation contractuelle; soit douze mois pour chacun de ces chapitres.

J'en viens à la question qui nous préoccupe maintenant, à savoir choisir un délai de six ou un délai de douze mois. Il est vrai que, à l'origine, le projet du Conseil fédéral visait à conserver les données secondaires pendant et après la relation contractuelle. C'était d'ailleurs le souhait de ce Parlement, qui avait adopté plusieurs motions visant à porter de six à douze mois la conservation des données secondaires. C'était même une décision du Parlement qu'on aurait pu considérer définitive, puisque les deux conseils s'étaient mis d'accord sur le délai de douze mois – cela a été rappelé par Monsieur Vogler. Là où l'appréciation de la commission diverge de l'avis de Monsieur Vogler et rejoint celui de Madame la conseillère fédérale Sommaruga, c'est sur le fait qu'il y a de bonnes raisons, des raisons tout à fait crédibles, de rouvrir cette divergence, de reconsidérer notre décision et de privilégier, tant au Conseil des Etats qu'en ce qui concerne la commission du Conseil national, un délai de six mois.

La situation a évolué – cela a été dit – notamment avec l'arrêt de la Cour de justice de l'Union européenne. Cela a été rappelé par plusieurs oratrices avant moi: l'arrêt ne lie pas notre pays, puisque nous ne sommes bien entendu pas membres de l'Union européenne. L'arrêt ne prévoit pas non plus une interdiction de conserver les données secondaires, pas plus qu'il ne prescrit une durée maximum de conservation.

Cependant, l'arrêt précise deux éléments importants: d'une part, que la conservation des données secondaires de télécommunication est une atteinte grave aux droits fondamentaux; d'autre part, qu'il est donc particulièrement important de veiller au respect du principe de la proportionnalité. C'est d'ailleurs pour cela que l'on constate une tendance à la baisse de la durée de conservation dans la plupart des pays de l'Union européenne. A titre d'exemple, la République fédérale d'Allemagne en est maintenant à dix semaines.

Une autre raison a convaincu la commission de ramener la durée maximale de conservation des données à six mois. Si les cantons souhaitaient initialement les conserver douze mois, ils sont désormais d'accord de se contenter de six mois, estimant que la version actuelle du droit en vigueur est suffisamment efficace. Comme cela a été dit, on parvient, en six mois, à élucider 99 pour cent des cas. En outre, passer de douze à six mois diminuerait très certainement la contestation vis-à-vis de la loi, ce qui permettrait une entrée en vigueur plus rapide de cet important projet de loi. Cela permettrait notamment de surveiller les télécommunications cryptées.

Loin de moi l'idée de vouloir refaire le débat d'Apple contre le FBI, mais il est clair qu'un des points centraux de la loi réside dans la possibilité de créer une base légale pour que les autorités de poursuite pénale ne soient



pas démunies face à des télécommunications cryptées.

Enfin, il y a tout de même un argument de poids du point de vue des entreprises concernées, à savoir qu'il leur coûtera moins cher de stocker les données pendant six mois au lieu de douze. Et c'est là un argument d'importance.

C'est donc pour cette raison qu'aux articles 19 et 26, la commission vous recommande, par 11 voix contre 9 et 1 abstention, de vous rallier à la version du Conseil des Etats.

Je souhaite encore faire un commentaire concernant les articles 21 et 22, qui traitent de la conservation des données après la fin de la relation contractuelle. Je ne vais pas me répéter sur le fond. Pour les raisons précédemment évoquées, la commission vous recommande de passer à six mois. Mais il y a tout de même une question rédactionnelle à laquelle il faut rendre le second conseil attentif. Cette question rédactionnelle – je l'en avertis – est réglée de manière similaire dans la version de la majorité et dans celle de la minorité Geissbühler.

Peu importe que nous nous prononcions aujourd'hui pour six ou douze mois, ce point devra être réglé, le second conseil devra y prêter attention. Il s'agit de la place du mot "que" tout à la fin tant de la proposition de la majorité que de celle de la minorité Geissbühler. Il est clair que le "que" ne porte que sur les six mois dans la variante de la majorité et sur les douze mois dans celle de la minorité, et non pas, comme c'est le cas dans la version du Conseil des Etats, qu'à des fins d'identification. J'espère que le second conseil, quand il sera nanti de notre décision, fera attention à ce point.

S'agissant des articles 21 et 22, la commission vous demande de vous rallier à la solution du Conseil des Etats, par 12 voix contre 7 et 2 abstentions. Je vous remercie d'en faire de même.

Art. 19 Abs. 4 – Art. 19 al. 4

Präsidentin (Markwalder Christa, Präsidentin): Die Abstimmung gilt auch für Artikel 45 Absatz 3 und Artikel 273 Absatz 3 StPO sowie für Artikel 70d Absatz 3 MStP.

AB 2016 N 136 / BO 2016 N 136

Abstimmung – Vote

(namentlich – nominatif; 13.025/13007)

Für den Antrag der Mehrheit ... 112 Stimmen

Für den Antrag der Minderheit ... 75 Stimmen

(0 Enthaltungen)

Art. 21 Abs. 2; 22 Abs. 2 – Art. 21 al. 2; 22 al. 2

Abstimmung – Vote

(namentlich – nominatif; 13.025/13008)

Für den Antrag der Mehrheit ... 98 Stimmen

Für den Antrag der Minderheit ... 89 Stimmen

(0 Enthaltungen)

Art. 26 Abs. 5 – Art. 26 al. 5

Präsidentin (Markwalder Christa, Präsidentin): Die Abstimmung gilt auch für Artikel 45 Absatz 3 und Artikel 273 Absatz 3 StPO sowie Artikel 70d Absatz 3 MStP.

Abstimmung – Vote

(namentlich – nominatif; 13.025/13009)

Für den Antrag der Mehrheit ... 97 Stimmen

Für den Antrag der Minderheit ... 90 Stimmen

(2 Enthaltungen)

Art. 26 Abs. 5bis

Antrag der Mehrheit

Festhalten

Antrag der Minderheit





(Vogler, Bauer, Flach, Guhl, Merlini, Schmidt Roberto)
Zustimmung zum Beschluss des Ständerates

Art. 26 al. 5bis

Proposition de la majorité

Maintenir

Proposition de la minorité

(Vogler, Bauer, Flach, Guhl, Merlini, Schmidt Roberto)

Adhérer à la décision du Conseil des Etats

Vogler Karl (C, OW): Bei Artikel 26 Absatz 5bis geht es um die Frage, wo die Anbieterinnen von Fernmeldediensten die Randdaten des Fernmeldeverkehrs aufbewahren müssen, sprich explizit in der Schweiz oder eben nicht. Warum ist es nicht angezeigt und nicht notwendig, dass diese Daten unbedingt in der Schweiz aufbewahrt werden müssen?

Vorab und um das klarzustellen: Ein Unternehmen, das in der Schweiz seine Dienste anbietet, muss das schweizerische Recht, namentlich auch das schweizerische Datenschutzrecht, beachten, und zwar völlig ungeachtet dessen, wo die Daten auf dieser Welt gelagert werden. Lagert ein Fernmeldedienstunternehmen seine Daten im Ausland, so muss das Unternehmen sicherstellen und garantieren, dass das schweizerische Datenschutzrecht eingehalten wird. Ist das nicht möglich, so dürfen keine Daten ausserhalb der Schweiz gelagert werden. Die Verantwortlichkeit für die Anbieterin von Fernmeldediensten bleibt genau gleich, ob die Daten im In- oder im Ausland gelagert werden.

Noch etwas: Wenn wir tatsächlich der Meinung sind, dass Daten nur in der Schweiz sicher gelagert werden können, so müsste man Entsprechendes ebenfalls zum Beispiel von den Privatversicherern, den Krankenkassen oder den Banken verlangen. Wird Entsprechendes nur von den Anbieterinnen von Fernmeldedienstleistungen verlangt, so ist das einigermaßen inkonsequent und letztlich auch diskriminierend.

Seien wir nicht naiv: Zu meinen, diese Daten würden einfach nur auf einem Datenträger in einem Tresor gelagert, ist nämlich einigermaßen naiv. Mit Artikel 26 Absatz 5bis schaffen wir einzig Scheinsicherheit. Diese Daten sind irgendwo im Web im Fluss, und zwar nicht nur in der Schweiz.

Schliesslich geht es darum, nicht zulasten unserer Telekommunikationsbranche eine obligatorisch-protektionistische Swissness-Vorschrift zu schaffen. Die Branche lehnt eine entsprechende Verpflichtung aus Gründen der Wettbewerbsfähigkeit denn auch ausdrücklich ab.

Ein Letztes: Wenn schon, so wäre dieses Gesetz der falsche Ort für eine entsprechende Legiferierung. Sie müsste im Datenschutzgesetz oder im Fernmeldegesetz gemacht werden.

Dementsprechend bitte ich Sie, dem Antrag der Minderheit auf Streichung zuzustimmen.

Grüter Franz (V, LU): Herr Kollege Vogler, wie können Sie es den Schweizerinnen und Schweizern erklären – diese Forderung gemäss Minderheit kommt ja von einigen Grosskonzernen, die diese Daten nicht in der Schweiz beherbergen möchten –, dass ihre persönlichen Kommunikations- und Bewegungsdaten in Ländern gespeichert werden, von denen man weiss, dass sich der Staat einen Deut um den Schutz kümmert und Überwachung bis zum Exzess ausgeübt wird?

Vogler Karl (C, OW): Es geht hier um zwei Sachen. Ich habe schon gesagt, dass diese Unternehmen garantieren müssen, dass die schweizerischen Datenschutzbestimmungen eingehalten werden. Die Unternehmen, die Daten im Ausland lagern, müssen das garantieren, andernfalls dürfen sie das nicht machen. Das wird auch entsprechend kontrolliert.

Nochmals: Die Lagerung der Daten in der Schweiz müssten Sie dann beispielsweise auch von den Banken verlangen. Diese lagern ihre Daten ja heute ebenfalls im Ausland. Warum wollen Sie die Lagerung im Inland nur dieser Branche aufbürden? Dafür gibt es eigentlich keinen Grund.

Weibel Thomas (GL, ZH): Wir Grünliberalen unterstützen bei Artikel 26 Absatz 5bis die Minderheit.

Ergänzend zu den Ausführungen von Kollega Vogler nochmals einige Präzisierungen: Wenn eine amerikanische Firma Daten von amerikanischen Kunden in der Schweiz aufgrund einer privatrechtlichen Vereinbarung auf einem Server speichert, dann gilt das amerikanische Recht. Entsprechend ist es umgekehrt: Wenn Schweizer Daten im Ausland speichern, dann gilt das schweizerische Recht. Zudem ist zu berücksichtigen, dass der Zugriff auf die Daten, dass die Zugriffsberechtigungen von der Schweiz aus über Fernwartung definiert werden. Aus wirtschaftlichen Überlegungen wird die Speicherung in der Schweiz sowieso häufig sehr interessant



sein. Daten sind im Fluss, hat Kollega Vogler gesagt. Abfragen und Speichervorgänge gehen in der Regel über Server im Ausland, sogar über Kontinente hinweg.

Die Mehrheit geht von einer falschen Vorstellung aus. Sie hat die realitätsfremde Erwartung, dass Bits und Bytes die Schweiz nicht verlassen können. Um das sicherzustellen, müsste eine spezielle Software entwickelt werden, welche den Datentransfer, diese Übermittlung über das Ausland, unterbindet. Wenn wir aber akzeptieren, dass die Datenströme international sind, ist es obsolet vorzuschreiben, wo der Datenspeicher stehen muss; es ist nämlich auch nicht relevant für die Sicherheit der Daten. Hier wird aus falschen Überlegungen Swisness und Heimatschutz betrieben.

Und – Herr Vogler hat schon darauf hingewiesen – es ist nicht konsequent. Für mich sind meine Sozialversicherungsdaten viel sensibler. Dort ist mein Interesse, dass sie nicht in falsche Hände gelangen, weitaus grösser, als es bei meinen Bewegungsdaten und den Daten darüber, wo in der Schweiz ich wann und mit wem telefoniert habe, ist. Wir kennen aber für die Sozialversicherungsdaten keine entsprechende Vorschrift. Wenn wir eine solche Regelung einführen wollten, dann wäre aus unserer Sicht das Büpf der falsche Ort. Wenn schon, dann müsste es im Fernmeldegesetz geregelt werden oder noch besser im Datenschutzgesetz, dort eben umfassend für alle sensiblen Daten.

Deshalb unterstützen wir Grünliberalen den Antrag der Minderheit Vogler.

AB 2016 N 137 / BO 2016 N 137

Schwander Pirmin (V, SZ): Herr Kollege Weibel, was nützen unsere Datenschutzgesetzgebungen, wenn die Daten im Ausland aufbewahrt werden?

Weibel Thomas (GL, ZH): Danke für diese Frage, Herr Kollege. Ich gehe davon aus, das entnehme ich Ihrer Frage, dass Sie allen anderen Ländern unterstellen, dass sie keine Rechtsstaaten sind. Ich habe da mehr Vertrauen und erwarte, dass Länder, welche die technischen Möglichkeiten haben, solche Services und Dienstleistungen anzubieten, auch bezüglich des Rechtsverständnisses ein ähnliches Niveau wie wir haben und sich entsprechend an das geltende Rechtssystem halten.

Schmidt Roberto (C, VS): Auch die CVP-Fraktion unterstützt diesen Minderheitsantrag Vogler. Für die Einhaltung des schweizerischen Datenschutzrechtes, Herr Schwander, ist es eben nicht nötig, dass die Randdaten auch bei uns aufbewahrt werden. Es wurde jetzt x-mal gesagt, auch in den Kommissionen und hier im Saal: Das schweizerische Datenschutzrecht gilt ungeachtet dessen, wo sich die Daten befinden, wo sie gelagert und bearbeitet werden. Der schweizerische Sicherheitsstandard – und der ist uns sehr heilig – muss durch alle Firmen gewährleistet werden, die bei uns tätig sind, die unsere Daten verwenden. Sie müssen diesen Standard einhalten, auch wenn sie im Ausland tätig sind, diese Daten dort bearbeiten oder speichern.

Vergessen Sie nicht, dass auch Telekommunikationsdienste zunehmend von international tätigen Unternehmen bereitgestellt werden, die mit diesen Randdaten arbeiten müssen, und zwar auch im Ausland, nicht nur in der Schweiz. Es ist unvermeidlich, dass Randdaten auch ausserhalb der Schweiz bereitgestellt werden und dort vielleicht auch gespeichert werden müssen. Wenn wir das verbieten wollen, wenn wir wollen, dass das nicht mehr geht, ist das ein allzu grosser Eingriff in die Wirtschaftsfreiheit.

Ich bitte Sie, die Minderheit zu unterstützen.

Guhl Bernhard (BD, AG): Ich gehe davon aus, dass viele von Ihnen Whatsapp, Facebook, Twitter oder andere Social Media nutzen. Machen Sie sich dort Gedanken, wo Ihre Daten gespeichert werden? Das tun wohl die wenigsten. Wenn mir langweilig wäre, könnte ich im Anschluss an diese Abstimmung hingehen und schauen, wer hier dem Antrag der Mehrheit zugestimmt hat, also der Speicherung von Randdaten in der Schweiz, aber Whatsapp usw. nutzt und sich dort überhaupt keine Gedanken macht. Das ist schlicht und einfach unglaublich unwürdig.

Hier soll nun den Fernmeldediensteanbietern eine Vorgabe gemacht werden, welche bei anderen Speicherdaten nicht gemacht wird. Das erstaunt. Die aufgeworfenen Sicherheitsfragen sind unberechtigt, das haben wir vorhin in der Diskussion bereits gehört. Die Datenschutzbestimmungen müssen eingehalten werden. Herr Grüter, ich kann Ihnen versichern, dass kein einziger Fernmeldediensteanbieter den Server in einem Land aufstellt, in dem die Datenschutzbestimmungen nicht eingehalten werden könnten.

Wenn Sie hier die Speicherung der Daten in der Schweiz verlangen würden, müssten Sie dies auch bei Krankenkassen, Banken, Spitälern usw. tun; das hat vorhin bereits der Anführer der Minderheit ausgeführt. Swisness ist bei dieser Vorlage nicht angebracht. Besonders bei denjenigen Parlamentariern, die sonst für eine liberale Wirtschaftsordnung, für unternehmerische Freiheit usw. plädieren, verstehe ich es nicht, wenn sie hier



eine Bestimmung bejahen, welche den Anbietern in Bereichen Vorschriften macht, in denen unternehmerische Freiheit gefragt ist.

Arslan Sibel (G, BS): Die Fraktion der Grünen bittet Sie, der Mehrheit zu folgen und diesen Minderheitsantrag nicht zu unterstützen.

Wir sind dafür, dass die Randdaten des Fernmeldeverkehrs in der Schweiz aufbewahrt werden sollen. Es geht um höchstpersönliche Daten, mit denen sorgfältig umgegangen werden müsste. Es ist selbstverständlich klar, dass die Telekommunikationsbranche nicht erfreut darüber ist, dass die Daten nicht ausserhalb der Schweiz gespeichert werden sollen. Ich möchte nicht Swissness betreiben, aber für die Grünen ist die Sicherheit wichtig, auch die Sicherheit unserer Datenaufbewahrung.

Die Sicherheit, die wir hier bei uns gewährleisten können, ist relativ hoch. Wir haben strengere Datenschutzbestimmungen. Wenn sich die Daten nicht in unserem Land befinden, kann es sein, dass sie in Ländern aufbewahrt werden, in denen andere gesetzliche Regelungen gelten, in denen es Ausnahmeregelungen gibt. Das wollen wir nicht. Es ist wichtig, dass die Daten bei uns bleiben und wir dann auch über diese Rechtsordnung, über diese Rechtssicherheit verfügen können.

Deshalb bitte ich Sie im Namen der grünen Fraktion, der Mehrheit zu folgen und die Daten bei uns in der Schweiz aufzubewahren.

Ruiz Rebecca Ana (S, VD): Le groupe socialiste vous invite à vous rallier à la décision de la majorité de la commission pour garantir le stockage des données secondaires de télécommunication en Suisse. Il nous paraît en effet essentiel que la conservation de telles données soit conforme à notre réglementation en matière de protection des données et de la sphère privée.

Ces données, il faut le répéter, sont sensibles. Elles permettent d'identifier quand ont eu lieu des télécommunications, quelle a été leur durée et où se trouvaient les personnes lors des différents échanges. De telles informations doivent pouvoir demeurer ici.

La proposition de la minorité Vogler pose problème parce qu'elle rend possible le stockage de ces données dans d'autres pays par des entreprises qui, bien que soumises au droit suisse, pourraient faire appel à des services d'informatique en nuage ou "cloud computing". Or, tous les pays hébergeant ces infrastructures n'ont pas les mêmes standards de protection des données que ceux prévus par notre législation.

Aussi, en adoptant la proposition de la minorité Vogler, on prendrait le risque qu'une entreprise stockant des données soit rachetée par une entreprise soumise à un droit étranger potentiellement peu sensible à la question de la protection des données. Cela pourrait être le cas avec les Etats-Unis, puisqu'on sait que le matériel informatique et les logiciels qui servent au stockage de données et aux réseaux informatiques proviennent en grande partie de constructeurs américains. Le problème qui pourrait alors se poser dans ce cas réside dans le fait que ces entreprises américaines, dans le cadre de procédures pénales, peuvent être obligées de fournir la totalité des données en leur possession, par exemple à leurs services secrets, sans en informer les titulaires. Pour nous prémunir contre ce type de risque, qu'on ne peut exclure, je vous invite à refuser la proposition défendue par la minorité Vogler.

Merlini Giovanni (RL, TI): Bei Artikel 26 Absatz 5bis will meine Fraktion keine unnötige Swissness-Vorschrift im Gesetz haben. Eine solche widerspräche eindeutig der zunehmenden Internationalisierung der gesamten Telekommunikationsbranche und würde die Wirtschaftsfreiheit ungebührlich einschränken.

Ein Unternehmen, das in der Schweiz aktiv ist, muss die datenschutzrechtlichen Bestimmungen auch dann beachten, wenn die Randdaten im Ausland gelagert werden; das haben wir heute Morgen schon x-mal gehört. Will ein Unternehmen seine Daten in einem anderen Land speichern und vermag es die Einhaltung des schweizerischen Datenschutzrechts nicht sicherzustellen, so darf es einfach in jenem Land keine Daten lagern. Es trägt auch eine strafrechtliche Verantwortung für die Datensicherheit. Eine gesetzliche Verpflichtung, diese Daten in der Schweiz aufzubewahren, wäre deshalb wenig sinnvoll. Man müsste nämlich auch sicherstellen, dass diese Datenabspeicherung über irgendwelche Computerprogramme nicht über ausländische Server läuft – was sich nicht bewerkstelligen lässt. Insofern ist

AB 2016 N 138 / BO 2016 N 138

eine solche Bestimmung obsolet, wenn man berücksichtigt, wo diese Datenströme überall durchgehen. Ich bitte Sie demzufolge, hier dem Antrag der Minderheit Vogler zuzustimmen.

Sommaruga Simonetta, Bundesrätin: Es geht hier um die Frage, ob das BÜP den Fernmeldediensteanbieterinnen vorschreiben soll, dass sie ihre Randdaten ausschliesslich in der Schweiz aufbewahren müssen. Dieser





Vorschlag stammt von Ihrem Rat. Der Ständerat, der Bundesrat und eine Minderheit Ihrer Kommission sind dagegen.

Ich möchte ein paar Argumente nennen, die gegen eine zwingende Aufbewahrung in der Schweiz sprechen: Diese zwingende Vorschrift ist für die Einhaltung des schweizerischen Datenschutzrechts gar nicht nötig. Es wurde bereits mehrfach erwähnt, dass alle Unternehmen, die in der Schweiz aktiv sind, das schweizerische Recht einhalten müssen, auch das Datenschutzrecht, und zwar ungeachtet dessen, wo die Daten effektiv gespeichert sind. Gemäss Datenschutzgesetz dürfen Personendaten – auch Randdaten – eben nur dann im Ausland aufbewahrt werden, wenn die Gesetzgebung des betroffenen Landes oder andere Garantien einen angemessenen Schutz gewährleisten. Dies gilt auch für die Aufbewahrung der Daten in einer Cloud auf einem Server im Ausland. Es gibt durchaus Staaten, die ein mit der Schweiz vergleichbares Schutzniveau haben. Ein Verbot der Datenaufbewahrung in solchen Ländern ist daher auch völlig unnötig.

Das Urteil des Europäischen Gerichtshofes vom 8. April 2014 zur Vorratsdatenspeicherung wurde erwähnt. Aber weder von diesem Urteil noch vom Urteil des Europäischen Gerichtshofes vom Oktober 2015 zu den sogenannten Safe-Harbor-Verträgen mit den USA lässt sich ableiten, dass die Daten in der Schweiz aufbewahrt werden müssen. Übrigens haben sich die EU und die USA vor wenigen Tagen bereits wieder auf einen neuen Rahmen für die Übermittlung personenbezogener Daten von europäischen Bürgern in die USA geeinigt.

Etwas möchte ich auch noch erwähnen: Wenn Sie hier solche besonderen Regeln für diese Daten aufstellen wollen, dann bin ich schon der Meinung, dass es noch ein paar andere sensible Daten gäbe, die dann erst recht auch in der Schweiz aufbewahrt werden müssten. Ich denke an Daten von Krankenversicherungen und überhaupt von Privatversicherungen, von Banken. Wenn Sie jetzt hier Daten zwingend in der Schweiz aufbewahrt haben wollen, dann gäbe es, denke ich, schon noch andere Daten, bei denen Sie umso mehr dieselbe Forderung stellen müssten. Von einer solchen Forderung habe ich aber hier nichts gehört.

Etwas darf man auch nicht vergessen: Die Telekommunikationsdienste werden ja oft von international tätigen Unternehmen bereitgestellt. Die von ihnen benötigten IT-Kommunikationssysteme werden in einigen wenigen Ländern zentralisiert, häufig eben ausserhalb der Schweiz. Deshalb ist es unvermeidbar, dass Randdaten die Landesgrenzen schon mal überqueren und dann auch ausserhalb der Schweiz gespeichert werden. Das gilt umso mehr bei den Anbieterinnen von abgeleiteten Kommunikationsdiensten, also z. B. von Facebook und Twitter.

Ich möchte noch ein wirtschaftliches Argument anfügen. Vergessen Sie nicht, dass die Schweiz sich in den letzten Jahren international einen hervorragenden Ruf im Bereich der Speicherung von Informatikdaten erarbeitet hat, und das vor allem dank den Kompetenzen und der Professionalität in diesem Bereich. Sensible Daten werden also häufig aus dem Ausland in die Schweiz übermittelt, um hier gespeichert zu werden. Für die Entwicklung dieser Branche wäre es inkonsequent, unter Umständen sogar kontraproduktiv, wenn Sie jetzt eine protektionistische Regelung hier im Büpf vornähmen. Stellen Sie sich vor: Wenn andere Länder das Gleiche tun, was jetzt die Kommissionsmehrheit will, wenn also alle Länder sagen, dass die Daten nur bei ihnen gespeichert werden dürfen, dann ist das für unsere Branche schädlich. Protektionismus ist eigentlich normalerweise keine Massnahme, die von einer wirtschaftsliberalen Haltung unterstützt wird. Deshalb sind wir auch im Sinne der Wirtschaftsfreiheit der Meinung, dass eine solche Regelung keinen Sinn macht.

Vielleicht noch ein gesetzestechnisches Argument – das ist zwar nicht das wichtigste Argument, aber ich erwähne es trotzdem -: Das Büpf wäre auf jeden Fall der falsche Ort, um eine solche Regelung einzuführen. Das müssten Sie, wenn schon, im Fernmeldegesetz machen, das wäre der richtige Ort. Wenn Sie die laufende Revision des Fernmeldegesetzes anschauen, dann stellen Sie fest, dass man dort in die genau entgegengesetzte Richtung legiferiert, indem man eben eine Liberalisierung und nicht solche protektionistischen Massnahmen anstrebt.

Zum Schluss noch etwas, was ich die Kommissionsmehrheit zu überdenken bitte: Wenn Sie beschliessen, dass die Daten in der Schweiz gespeichert werden müssen, dann müssen Sie einfach auch ganz ehrlich sagen, dass Sie das gar nicht kontrollieren können. Das müssen Sie einfach sagen – das ist so. Jemand müsste mir sagen, wie Sie kontrollieren wollen, dass diese Daten tatsächlich in der Schweiz gespeichert werden. Die zuständige Behörde hat ja gar keinen Einblick in die Netzarchitektur der Fernmeldediensteanbieterinnen. Sie müsste diese dann zwingen, ihre Netzarchitektur so zu gestalten, dass die Randdaten auch nach einem Transit ins Ausland am Schluss wieder in die Schweiz gelangen. Niemand kann aber kontrollieren, ob einer solchen Verpflichtung auch nachgekommen würde, nämlich indem alle Randdaten im Ausland gelöscht würden und sie am Schluss wieder in die Schweiz geholt würden. Man müsste hier eine Selbstdeklaration der Anbieterinnen vorgeben und sich darauf verlassen können. Aber echt kontrollieren, das müssen Sie ehrlich zugeben, können Sie diese Vorgänge nicht.

Aus all diesen Gründen bitte ich Sie, die Minderheit der Kommission zu unterstützen und damit auch die



Haltung des Ständerates und des Bundesrates.

Flach Beat (GL, AG), für die Kommission: Wir befinden uns jetzt bei der letzten Differenz zum Ständerat. Sie haben vorhin dem Ständerat zugestimmt, was die Dauer der Aufbewahrung dieser Randdaten anbelangt. Die Kommission hat zu den Fragen zu all diesen Aufbewahrungs- und Überwachungsgeschichten viele Anhörungen durchgeführt. Wir haben festgestellt, dass es sich halt um eine sehr technische Vorlage handelt, und wir haben teilweise auch ein bisschen vorgegriffen. Die Frau Bundesrätin hat es gesagt: Wir werden die Diskussion zu dieser Thematik noch weiterführen: beim Fernmeldegesetz, aber auch beim Datenschutzgesetz. Die Kommission hat während ihrer Beratung insbesondere auch einige Petitionen behandelt. Auf die möchte ich noch kurz eingehen. Es handelt sich um die Petitionen 13.2043 und 13.2049, bei denen es darum geht, wie die Government Software anzuwenden ist. Es wurde auch ein Nichteintretensantrag gestellt, und die Kommission hat sich mit diesen Petitionen auseinandergesetzt.

Nun zur Frage des Aufbewahrungsortes dieser Randdaten: Diese Randdaten sind halt sensible Daten. Sie umfassen Bewegungsdaten der Telekommunikationsnutzer, sie umfassen die Verbindungsdaten. Deshalb ist es der Mehrheit der Kommission wichtig, dass diese sensiblen Daten physisch in der Schweiz gespeichert werden. In der Kommission war ein allgemeines Unbehagen dazu zu spüren, dass diese Daten irgendwo auf der Welt physisch aufbewahrt werden könnten. Die Kommission hat letztlich mit 16 zu 6 Stimmen bei 0 Enthaltungen dem Antrag zugestimmt, dass diese Randdaten in der Schweiz aufbewahrt werden müssen. Ich bitte Sie, hier der Mehrheit zu folgen.

Schwaab Jean Christophe (S, VD), pour la commission: La majorité de la commission vous recommande de maintenir sa décision – cette dernière a été prise par 16 voix contre 6 –, et donc d'obliger les entreprises de télécommunication à stocker les données secondaires de télécommunication dans notre pays.

Cela a été dit, notamment par Madame Ruiz Rebecca, mais aussi démontré par l'expérience menée par Monsieur Glättli

AB 2016 N 139 / BO 2016 N 139

il y a quelques mois, les données secondaires sont des données extrêmement sensibles. Certes, cela a l'air anodin comme cela, de savoir où et quand et avec qui on a téléphoné, mais lorsque l'on recoupe ces données, on arrive à reconstituer de manière assez précise l'emploi du temps de la personne qui utilise des services de télécommunication. Partant, cela permet de déterminer ce qu'elle a fait exactement de sa journée, à la minute près, et de découvrir un nombre impressionnant de détails sur sa vie privée, pour ne pas dire sur sa vie intime. Aujourd'hui, ces données peuvent être stockées n'importe où. Cela peut être en Suisse; cela peut être dans des pays qui connaissent un niveau de protection des données tout à fait suffisant, comparable à celui qui est en vigueur dans notre pays, mais cela peut être aussi dans des pays où l'on sait qu'en général la protection des données est insuffisante – je pense aux Etats-Unis, à la Chine, voire à des pays où les services secrets peuvent allègrement se servir et consulter ces données, sans même s'appuyer sur des décisions judiciaires.

Il nous paraît donc légitime et nécessaire que ces données sensibles soient conservées dans notre pays. C'est une question de souveraineté en matière de données; il s'agit de garantir une meilleure protection des données; il s'agit de garantir une meilleure sécurité des données.

Et pour répondre peut-être à Monsieur Guhl, qui disait qu'en définitive, les personnes s'offusquent de savoir que leurs données secondaires sont stockées dans d'autres pays mais que, parallèlement, elles laissent un certain nombre de données personnelles circuler sur Facebook, sur whatsapp, sur Twitter, et j'en passe, je me permettrai une remarque personnelle: moi aussi, j'utilise Facebook, moi aussi j'utilise whatsapp, mais je n'ai pas le choix! Si je souhaite utiliser ces services, je n'ai absolument aucun moyen de contrôler où vont mes données. Je sais que Facebook en fait n'importe quoi, mais du moment que je souhaite utiliser ce service, qui jouit d'une position dominante en matière de réseaux sociaux, je n'ai d'autre choix que d'avalier cette couleuvre. Il nous paraît donc important, en matière de données aussi sensibles que les données secondaires de télécommunication, d'imposer une protection des données avec un label de qualité suisse.

Et puis enfin, il est aussi important de positionner notre pays en tant que coffre-fort numérique du monde. Et là, Monsieur Weibel, nous ne faisons pas de protection du patrimoine. Nous faisons tout simplement de la promotion économique.

C'est pour cette raison que je vous recommande de suivre la majorité de la commission.

Präsidentin (Markwalder Christa, Präsidentin): Die SVP-Fraktion unterstützt den Antrag der Mehrheit.

Abstimmung – Vote





(namentlich – nominatif; 13.025/13010)
Für den Antrag der Mehrheit ... 114 Stimmen
Für den Antrag der Minderheit ... 72 Stimmen
(3 Enthaltungen)

Art. 45 Abs. 3

Antrag der Mehrheit

Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

Festhalten

Art. 45 al. 3

Proposition de la majorité

Adhérer à la décision du Conseil des Etats

Proposition de la minorité

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

Maintenir

Angenommen gemäss Antrag der Mehrheit

Adopté selon la proposition de la majorité

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

Ziff. II Ziff. 1 Art. 269quater Abs. 4, 5

Antrag der Kommission

Zustimmung zum Beschluss des Ständerates

Ch. II ch. 1 art. 269quater al. 4, 5

Proposition de la commission

Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

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

Antrag der Mehrheit

Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

Festhalten

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

Proposition de la majorité

Adhérer à la décision du Conseil des Etats

Proposition de la minorité

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)

Maintenir

Angenommen gemäss Antrag der Mehrheit

Adopté selon la proposition de la majorité



Ziff. II Ziff. 1 Art. 286 Abs. 2 Bst. i; Ziff. 2 Art. 70quater Abs. 4, 5

Antrag der Kommission

Zustimmung zum Beschluss des Ständerates

Ch. II ch. 1 art. 286 al. 2 let. i; ch. 2 art. 70quater al. 4, 5

Proposition de la commission

Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

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

Antrag der Mehrheit

Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)
Festhalten

Ch. II ch. 2 art. 70d al. 3

Proposition de la majorité

Adhérer à la décision du Conseil des Etats

Proposition de la minorité

(Geissbühler, Egloff, Guhl, Nidegger, Schmidt Roberto, Tuena, Vogler, Vogt, Walliser)
Maintenir

Angenommen gemäss Antrag der Mehrheit

Adopté selon la proposition de la majorité

AB 2016 N 140 / BO 2016 N 140