

13.025

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Änderung

Loi sur la surveillance de la correspondance par poste et télécommunication. Modification

Erstrat – Premier Conseil

Botschaft des Bundesrates 27.02.13 (BBl 2013 2683)
Message du Conseil fédéral 27.02.13 (FF 2013 2379)

Ständerat/Conseil des Etats 10.03.14 (Erstrat – Premier Conseil)

Ständerat/Conseil des Etats 19.03.14 (Fortsetzung – Suite)

Engler Stefan (CE, GR), für die Kommission: Der Bundesrat unterbreitet dem Parlament und dem Ständerat als Erstrat mit der Botschaft zum Geschäft 13.025 die Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs – ich zwingen mich, die unaussprechliche Abkürzung dafür nicht zu verwenden.

Diese Totalrevision soll die Voraussetzungen dafür schaffen, dass der Post- und Fernmeldeverkehr, wenn ein Verdacht auf Begehung einer schweren Straftat besteht, zum Zweck der Strafverfolgung im Vergleich zu heute zwar nicht mehr, aber besser überwacht werden kann. Die Totalrevision ist nach dem Dafürhalten der Kommission notwendig, denn das Gesetz muss an die technologischen Entwicklungen der letzten Jahre angepasst werden, damit eine effiziente Strafverfolgung gewährleistet ist. Oder anders formuliert: Mit der Revision soll sichergestellt werden, dass die notwendigen Überwachungen des Fernmeldeverkehrs nicht durch die Verwendung neuer Technologien verhindert werden können. In den meisten Fällen, in denen eine solche Überwachung die Aufklärungsarbeit unterstützt, handelt es sich um schwere und schwerste Delikte in Bereichen der organisierten Kriminalität wie Kinderpornografie, Tötungs- oder schwere Vermögensdelikte. Es geht also bei diesem Gesetz um den Unterschied zum Nachrichtendienstgesetz nicht um eine flächendeckende präventive Überwachung der Bürgerinnen und Bürger. Das Gesetz bezweckt auch nicht eine flächendeckende Überwachung, wie sie offenbar der amerikanische Geheimdienst NSA über Jahre bei Freund und Feind praktizierte.

Die Kommission für Rechtsfragen hat sich ungewöhnlich lang, nämlich an nicht weniger als fünf Sitzungstagen, mit dieser Vorlage auseinandergesetzt. Wir haben den Dienst zur Überwachung des Post- und Fernmeldeverkehrs vor Ort besucht und uns die Prozesse im Detail erklären lassen, und wir haben unzählige Anhörungen durchgeführt und die verschiedenen Interessengruppen zu Wort kommen lassen: die Kantone, die Strafverfolgungsbehörden und die Polizei, einen Verfassungsrechtler, einen mit der digitalen Welt vertrauten und spezialisierten Rechtsanwalt, den Datenschutzbeauftragten des Bundes, Herrn Thür, dann aber auch verschiedene Vertreter der Provider, zusammengeschlossen im Schweizerischen Verband der Telekommunikation.

Seitens der Strafverfolgungsbehörden wurde dabei betont – ich zitiere Herrn Andreas Brunner, den Leitenden Oberstaatsanwalt des Kantons Zürich –, dass eine funktionierende Kommunikationsüberwachung für eine erfolgreiche Strafverfolgung von schweren und schwersten Delikten unabdingbar sei. Sinngemäss und verkürzt stellt sich die Telekommunikationsbranche demgegenüber auf den Standpunkt, nicht die Rolle des Hilfsheerführers bzw. Erfüllungsgehilfen der Strafverfolgungsbehörden übernehmen zu wollen.

Als Folge dieser Anhörungen hat die Kommission auch eine Reihe von Anpassungen am Gesetzentwurf vorgenommen.

Was macht eigentlich diese Vorlage schwierig und gleichzeitig umstritten? Es sind die gegenläufigen Interessen. Der Schutz von Grundrechten, der Persönlichkeit und der persönlichen Daten steht dem öffentlichen Interesse an einer wirksamen Strafverfolgung gegenüber. Dieses wiederum konkurriert mit dem Interesse der Provider, ihr Geschäftsmodell möglichst ungehindert kommerziell anbieten zu können. In diesem mehrfachen Interessenkonflikt sucht 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 Rechtsschutz garantiert. Das Machbare, das Mögliche und das Notwendige – in diesem Spannungsfeld spielt sich die Debatte um die Überwachung des Post- und Fernmeldeverkehrs ab.

Als speziell herausfordernd erwies sich die Frage verdeckter Ermittlungen im Internet. Die Frage, ob die Strafverfolgung im Internet, etwa die Überwachung des E-Mail-Verkehrs oder der Internettelefonie, zulässig ist, wird nur noch von den wenigsten gestellt. Die Antwort ist klar Ja. Die Diskussionen drehen sich also nicht mehr um das Ob, sondern vor allem noch um das Wie der Strafverfolgung. Je ausgefeilter die technischen Möglichkeiten sind, desto höher ist in einem grundrechtssensiblen Bereich, wie es der vorliegende ist, die Messlatte für einen wirksamen Schutz der Grundrechte anzulegen. Da war sich die Kommission von Anfang an einig. Gemeint sind hohe Anforderungen an die Bestimmtheit der gesetzlichen Grundlagen, die Beachtung des Gebots der Subsidiarität, die Konkretisierung der Verhältnismässigkeit und der Rechtsschutz, aber auch die Pflicht zur nachträglichen Mitteilung und zur Garantie der daran anknüpfenden Beschwerdemöglichkeiten der Betroffenen. Am Beispiel der Echtzeitüberwachung eines E-Mail-Verkehrs hiesse dies: Sie ist nur zulässig, wenn ein dringender Tatverdacht vorliegt, eine im Deliktskatalog aufgeführte Tat im Raum steht, sie durch einen Staatsanwalt angeordnet und innerhalb von 24 Stunden durch das Zwangsmassnahmengericht bestätigt wurde.

Diese Gesetzesrevision verläuft somit auf einem schmalen Grat zwischen dem, was technisch möglich ist, und dem, was rechtlich zulässig sein soll, um Strafverfolgungen bei einem Verdacht bezüglich einer schweren Tat zu unterstützen. Gerade der Einsatz sogenannter Spyware wie zum Beispiel Govware macht den Konflikt deutlich: Nicht alles, was technisch möglich ist, muss rechtlich zulässig sein, und nicht alles, was rechtlich zulässig erscheint, ist mit gleicher technischer Zuverlässigkeit umsetzbar. Inhaltlich obliegt es also dem Gesetzgeber, bei der Ausgestaltung dieser Ermächtigungsgrundlagen nicht nur den Sicherheitsanliegen der Allgemeinheit, sondern auch den Freiheiten und Rechten der Einzelnen Rechnung zu tragen.

Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs und die daran angehängte Revision der Strafprozessordnung befassen sich mit unterschiedlichen Regelungsgegenständen. Ersteres regelt vornehmlich organisatorische und technische Aspekte sowie die Rechte und Pflichten der mit der Überwachung beauftragten Personen. Die Strafprozessordnung ihrerseits bestimmt die grundrechtsrelevanten Überwachungsmassnahmen und die an sie geknüpften Voraussetzungen. Die am 1. Januar 2011 in Kraft getretene Strafprozessordnung hält denn auch verschiedene Ermächtigungsgrundlagen bereit, die eine Beweissammlung im Internet ermöglichen. Von Interesse sind dabei die Beschlagnahme und Durchsuchung von Datenträgern, die Überwachung des Post- und Fernmeldeverkehrs, die Observation sowie Regelungen über verdeckte Ermittlungen.

Ein Wort noch zur Häufigkeit solcher Überwachungsmassnahmen: Aus der erst kürzlich publizierten Statistik für das Jahr 2013 lässt sie sich herauslesen. Die Strafverfolgungsbehörden haben im letzten Jahr 10 860 Überwachungen angeordnet, was als viel erscheinen mag. Bei rund 750 000 verfolgten Kriminaldelikten bedeutet dies aber, dass gerade einmal für 1,4 Prozent der Fälle auf diese Ermittlungsmethoden zurückgegriffen wurde. Berücksichtigt man nur die Echt-

zeitüberwachungen, im Jahre 2013 waren es 3945, so sinkt der Anteil auf rund 0,5 Prozent aller verfolgten Kriminaldelikte. Von einer überbordenden Überwachung kann somit keine Rede sein. Etwa ein Drittel dieser Überwachungsmassnahmen wurde von den Strafverfolgungsbehörden angeordnet, um schwere Widerhandlungen gegen das Betäubungsmittelgesetz aufzuklären. Ein weiteres Drittel betrifft schwere Vermögensdelikte. Der Rest teilt sich auf diverse Deliktarten auf, darunter schwere Gewalt- und Sexualdelikte.

Was sind die Kernpunkte der Gesetzesrevision? Beginnend beim Geltungsbereich bestimmt das Gesetz, wer neu dazu verpflichtet werden kann mitzuwirken, sei dies aktiv, d. h., wer selber zu überwachen hat, oder passiv, d. h., wer eine Überwachung durch den Dienst zur Überwachung des Post- und Fernmeldeverkehrs dulden muss.

Ein zweiter Schwerpunkt betrifft die Aufbewahrung der Daten. Dabei stehen die sogenannten Randdaten im Vordergrund: Demnach soll neu für 12 statt wie bisher 6 Monate gespeichert werden können, wer wann mit wem wie lange und von wo telefoniert oder gemailt hat; diese Randdaten sind Informationen über einen elektronischen Kommunikationsvorgang, die nicht den Inhalt betreffen.

Ein drittes Anliegen der Revision betrifft die verschlüsselte Kommunikation und eine zusätzliche Ermächtigung in der Strafprozessordnung: Mit der sogenannten Govware, landläufig auch als Staatstrojaner bezeichnet, sollen unter strengsten Voraussetzungen, nur subsidiär und nur im Zusammenhang mit schwersten Straftaten Daten vor der Verschlüsselung abgefangen werden. In diesem Kontext ist auch die gesetzliche Grundlage für den Einsatz der sogenannten IMSI-Catcher zu nennen, mit denen sich Nutzer von Mobiltelefonen im Umkreis eines Catchers identifizieren und auch Gespräche mitschneiden lassen. Heftig umstritten ist, wie die Kosten für die Überwachungsmassnahmen zwischen Strafbehörden, Bund und mitwirkungspflichtigen Providern aufzuteilen sind.

Schliesslich hat sich Ihre Kommission für Rechtsfragen auch noch mit der Frage auseinandergesetzt, ob und gegebenenfalls inwieweit der Abbruch des ISS-Projekts zur Einführung eines Verarbeitungssystems beim Dienst für die Überwachung des Post- und Fernmeldeverkehrs Auswirkungen auf diese Gesetzgebung hat. Der Kommission wurde dabei versichert, dass nach dem heutigen Wissensstand der Wechsel zu einem neuen Systemanbieter keine Auswirkungen auf diese Totalrevision habe.

Nebst verschiedenen Anpassungen der Kommission am Entwurf als Folge der Anhörungen stehen sich Anträge von Mehr- und Minderheiten gegenüber, dies in der Frage der Aufbewahrungsdauer für die Randdaten – und zwar sowohl bei jenen des Post- wie bei jenen des Fernmeldeverkehrs –, bei der Kostenaufteilung für Überwachungsmassnahmen und bei den Übergangsbestimmungen. Es scheint nun so, dass mit den Einzelanträgen Fetz und Graber Konrad eine unübersichtliche Anzahl zusätzlicher Anträge in die Plenardebatte gelangt. Nach meinem Dafürhalten lassen sich die Anliegen, die mit diesen Anträgen vertreten werden, zusammenfassend auf drei inhaltliche Absichten bündeln, die damit verfolgt werden. Es geht erstens um die Ausgestaltung der Mitwirkungspflichten bestimmter Personenkreise, die im persönlichen Geltungsbereich dieser Gesetzgebung unterstellt werden, es geht zweitens um die Verordnungskompetenz des Bundesrates, und es geht drittens um die Frage der Kostenaufteilung zwischen den Akteuren. Ich glaube, dass wir, vor allem auch weil der Ständerat als Erstrat über dieses Gesetz entscheidet, durchaus in der Lage sind, diese Anträge in der Detailberatung zu diskutieren und auch darüber zu entscheiden.

Alles in allem lässt sich nach Auffassung der Kommission sagen, dass diese Revision den sich laufend verändernden Bedürfnissen der Strafverfolgung Rechnung trägt. Sie beachtet die grundrechtlichen Anforderungen und schafft vor allem eine saubere gesetzliche Grundlage für verdeckte Ermittlungen im Internet.

Die Kommission für Rechtsfragen empfiehlt Ihnen deshalb, auf die Vorlage einzutreten.

Stadler Markus (GL, UR): Die vorliegende Gesetzesrevision soll, wie wir gehört haben, vor allem sicherstellen, dass die notwendigen Überwachungen des Post- und Fernmeldeverkehrs möglich sind bzw. durch die Verwendung neuer Technologien, etwa die Verschlüsselung, nicht verhindert werden können. Die Notwendigkeit von Überwachungen besteht, wenn ein dringender Verdacht auf Begehung einer schweren Straftat besteht.

Hinter dem Anliegen stehen die Erfahrungen der Strafverfolgungsbehörden, die sich entsprechend für die Änderung und Umsetzung des Gesetzentwurfes aussprechen. Dieses Engagement im Interesse der Kriminalitätsbekämpfung ist aus dem Blickwinkel der Strafverfolgung verständlich. Allerdings gilt es, auch die mögliche Schwere des Eingriffs in die Daten- und Persönlichkeitsrechte der künftigen Betroffenen zu berücksichtigen. Weshalb? Es kann sich bei den Betroffenen auch um unschuldige überwachte Personen handeln, deren Unschuld erst im Nachhinein festgestellt wird.

Die beabsichtigten Überwachungsmethoden, gerade der Staatstrojaner – in der Botschaft Govware genannt –, ermöglichen es technisch, dass Datenarten und Personen erfasst werden, die eigentlich nach dem Sinne des Gesetzes oder in der Intention der Behörde nicht gemeint sind bzw. nicht gemeint sein dürfen. Bei den angesprochenen Datenkategorien kann es sich beispielsweise auch um solche handeln, die nicht aus der Datenübertragung stammen. Bei der Überwachungstätigkeit werden Zufallsfunde entstehen, zum Beispiel bei Leuten, die dauernd im gleichen Mehrfamilienhaus oder zufällig im gleichen Hotel wohnen oder sich gerade in der Nähe der gemeinten Person befinden. Neben eigentlichen Zufallsfunden im Sinne des Gesetzes wird es aber auch Einblicke in Daten von Personen geben, die aus irgendwelchen, auch privaten Gründen von Interesse sein könnten.

Eine Aufbewahrungspflicht für verdachtsunabhängige Daten, wenn auch nur Randdaten, ist an sich nicht unproblematisch. Der Bundesrat will diese Pflicht bei den Anbietern von Post- und Fernmeldediensten wesentlich ausweiten, was eigentlich den Nachweis von heute eindeutig zu kurzen Fristen verlangen würde. Die Kommission stellt mit ihrer Mehrheit, zu der ich zähle, bei den Postdiensten den Antrag, diese Frist zu kürzen. Ein Minderheitsantrag, den ich mittrage, will auch die beantragte Frist bei den Fernmeldediensten kürzen.

Behörden bestehen nicht aus Robotern, sondern aus Menschen, die unwillentlich Fehler machen oder die unlautere Absichten haben können. Missbrauch von Daten ist also denkbar. Es ist auch denkbar, dass durch den staatlichen Eingriff Private Zugang zu Daten anderer Privater erhalten, was die Tür für Missbrauch zusätzlich öffnet.

Eine Überwachung kann zwar nicht allein von der zuständigen Behörde entschieden werden, sondern braucht die Genehmigung eines Zwangsmassnahmengerichtes. Damit lastet aber viel auf dieser Instanz und selbstverständlich auch auf jener des Staatsanwaltes. Im Falle eines Begehrens der Staatsanwaltschaft, das unter Zeitdruck eingereicht wird, wird es für das Zwangsmassnahmengericht nicht einfach sein, dem Schutz der Grundrechte der betroffenen Person gebührendes Gewicht zu geben; einmal abgesehen davon, dass im Zweifelsfall eine Bewilligung einfacher zu begründen sein wird als eine Ablehnung des Gesuchs. Man darf sich auch fragen, ob ein Zwangsmassnahmenrichter ohne Weiteres in der Lage sein wird, nicht nur die juristischen Fragen einer Überwachungsmassnahme, sondern eben auch die technischen Möglichkeiten der einzusetzenden Geräte und Software, die ja in ständiger Entwicklung sein werden, genügend zu verstehen und die Auswirkungen auf eine Überwachungsmassnahme zu überblicken.

Auch bei der Notsuche und bei der Fahndung nach verurteilten Personen können Datenarten und Daten über Personen anfallen, die nicht im eigentlichen Sinne des Gesetzes sind. Auch hier, nicht nur bei der Überwachung zugunsten der Kri-

minalitätsbekämpfung, stellt sich im Vollzug die Frage, ob diese Daten zeitgerecht und umfassend und ohne vorausgehenden Fehlgebrauch gelöscht werden. Dass Wissen Macht ist und dass gerade das Wissen um die geheimen Gedanken und Taten des Menschen andere Menschen besonders stark interessieren könnte, muss nicht besonders betont werden.

Der Vollzug des beantragten Gesetzes setzt bei den involvierten Behörden und Diensten Menschen voraus, die bei der Überwachungstätigkeit punkto juristisch-technischen Wissens und Könnens sowie Integrität total auf der Höhe sind. Wird dem immer so sein? Es geht bei dieser Gesetzesvorlage also nicht bloss um Verbrechensbekämpfung, sondern auch um den Schutz unserer Grundrechte. Absolute Sicherheit wird es nicht geben – bei keinem Überwachungssystem. Umso mehr darf man, überspitzt gesagt, auch keine absolute Überwachung anvisieren. Es kommt dazu, dass die schweizerische Gesetzgebung ihren Zugriff auf inländische Anbieter beschränken muss.

Die Elemente «dringender Verdacht», «besondere Schwere der Tat» und «rechtsstaatliche Garantien» sind zwar gut, aber sie machen noch nicht das ganze Eingriffssystem aus, das beabsichtigt ist und notabene rechtlich oder eben auch missbräuchlich möglich sein wird. Wenn es bei Friedrich II. und besonders bei Voltaire schon vor 250 Jahren geheissen hat: «Die Gedanken sind frei», sollte es künftig nicht heissen: «Die Gedanken sind frei zugänglich.»

Nachdem ich aufgrund der Diskussionen in der Kommission davon ausgehen kann, dass heute die Themen Verbrechensbekämpfung und deren Finanzierung genügend Beachtung finden werden, habe ich mich auf den Aspekt des Grundrechtsschutzes konzentriert. Die Absichten, die hinter der Vorlage stehen, sind verständlich. Schliesslich darf der Staat nicht vor der Kriminalität kapitulieren. Deshalb habe ich mich dem Eintretensentscheid in der Kommission angeschlossen. Aber das Gebot der Verhältnismässigkeit und, im Vollzug, des zurückhaltenden Umgangs mit den privaten Daten muss entsprechend hoch gewichtet werden. Gerade die Pflicht zur langen Datenaufbewahrung und der Einsatz von Staatstrojanern erfordern in unserem Saal einen sehr kritischen Blick. Nach dem derzeitigen Stand der Diskussion und aufgrund des Antrages der Kommission kann ich der Vorlage noch nicht zustimmen. Ich habe mich deshalb in der Kommission der Stimme enthalten. Es erstaunt mich daher nicht sonderlich, dass nun im Plenum noch verschiedene Einzelanträge gestellt worden sind.

Savary Géraldine (S, VD): Effectivement, l'entrée en matière n'est pas contestée, même si un certain nombre de débats de principe ont eu lieu, et je remercie Monsieur Stadler de les avoir évoqués. Je souhaiterais faire quelques remarques et commentaires sur ce projet.

La première remarque est que le projet de modification de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication n'est pas celui de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure que nous allons discuter ces prochains mois. Je le dis parce que parfois on confond, parce que parfois on imagine que tous les moyens qui sont prévus dans la loi sur la surveillance de la correspondance par poste et télécommunication s'exprimeraient déjà comme un préambule aux mesures que nous allons discuter dans la loi sur la sûreté intérieure. Eh bien, non, ce projet de modification est véritablement une adaptation à la situation actuelle.

On peut dire sans trop s'avancer que la criminalité use et abuse des nouveaux moyens de télécommunication en particulier des réseaux Internet et des téléphones mobiles. Il paraît clair aujourd'hui qu'un revendeur de drogue par exemple ne va pas envoyer une lettre en courrier B pour fixer un rendez-vous pour trafiquer, tout comme il est désormais connu qu'un pédocriminel utilise la Toile pour tisser la trame de son délit. Comme le dit le Conseil fédéral, les nouvelles technologies facilitent les possibilités d'infraction. Ce n'est donc pas aujourd'hui d'une extension de la surveillance publique que nous discutons, mais d'une mise en adéquation

entre les moyens de la justice et les pratiques criminelles. Personne ne souhaite ici, j'espère, que les autorités pénales se déplacent en tricycle quand les criminels roulent en Ferrari.

Deuxième remarque: les procédures nécessaires pour ordonner des écoutes téléphoniques ou la récolte de données secondaires sont longues et scrupuleuses. Seules des personnes fortement soupçonnées d'avoir commis des infractions graves peuvent y être soumises. On ne parle pas ici de surveillance préventive. La liste des infractions mentionne par exemple les délits de criminalité économique, le trafic de stupéfiants ou la pédocriminalité. Au grand regret d'ailleurs des autorités de poursuite judiciaire! Si vous lisez les réponses à la consultation, vous voyez que certaines autorités de poursuite judiciaire regrettent que le champ d'intervention soit restreint à ce point-là. Au grand regret des autorités pénales, un certain nombre d'infractions échappent aux autorisations d'écoute ou de transmission de données secondaires. La surveillance doit être autorisée par le tribunal des mesures de contrainte. La demande est adressée par un juge. Le cadre reste donc très strict. Les autorités de poursuite n'en profitent pas, en principe.

Selon les chiffres du service de surveillance de la Confédération, on constate bien sûr une forte augmentation de la surveillance active ces dernières années. Mais cela s'explique non pas par le nombre de personnes sous surveillance, mais par le nombre de raccordements téléphoniques. Même un petit trafiquant qui est aujourd'hui dans nos rues a trois ou quatre Natels. A chaque fois, une demande de raccordement doit être formulée.

En 2011, il y avait, en moyenne nationale, 0,3 mesure de surveillance active pour 1000 habitants, ce qui se traduit, pour les localités les plus importantes, par: 0,5 à Zurich, 0,1 à Berne, 0,4 dans le canton de Vaud, 1,3 à Genève. On constate donc que Zurich et Genève ordonnent le plus de surveillance. Ce constat s'explique par le fait que ces villes disposent d'un aéroport, qui induit un trafic de personnes et parfois aussi des délits.

La nouvelle loi ne changera rien à cette dynamique. Elle ne donne pas plus de marge de manoeuvre aux autorités de poursuite, mais elle fixe les responsabilités de chacun, étend la liste des personnes contraintes de collaborer et inscrit dans des articles de lois ce qui figure aujourd'hui dans une ordonnance.

Enfin, les programmes informatiques «Govware», appelés en français «cheval de Troie», sont autorisés, mais là aussi à des conditions extrêmement strictes, pour des infractions pour lesquelles une investigation secrète est autorisée, selon l'article 269 alinéa 2 du Code de procédure pénale.

Ma dernière remarque concerne les coûts de la surveillance. C'est un sujet qui a été extrêmement discuté en commission. Manifestement, il le sera aujourd'hui aussi puisque notre collègue Konrad Graber a aussi déposé des propositions sur ce point. Cette question des frais et émoluments à l'article 38 est évidemment très importante.

L'intransigeance des opérateurs qui nous ont invités à refuser d'entrer en matière lors des auditions en nous expliquant que la Constitution serait bafouée, leur manque de compréhension total face aux difficultés que rencontrent aujourd'hui les autorités de poursuite, l'absence complète de réponses quant aux coûts occasionnés par les demandes de la justice à collaborer à des mesures de surveillance ont incité la majorité des membres de la commission à leur faire assumer la totalité des coûts et émoluments nécessaires à l'exécution de leurs obligations, j'y reviendrai plus en détail quand nous examinerons l'article 38. Je pense que, dans la poursuite des infractions, nous sommes face à une responsabilité collective. Nous devons donner un cadre strict, mais qui permet aux individus d'être protégés contre l'intrusion dans leur sphère privée. Cependant, nous devons aussi permettre aux autorités pénales de faire leur travail. Ces dernières doivent pouvoir travailler avec les instruments modernes indispensables à leurs enquêtes, sans que des coûts excessifs, exagérés, ne les fassent renoncer à ces enquêtes. Les personnes obligées de collaborer, c'est-à-dire les opérateurs et

autres prestataires de services Internet, doivent aussi mettre un peu de bonne volonté, un peu de compréhension et, pourquoi pas, quelques moyens financiers et en personnel à disposition pour atteindre cet objectif.

C'est pour cette raison que je vous invite à entrer en matière – cela n'est de toute façon pas contesté – et à accepter en particulier les propositions de la majorité de la commission, notamment à l'article 38. Il est important que chacune et chacun d'entre nous prenne ses responsabilités, nous en tant que parlementaire, ainsi que le Conseil fédéral, en donnant un cadre strict et les cantons en ordonnant des enquêtes et en respectant la sphère privée des uns et des autres. Mais les opérateurs pourraient aussi assumer une part des responsabilités. Franchement, pour être honnête, jusqu'à maintenant, je ne les ai pas beaucoup entendus parler de responsabilités, mais plutôt de moyens financiers.

Ce sont les raisons pour lesquelles je vous invite à adopter ce projet, tel qu'il est présenté par votre commission.

Janiak Claude (S, BL): Technologische Entwicklungen sind ein grosser Segen für uns alle. Es ist aber auch eine Tatsache, dass sie auch von denjenigen genutzt werden, die nicht unbedingt das Gute wollen. Die neuen Möglichkeiten in der Telekommunikation müssen beim Verdacht auf schwere Kriminalität so überwacht werden können, dass keine Lücken entstehen. Wenn E-Mails oder Telefongespräche verschlüsselt werden können und die Strafverfolgung keinen Zugang dazu hat, dann werden Kriminelle geradezu dazu eingeladen, nur noch über verschlüsselte Kommunikationstechnologien zu kommunizieren. Notwendige Überwachungen des Fernmeldeverkehrs dürfen nicht durch die Verwendung von neuen Technologien verhindert werden können.

Solche Überwachungsmöglichkeiten sind indessen Eingriffe in die Grundrechte, die sehr weit gehen können. Da steht der Vorwurf «Schnüffelstaat» oder «Eingriff in die Privatsphäre» sehr schnell im Raum. Wie überall im Strafverfahren müssen die Voraussetzungen, unter denen solche Eingriffe zulässig sind, klar umschrieben sein. Die Anordnung von derartigen Massnahmen muss als Ultima Ratio zur Verfügung stehen, wenn andere Mittel der Strafverfolgung versagen.

Facebook, Google, Whatsapp – wer nutzt diese Dienste nicht? Und sind nicht alle glücklich, dass alles gratis ist? Wer ist sich schon wirklich bewusst, dass seine Daten im Gegenzug verwendet werden dürfen? Sicher die wenigsten ahnen das Ausmass. Nur so lässt es sich erklären, dass viele jener, die ihre Privatsphäre gefährdet sehen, auch ungefragt Persönliches an Empfänger weiterleiten, die sie nie darum gebeten haben.

Diese Widersprüche sind für mich jedenfalls teilweise Erklärungen für den Inhalt zahlreicher Schreiben, die wir im Zusammenhang mit dem Büpfi erhalten haben. Da wird so ziemlich alles durcheinandergemischt. Die NSA-Aktivitäten und die Unsicherheit, die sich darum herum verbreiten lässt, erleichtern den Durchblick auch nicht gerade. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, der uns übrigens in der Kommission immer auch begleitet hat, insbesondere auch während der Detailberatung, hat in einem lezenswerten Interview in der «NZZ» vom vergangenen Donnerstag die Fragen verständlich aufgezeigt, die sich im Zusammenhang mit dem Büpfi und dem Nachrichtendienstgesetz, das den Räten schon zugewiesen worden ist, stellen.

Bei der Beratung dieser Vorlage ist es wichtig zu unterstreichen – das ist schon mehrfach getan worden, aber ich mache es jetzt noch einmal –, dass es hier nicht um die präventive Überwachung geht; diese wird bei der Beratung des neuen Nachrichtendienstgesetzes das Thema sein. Hier geht es allein um die Aufklärung schwerer Straftaten; sie soll nicht durch neue Kommunikationstechnologien verhindert oder verunmöglicht werden. Im Fokus stehen die Bereiche organisiertes Verbrechen, Drogenhandel, Terrorismus und Kinderpornografie. Dabei gibt es, das ist sehr wichtig, genau definierte Spielregeln. Das ist der Inhalt der Revision, insbesondere auch der Revision der Strafprozessordnung.

Ein zentrales Thema der Revision ist der Einsatz von Govware oder Staatstrojanern als Antwort auf die zunehmende Verbreitung der Datenverschlüsselung. In der Botschaft wird erläutert, was der Unterschied zwischen Govware und Trojanern ist; ich verweise auf Seite 2772 oben. Beim Einsatz von Govware geht es nicht um die Verbreitung von Überwachungsprogrammen, sondern um die Möglichkeit, ein Gerät beziehungsweise eine konkrete Person zu überwachen. Bei verschlüsselter Kommunikation kommt man nur mit solchen Programmen überhaupt an die Daten heran. Mit Govware lassen sich die Daten an der Quelle abfangen, bevor sie verschlüsselt werden.

Weil in das Informatiksystem einer überwachten Person eingedrungen wird, unterliegt der Einsatz von Govware strengeren Bedingungen als die klassische Überwachung. Der Deliktskatalog entspricht dem für die verdeckte Ermittlung massgebenden Artikel 286 der Strafprozessordnung. Die Programme dürfen nur im Zusammenhang mit den schwersten Straftaten verwendet werden; sie dürfen nur subsidiär eingesetzt werden; sie dürfen ausschliesslich zur Überwachung des Fernmeldeverkehrs eingesetzt werden, nicht etwa zur Beschaffung anderer Daten auf dem betreffenden Computer. Die Beschränkung auf Kommunikationsdaten ist gesetzlich festgeschrieben. Eine Online-Durchsuchung ist nicht zulässig. Es bedarf einer richterlichen Genehmigung durch das Zwangsmassnahmengericht. Daten, die nicht aus dem Fernmeldeverkehr stammen, müssen vernichtet werden und sind ohnehin nicht verwertbar. Aber es schleckt keine Geiss weg, dass hier das Spannungsfeld zwischen der persönlichen Freiheit, der Privatsphäre und dem Schutz der Grundrechte einerseits und den Interessen auf dem Gebiet der Kriminalitätsbekämpfung andererseits offensichtlich wird.

Das Büpfi ist ja die Hauptvorlage; es schafft den Rahmen für die Umsetzung von Überwachungsmassnahmen, die von der Strafprozessordnung vorgesehen sind. Wir schaffen nicht Überwachungsmassnahmen an sich; das Büpfi ist nur der Rahmen, um die Überwachungsmassnahmen, die in der Strafprozessordnung vorgesehen sind, umsetzen zu können. Das Büpfi gehört zum Verwaltungsrecht, es regelt insbesondere die Pflichten der Personen, die mit Überwachungen beauftragt sind. Die Strafprozessordnung dagegen bestimmt, welche Massnahmen unter welchen Bedingungen zulässig sind. Bei den verschiedenen Massnahmen gibt es eine Eskalation bzw. verschiedene Bedingungen, die erfüllt werden müssen.

Nochmals: Die Strafprozessordnung sieht vor, dass eine Überwachung erst dann durchgeführt wird, wenn in einem Strafverfahren der dringende Verdacht besteht, dass eine schwere Straftat begangen worden ist, und andere Mittel zu keinem Ergebnis geführt haben. Die Überwachung muss immer von einem Zwangsmassnahmengericht genehmigt werden. Wie überall, wo Richter entscheiden, hängt es auch von den Persönlichkeiten ab. Sie müssen prüfen, ob der Tatverdacht eine schwere Straftat betrifft und ob mildere Massnahmen geprüft worden sind. Die Strafverfolger müssen dartun können, dass bisherige Untersuchungshandlungen erfolglos geblieben oder die Ermittlungen sonst aussichtslos sind oder auf unverhältnismässige Weise erschwert werden. Diese Voraussetzungen müssen kumulativ erfüllt sein.

Die Botschaft ist bei diesen Massnahmen bzw. bei den Voraussetzungen, die an Letztere gestellt werden, ausführlich. Ich verweise auf die Seiten 2767ff. Die richterliche Behörde verfügt also für ihre Entscheide über genügend Materialien, die darlegen, wie diese Bestimmungen, sofern überhaupt Bedarf besteht, zu interpretieren sind. Der Wille des Gesetzgebers ist klar zum Ausdruck gebracht.

Noch ein kurzes Wort zur Frage der Aufbewahrung der Daten, die auch Gegenstand der Revision ist: Der Übergang zur zentralen Langzeitaufbewahrung der Daten ist eine Neuerung des Büpfi. Die durch die Fernmeldeüberwachung gesammelten Daten werden im Informatiksystem des Dienstes ÜPF langfristig aufbewahrt. Heute übermittelt der Dienst diese Daten auf Datenträgern per Post an die Strafverfolgungsbehörden. Wenn die Behörden die Daten erhal-

ten haben, werden sie aus dem System des Dienstes gelöscht. Die Strafverfolgungsbehörden, die beschuldigte Person und deren Rechtsbeistand können mit dem neuen Gesetz grundsätzlich online auf die Daten im neuen System zugreifen. Das ist sicher eine praktische Änderung, die hier vollzogen wird. Umstritten ist, auch das war ein Thema bei meinen Vorrednern, wie lange die Randdaten aufbewahrt werden müssen, 6 oder 12 Monate.

Ich bitte Sie, der Mehrheit zu folgen und dort, wo es einen Antrag der Minderheit Stadler Markus gibt, dieser zu folgen. Das würde helfen, den vielen öffentlich bekundeten Bedenken in diesem Zusammenhang – auch denjenigen des Edöb, im Übrigen – Rechnung zu tragen. Ich darf auch noch darauf hinweisen, dass wir bei verschiedenen Bestimmungen verlangt haben, dass Statistiken über diese Überwachungen geführt werden, damit wir auch einen weiteren Anhaltspunkt haben, wie dieses Gesetz dann vollzogen wird.

Ich bitte Sie, auf die Vorlage einzutreten und im Wesentlichen Ihrer Kommission zu folgen. Im Zusammenhang mit den Randdaten bitte ich Sie, bei Artikel 19 Absatz 4 der Mehrheit zu folgen und bei Artikel 26 Absatz 5, wo es einen Antrag der Minderheit Stadler Markus zum gleichen Thema gibt, dieser zu folgen.

Schmid Martin (RL, GR): Ich kann Ihnen bestätigen, dass ich auch an den fünf Tage dauernden Kommissionsberatungen über das BÜP teilgenommen habe. Ich kann Ihnen auch versichern, dass wir uns in der Kommission schwergetan haben. Einerseits anerkennen wir den technologischen Fortschritt. Wir alle brauchen die neuen Kommunikationsmittel. Viele von uns pflegten beruflich auch eine gewisse Nähe zu den Strafverfolgungsbehörden, sei es als Anwälte, sei es als Polizei- und Justizdirektoren. Wir hörten auch die entsprechenden Kreise an. Die Botschaft, mit welcher wir uns hier auseinanderzusetzen haben, ist technisch komplex, auch von den Anwendungsbereichen her. Es ist schwierig nachzuvollziehen, sofern man selber nicht Informatikspezialist ist, welche Möglichkeiten in Zukunft überhaupt denkbar sind, wenn wir jetzt die gesetzlichen Grundlagen schaffen. Denn eines müssen wir anerkennen: Die technologische Entwicklung wird weitergehen, die Botschaft gibt nicht den Stand von heute wieder. Wir schaffen eine Gesetzgebung, welche auch morgen und übermorgen bei weiteren technologischen Entwicklungen den Strafverfolgungsbehörden die Möglichkeit geben sollte, im Bereich des Fernmelde- und Internetverkehrs auf Daten zuzugreifen.

Wir haben letztlich grundsätzlich darüber zu entscheiden, welches das erwünschte Ausmass an Überwachung sein soll. Ich meine, die Kommission hat hier eine gute Abwägung aufgrund der bundesrätlichen Vorlage vorgenommen, die wir auch als gut qualifiziert haben. Wir haben es uns nicht einfach gemacht. Persönlich bin ich der Auffassung, ein wenig geprägt vom Hintergrund des diskutierten Datenmissbrauchs, dass wir insbesondere im Bereiche der Vorratsdaten und der Aufbewahrungsfristen uns eher am kürzeren Ende orientieren sollten. Ich bin deshalb wie gewisse Vorredner auch der Auffassung, dass die Minderheits- bzw. Mehrheitsanträge, welche in diesem Bereich keine allzu grosse Ausdehnung gegenüber der heutigen gesetzlichen Regelung bewirken, eine gute Ausgangslage bieten, um einerseits die neuen technologischen Möglichkeiten im Gesetz zu implementieren und andererseits auch nicht übers Ziel hinauszuschiessen. Denn es konnte in der Kommission auch nicht aufgezeigt werden, welche zusätzlichen Delikte hätten aufgeklärt werden können, wenn man noch ein paar Monate mehr für die Vorratsdatenspeicherung zur Verfügung gehabt hätte. Wichtig ist, dass es dieses Instrument gibt.

Es wurde schon von vielen Votanten darauf hingewiesen, dass ein wesentlicher Kernpunkt eben letztlich die Kostenfrage ist. Ich begründe dazu dann auch meinen Minderheitsantrag und erkläre, warum dem bundesrätlichen Entwurf zu folgen ist. Ich sehe das im Gesamtkontext dieser Vorlage. Für mich geht es hier nicht allein um die Gebührenfrage; das ist nur ein Teil. Für mich geht es im Prinzip einfach darum, wer im Bereich der Strafverfolgung die Kosten übernehmen

soll, und dann geht es um eine noch wesentlichere Frage: Wenn diese Untersuchungsmassnahmen einmal kostenlos wären, würde dann nicht die Gefahr bestehen, dass die Strafverfolgungsbehörden primär nur noch dieses Mittel einsetzen würden? Ich möchte hier bewusst diese Frage in den Raum stellen. Die Antwort können wir dann im Detail bei meinem Minderheitsantrag diskutieren.

Ich persönlich habe mir meine Meinung gemacht und bin der festen Überzeugung, dass wir in diesem Bereich doch eine gewisse Schwelle, eine gewisse Hürde einbauen sollten, damit die weiteren gesetzlichen Möglichkeiten, die wir jetzt im Bereich der Überwachung schaffen, in der Praxis nur dann angewendet werden, wenn es verhältnismässig ist, wenn es auch gemäss den Strafverfolgungsbehörden als adäquat betrachtet wird. Ich glaube, das ist dann der Fall, wenn es eben auch die Kantone, die Strafverfolgungsbehörden, noch etwas kostet. Dann überlegt man sich eben wirklich, ob dieses Mittel eingesetzt werden sollte. Ansonsten, wenn man eben in jedem Falle eine kostenlose Untersuchung starten kann – obwohl noch der Filter des Zwangsmassnahmengerichtes da ist –, befürchte ich, dass die Gefahr besteht, dass man in Zukunft dieses Mittel sehr viel mehr einsetzt, weil es eben dann letztlich für Strafverfolgungsbehörden die bequemere, finanziell günstigere Lösung ist.

Ich möchte Ihnen beliebt machen, auf diese Vorlage einzutreten, weil ich, entgegen gewissen Schreiben, die wir erhalten haben, nicht der Auffassung bin, dass wir sie nicht seriös vorgeprüft hätten, dass wir uns nicht adäquat und seriös mit der Frage der Abwägung zwischen dem Schutz der Privatsphäre und den Interessen der Strafverfolgungsbehörden auseinandergesetzt hätten.

Ich möchte Sie auch bitten, der Minderheit Stadler Markus und, im Bereich der Kostenfolgen, der Minderheit Schmid Martin zu folgen, ansonsten der Mehrheit der Kommission.

Fetz Anita (S, BS): Im Gegensatz zu allen Vorrednern und zur Vorrednerin bewerte ich die Vorlage deutlich kritischer, um es gerade vorneweg zu sagen. Der Bundesrat will mit diesem Überwachungsgesetz nach seinen eigenen Worten «nicht mehr, sondern besser» überwachen können, so sagt er es in der Botschaft. Es geht ihm also nach seinen eigenen Worten um Qualität und nicht um Quantität. Das finde ich an und für sich gut. Das ist aber deswegen seltsam, weil in der gesamten Botschaft keine einzige Aussage zur Qualität des bisherigen Überwachungsregimes in Strafsachen enthalten ist – keine einzige.

Wir wissen zwar, wie oft wegen welcher Straftaten überwacht worden ist, aber wir haben keine Ahnung, wie oft solche Überwachungen überhaupt zu Strafverfahren und Verurteilungen geführt haben und welche dieser Verfahren und Verurteilungen überhaupt die ursprünglichen Delikte betrafen und nicht etwa Zufallsfunde waren; das sind jetzt nur zwei Beispiele. Wir finden zu all diesen qualitativen Aspekten der Überwachung keine Aussagen in der Botschaft – keine einzige. Das heisst: Es ist völlig unklar, wie wirksam diese Überwachung ist. Ich habe nichts gegen Überwachung bei kriminellen Straftaten, aber dann möchte ich etwas über die Wirksamkeit wissen. Entweder wird sie nicht erhoben, oder es steht irgendwo anders. Das ist für mich die absolut zentrale Frage. In diesem heiklen Bereich von Bürgerrechten und Datenspeicherungen auf Vorrat finde ich das sehr befremdlich. Noch befremdlicher aber finde ich unter diesen Vorzeichen, dass der Anwendungsbereich des bisherigen Überwachungsgesetzes ausgedehnt werden soll – und zwar nicht in erster Linie qualitativ, sondern von der Menge und vom Geltungsbereich her. Darauf werde ich im Zusammenhang mit meinen Anträgen zurückkommen.

Ich bin mir bewusst, dass hier von Strafverfolgung die Rede ist. Es geht um die überwachungstechnische Verfolgung von Straftätern im gesetzlich geordneten Rahmen eines Rechtsstaates; dagegen habe ich nichts. Wir sollten das aber nicht als Killerargument gegen die Wahrung der Bürgerrechte einsetzen. Im Katalog der entsprechenden Straftaten, bei denen überwacht werden darf, sind nicht nur unbestrittene Schwerststraftaten enthalten, z. B. Verbrechen gegen die

Menschlichkeit, Mord oder Kindsmissbrauch, sondern es ist auch der einfache Diebstahl ab einer gewissen Schwere dabei – dies im Gegensatz zum illegalen Waffenhandel, den wir erst heute hinzufügen werden.

Diese Gratwanderung zwischen Bürgerrecht und Strafverfolgung ist darum heikel, weil die Datenspeicherung auf Vorrat im Bereich der Grundrechte liegt. Das ist in einer Demokratie und in einem Rechtsstaat die allerwichtigste Komponente, die es zu beachten gilt. Denn mit allen Daten, die nicht der verdächtigen Nadel im Heuhaufen entsprechen – diese sucht man ja, die verdächtige Nadel im grossen Datenheuhaufen –, sind potenziell Bürgergrundrechte tangiert. Wir reden hier immerhin von flächendeckenden Sammlungen von Daten, bei denen keine Verdachtsmomente bestehen. Das ist nach der Snowden-Aufklärung umso befremdlicher, weil grosse Datensammlungen dazu verführen, dass man sie missbraucht. Wir müssen uns also die Frage gefallen lassen, was wir wie lange sammeln lassen wollen und wie lange diese Daten aufbewahrt werden sollen.

Noch ein Wort zum Staatstrojaner: Das ist ja die Spionagesoftware, die auf Smartphones und Computern benutzt werden soll. Ich finde bemerkenswert, was die Botschaft zu den Trojanern festhält: «Aus Sicht der kontaktierten Fachleute aus dem wissenschaftlichen Bereich ist es jedoch nicht möglich, Govware» – das ist diese Spionagesoftware – «zu entwickeln und in Betrieb zu halten, die unter allen Umständen korrekt funktioniert, d. h. keinen Einfluss auf andere Programme oder Funktionen hat ... Es könnten beliebige System- und Nutzerdaten ohne Wissen des Inhabers kopiert, verändert, gelöscht oder hinzugefügt werden. Diese Hintertür führe zudem zu einer Schwachstelle im Computersystem, welche auch von Dritten ausgenutzt werden könne.» Sie finden dieses Zitat auf Seite 2775 der Botschaft. Das ist eine sehr ehrliche Aussage des Bundesrates, aber eine sehr happige. Jetzt müssen Sie das einmal auf sich wirken lassen und überlegen, was es heisst. In deutschen Medien konnte man in den letzten Wochen lesen, dass Deutschland seit Jahren keine Staatstrojaner mehr einsetzt, weil der deutsche Staat nicht in der Lage war, sie so zu gestalten, dass sie mit dem Grundgesetz konform waren. Deshalb stelle ich zwei Fragen an Sie, Frau Bundesrätin. Die erste Frage: Ist der Bundesrat wirklich überzeugt, dass er Govware ohne Grundrechtsverletzung einsetzen kann? Das würde ja heissen, dass er bessere Programme habe als der deutsche Staat. Die zweite Frage: Wer programmiert diese Govware – staatliche Stellen oder private Firmen? Bei privaten Firmen müsste man sich dann fragen: Ist garantiert, dass sie nicht auch wieder eine verdeckte Überwachung in der Überwachung haben? Das ist für mich eine wichtige Frage; wir sind uns heute ja alles gewohnt.

Ich bin nicht Mitglied der zuständigen Kommission, aber ich habe mir die Mühe genommen, sämtliche Protokolle durchzusehen, weil mir dieses Thema sehr wichtig ist. Zusammen mit der Fahne macht das etwa ein Kilogramm Papier. Aufgrund dieser Unterlagen habe ich den einen oder anderen Antrag deponiert, damit wir bei einigen Punkten zusätzliche Klarheit schaffen und für mehr Transparenz sorgen können. In diesem heiklen Bereich zwischen flächendeckenden Datensammlungen, Bürgerrechten und berechtigten Interessen der Strafverfolgung müssen wir für vernünftige Regeln und vor allem für kontrollierte Transparenz sorgen.

Meine Zustimmung zu diesem Gesetz bedingt, dass die Überwachungszeit nicht ausgeweitet wird, sondern bei 6 Monaten bleibt, dass es keine Kostenübernahme gibt – da bin ich ganz auf der Linie Schmid –, denn sonst wird flott überwacht, und dass gewisse Anträge von mir, es müssen nicht alle sein, übernommen werden, denn sie schaffen wirklich eine gewisse Klarheit und Abgrenzung. Dann bin ich bereit, der Änderung zuzustimmen.

Graber Konrad (CE, LU): Zuerst danke ich der Kommission für Rechtsfragen für die intensive Beratung der komplexen Materie, sie ist von verschiedenen Kommissionsmitgliedern dargelegt worden. Persönlich komme ich zur Auffassung, dass es sich insgesamt um ein Gesetz handelt, das man

heute verabschieden kann. Wenn ich jetzt noch Änderungsanträge mit zwei Stossrichtungen einreiche, tue ich das deshalb, weil es mir wichtig erscheint, dass die damit verbundene Thematik im Ratsplenum diskutiert wird. Es handelt sich also nicht um eine Kritik an der Arbeit der zuständigen Kommission.

Ich bin Vorstandsmitglied der Asut, des Schweizerischen Verbands der Telekommunikation, womit ich meine Interessen offenlege. Zum Hinweis von Frau Savary möchte ich einfach sagen: Ich stehe hinter dem Gesetz. Ich übe keine Kritik. Ich werde auch für Eintreten sein, ich bin aber schon der Meinung, dass die Möglichkeit bestehen muss, gewisse Punkte noch zu ändern. Mir ist es vor allem auch ein Anliegen, wie das gesagt worden ist, dass schwere Straftatbestände verfolgt werden können und dass die Justiz gleich lange Spiesse hat wie allfällige Rechtsbrecher. Es geht also um gleich lange Spiesse, um gleiche Mittel, und das scheint mir wichtig zu sein, dazu stehe ich.

Ich bin deshalb für Eintreten. Ich möchte mit meinen Anträgen vor allem zwei Themen noch ansprechen: Zum Ersten geht es, es ist heute von Herrn Schmid und Frau Fetz angesprochen worden, um eine wirkungsorientierte und effiziente Überwachung. Neue Überwachungsmassnahmen ziehen Investitionen in technische Einrichtungen sowie Betriebskosten nach sich. Es muss deshalb sichergestellt werden, dass nur dann Investitionen zur Überwachung einzelner Dienstleistungen gemacht werden müssen, wenn diese Dienste auch eine massgebliche Bedeutung für die Aufklärung von strafbaren Handlungen haben. Es geht also um die Frage der Verhältnismässigkeit. Es soll verhindert werden, dass vorab Investitionen in Einrichtungen getätigt werden müssen, die dann nur höchst selten beziehungsweise nie genutzt werden oder die keine Bedeutung haben für die Aufklärung von Straftaten. Dieses Prinzip soll aus meiner Sicht noch in den Artikeln 22, 26 und 27 verankert werden. Der Präsident der Kommission hat es angesprochen: Wir haben hier wahrscheinlich nicht so manches Thema zu besprechen; dies ist aus meiner Sicht aber ein zentrales Thema.

Ein zweites Thema betrifft die Kosten der Überwachung selber. Aus Sicht der Branche ist eine angemessene Entschädigung für die Investitionen und Betriebskosten, wie dies in Österreich oder England der Fall ist, erforderlich. Die Mehrheit der Kommission des Ständerates hat jegliche Entschädigung der betroffenen Unternehmen aus dem Bundesgesetz gestrichen. Wenn wir dies bis zum Schluss durchdenken, erkennen wir, dass dies letztlich einer Subventionierung der Straftäter durch die Endkunden, durch die Konsumentinnen und Konsumenten, gleichkommen würde, d. h., die Unternehmen finanzieren die Überwachung und übertragen diese Ausgaben dann auf die Kosten für die Netznutzung respektive auf ihre Tarife. Da muss ich Ihnen Folgendes sagen: Wir können ja nicht im Ernst eine Subventionierung der Straftäter durch die Kundinnen und Kunden befürworten. Daher fordere ich, dass mindestens die variablen Kosten der Branche gedeckt werden, d. h. die Kosten, die verursacht werden, wenn ein entsprechender Auftrag erteilt wird. Wie das in jedem anderen Bereich üblich ist, soll derjenige, der einen Auftrag erteilt, auch die Kosten tragen. Selbstverständlich kann man auch Offerten einholen, um sicher zu sein, dass die Kosten nicht in einem Missverhältnis zum Nutzen stehen.

Ich bin aus diesen Überlegungen für Eintreten. Ich bitte Sie aber, in der Detailberatung diesen zwei Punkten spezielle Beachtung zu schenken und dann den entsprechenden Anträgen zuzustimmen.

Savary Géraldine (S, VD): Je voudrais répondre brièvement à Monsieur Graber, car la question de la subvention indirecte que les opérateurs offriraient aux autorités de poursuite a aussi été discutée. On peut considérer que – de mauvais gré bien sûr – les opérateurs ont également comme clients des criminels, qui sont des criminels pour toutes sortes de délits mais qui en principe paient leurs abonnements de téléphonie mobile, et c'est aussi, au fond, parce qu'ils sont acteurs – sans le vouloir évidemment – que les

opérateurs ont une contribution à apporter à la poursuite des délits et des infractions en Suisse. Il n'est donc pas tout à fait correct de parler de subvention, puisque parmi les clients de ces opérateurs on trouve malheureusement des criminels. C'est non seulement le travail des autorités de poursuite, mais également celui des opérateurs, de faire en sorte que ces criminels soient repérés et arrêtés.

Sommaruga Simonetta, Bundesrätin: Ich glaube, ich habe noch selten erlebt, dass man in ein Gesetz so vieles hineinliert, was gar nicht drinsteht. Deshalb möchte ich Ihnen heute ausnahmsweise zuerst einmal sagen, worum es in diesem Gesetz nicht geht: Es geht in diesem Gesetz nicht um den Nachrichtendienst, es geht nicht um präventive Überwachung, und es geht auch nicht um das Bespitzeln und Ausspionieren von unbescholtenen Bürgerinnen und Bürgern. Es geht beim Gesetz, das wir heute beraten, um Folgendes: Wenn in einem laufenden Strafverfahren der dringende Verdacht besteht, dass eine schwere Straftat begangen wurde, dann soll man auch die Telekommunikation der betreffenden Person überwachen können. Darum geht es in diesem Gesetz. Es geht also nur um Fälle, bei denen erstens ein Strafverfahren eröffnet wurde, zweitens der Verdacht besteht, dass eine schwere Straftat begangen wurde, und drittens ein Gericht die Überwachungsmassnahme bewilligt hat. Damit Sie das auch wissen: Das ist heute schon möglich. Es ist auch nicht so, dass wir irgendwelche neuen Überwachungsmassnahmen beschliessen würden.

Warum also eine Totalrevision dieses Gesetzes mit dem schönen Namen Büp? Wir schlagen Ihnen eine Totalrevision vor, weil sich die Telekommunikation in den letzten Jahren enorm entwickelt und verändert hat. Davon profitieren wir alle und sind – jedenfalls meistens – auch ganz glücklich damit. Aber eben nicht nur wir sind glücklich damit, von diesen neuen Technologien und den technologischen Möglichkeiten profitieren auch die Kriminellen. Es kann aber ja nicht sein, dass wir ihnen diese neuen Technologien einfach überlassen und aufgrund fehlender gesetzlicher Grundlagen auf die Aufklärung schwerer Delikte, z. B. im Drogenhandel, in der Kinderpornografie, im Terrorismus oder in der organisierten Kriminalität allgemein, verzichten.

Ich bin mir sehr wohl bewusst, dass es sich bei diesen Überwachungsmassnahmen – gerade wenn es um das Eindringen in Computer geht, ich komme noch darauf zurück – um weitgehende Eingriffe in die Grundrechte des Individuums handelt. Die persönliche Freiheit und der Grundrechtsschutz haben in unserem Land einen hohen Stellenwert, und das soll auch so bleiben. Deshalb haben wir ein Interesse, dass erstens die gesetzlichen Grundlagen mit der technischen Ausgangslage übereinstimmen – das schafft Rechtssicherheit – und dass zweitens für jede Überwachungsmassnahme eine Güterabwägung vorgenommen wird, nämlich individuelle Freiheit versus Verbrechensbekämpfung und Aufklärung schwerer und schwerster Straftaten. Diese Güterabwägung spielt bei dieser Gesetzesrevision eine ganz wichtige Rolle. Es gilt der Grundsatz: Je stärker eine bestimmte Massnahme die persönliche Freiheit des Individuums beeinträchtigt, desto höher muss die Hürde sein, die es zu nehmen gilt, damit eine solche Massnahme bewilligt werden kann.

Ich habe die Vorbehalte von Herrn Stadler gehört. Ich kann sie auch ein Stück weit nachvollziehen, denn es ist wirklich so, dass auch etwas, was man mit besten Absichten tut, sich ins Gegenteil verkehren kann. Das kann auch bei diesem Thema der Fall sein. Die Frage ist nur: Was ist die Alternative? Wenn wir nicht davon ausgehen können, dass es nie Missbräuche geben wird – und wir haben ja gerade in der letzten Zeit einige Erfahrungen mit dem missbräuchlichen Umgang mit Daten sammeln können, die wir lieber nicht gemacht hätten, aber so ist es nun einmal –, wenn wir also Missbräuche nicht zu 100 Prozent ausschliessen können, dann, muss ich sagen, entscheide ich mich dafür, nicht einfach nichts zu tun, sondern diese Möglichkeit für die Verbrechensbekämpfung einzusetzen und gleichzeitig alle möglichen Schutzmassnahmen vorzukehren, um Missbräuche zu

verhindern. Aber Sie haben Recht, Herr Stadler, völlig ausschliessen können wir sie nicht.

Frau Fetz hat ebenfalls wichtige Fragen gestellt. Sie hat gefragt, ob das denn überhaupt wirke, ob diese ganze Überwachung der Telekommunikation etwas bringe, warum wir Ihnen nicht eine Statistik beigelegt hätten, die sagt: so viele Überwachungen, so viele Überführungen, so viele Verurteilungen. Ich kann Ihnen sagen, warum wir das nicht machen können: Die Telekommunikationsüberwachung ist nur ein Bestandteil der Strafverfolgung, und man kann eben nicht sagen, eine Überwachung führt auch zu einer Verurteilung. Die Überwachung dient der Identifizierung eines möglichen Täters. Das ist das, was wir mit der Überwachung machen können, aber den Beweis erbringen und eine Verurteilung erwirken, das können wir mit der Telekommunikationsüberwachung nicht. Deshalb können wir auch nicht sagen, jede Überwachung bringt automatisch eine Verurteilung mit sich. Wir können aber umgekehrt sagen: Ohne Überwachung haben wir in vielen Fällen gar keine Chance, den Täter überhaupt zu identifizieren. Dieser ein bisschen unangenehme Umkehrschluss gilt hier. Sie haben Recht, es ist nicht so, dass jede Überwachung zu einer Verurteilung führe, aber wenn wir keine Überwachung machen, weil nicht jede Überwachung eine Verurteilung bringt, dann machen wir am Schluss gar nichts mehr. Auch hier muss ich sagen: Im Abwägen dieser Fragen entscheide ich mich dafür, dass wir diese Massnahmen auch treffen können. Aber wir müssen es sorgfältig tun, und wir müssen für Rechtssicherheit sorgen, deshalb ist dieses Gesetz so wichtig.

Ich habe es Ihnen gesagt: Überwachungen werden heute schon durchgeführt. Wir wollen jetzt aber in den gesetzlichen Grundlagen festlegen, was gemacht werden darf und was nicht. Ich hoffe, dass ich mit diesen Ausführungen klar machen konnte, dass es in diesem Gesetz im Unterschied zum Nachrichtendienstgesetz, über das Sie in Bälde auch beraten werden, ausschliesslich um Überwachungsmassnahmen geht, die im Rahmen eines Strafverfahrens durchgeführt werden, die also der Aufklärung von Straftaten dienen und – ich sage es noch einmal – ausserdem von einem Zwangsmassnahmengericht bewilligt werden müssen. Das gilt für den Nachrichtendienst und das Nachrichtendienstgesetz nicht.

Nachdem ich diese Ausführungen gemacht habe, möchte ich etwas noch ganz präzise festhalten – einfach, damit Sie mir nicht sagen werden, ich hätte das nicht erwähnt –: Wir sehen in diesem Gesetz auch zwei Ausnahmen vor. Die erste Ausnahme besteht darin, dass Überwachungsmassnahmen angeordnet werden können, wenn in einem Notfall eine vermisste Person in Gefahr ist. Sie erinnern sich an den sehr, sehr tragischen Fall von Lucie Trezzini. Im Nachhinein konnten wir dort Überwachungsmassnahmen treffen. Ich denke, in einem solchen Ausnahmefall muss man eingreifen können, obwohl noch kein Strafverfahren läuft. Deshalb wollen wir hier diese Überwachungsmöglichkeiten vorsehen. Wenn in einem Notfall eine vermisste Person in Gefahr ist, soll diese Ausnahmemöglichkeit bestehen, weil wir damit unter Umständen Menschenleben retten können. Die zweite Ausnahme betrifft die Situation, dass man nach einer Person fahndet, die bereits zu einer Freiheitsstrafe verurteilt ist und sich auf der Flucht befindet. Auch da gibt es leider unruhliche Beispiele, und auch da geht es darum, allenfalls weitere Straftaten zu verhindern und Menschenleben zu retten. Das sind die beiden Ausnahmen, die wir Ihnen vorschlagen. Sonst gilt das, was ich vorhin gesagt habe.

Ich möchte Sie noch bitten, bei dieser Gesetzesberatung zwei Dinge auseinanderzuhalten:

Zum einen regeln wir im Büp, wer solche Überwachungsmassnahmen dulden muss. Ausserdem geht es darum, wie die Zusammenarbeit der verschiedenen Akteure geregelt sein muss, damit sie verbessert werden kann. Schliesslich soll im Büp auch festgehalten werden, wer welche Kosten dieser Überwachungsmassnahmen tragen soll – Herr Graber hat bereits etwas dazu gesagt. Wir kommen sicher in der Detailberatung noch ausführlich darauf zurück, im Moment äussere ich mich nur zum Eintreten.

Zum andern regeln wir in der Strafprozessordnung – das ist Bestandteil dieser Revision –, unter welchen Voraussetzungen welche Überwachungsmaßnahmen angeordnet werden können. Dabei geht es in erster Linie um den Einsatz der sogenannten Government Software, der Govware oder Staatstrojaner. Diese Massnahme ist natürlich ganz besonders umstritten. Aber die Tatsache, dass heute die Verschlüsselungstechnologien beim E-Mail- und beim Telefonverkehr die herkömmlichen Strafverfolgungsmöglichkeiten einfach ausschliessen, weil wir mit den herkömmlichen Verfolgungs- oder Überwachungsmöglichkeiten bei Skype und bei verschlüsselten E-Mails keinen Zugriff haben, können wir doch nicht einfach so hinnehmen! Wir würden sonst einfach sagen: Die verschlüsselte Telekommunikation gehört den Kriminellen. Das ist doch unvorstellbar! Ich denke, wir werden das in der Detailberatung noch anschauen. Wir haben hier natürlich festgehalten: Weil diese Überwachungsmaßnahmen oder diese Eingriffe besonders weit gehen, kann man sie wirklich nur dann einsetzen, wenn es um schwerste Straftaten geht. Wir haben hier die Anwendung also noch einmal eingeschränkt.

Frau Ständerätin Fetz hat die Botschaft zitiert und gesagt, der Bundesrat habe dargelegt, wie problematisch diese Massnahmen seien. Ja, es stimmt, sie sind problematisch. Aber wir haben auch einiges dafür getan, um das zugelassene Eindringen in die Privatsphäre in diesem Gesetz ganz genau zu umschreiben. Wir verbieten zum Beispiel explizit Online-Durchsuchungen. Wir sagen: Diese Staatstrojaner dürfen nur eingesetzt werden, wenn es um schwerste Straftaten geht, und sie dürfen nur subsidiär eingesetzt werden, also dann, wenn man alle anderen Möglichkeiten ausgeschöpft hat und nicht an die Informationen herangekommen ist. Dann darf man sagen: «Jetzt müssen wir Zugang zur verschlüsselten Telekommunikation haben.» Dann braucht es diese Staatstrojaner oder auch den Einsatz von IMSI-Catchern. Auch das wollen wir neu in der Strafprozessordnung regeln. Auch hier gilt: Diese Methode soll nur eingesetzt werden dürfen, wenn sich die klassischen Überwachungsmaßnahmen als unwirksam erwiesen haben.

Ich bitte Sie, im Einklang mit dem Antrag Ihrer Kommission für Rechtsfragen auf das Gesetz einzutreten und dafür zu sorgen, dass wir die neuen Technologien nicht den Kriminellen überlassen, gleichzeitig aber auch der individuellen Freiheit und dem Schutz der Privatsphäre weiterhin grosses Gewicht beimessen. Ich bin der Meinung, dass uns das mit dem vorliegenden Gesetzentwurf gelungen ist. Es freut mich, dass Ihre Kommission das auch so sieht.

*Eintreten wird ohne Gegenantrag beschlossen
L'entrée en matière est décidée sans opposition*

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

Detailberatung – Discussion par article

Titel und Ingress, Art. 1

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Titre et préambule, art. 1

Proposition de la commission

Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Art. 2

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Antrag Fetz

Bst. e

e. Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz im Rahmen einer wirtschaftlichen Tätigkeit Dritten zur Verfügung stellen;

Art. 2

Proposition de la commission

Adhérer au projet du Conseil fédéral

Proposition Fetz

Let. e

e. les personnes qui laissent leur accès à un réseau public de télécommunication à la disposition de tiers dans le cadre d'une activité économique;

Engler Stefan (CE, GR), für die Kommission: Ich werde mich nur dort äussern, wo gegenüber der heutigen Gesetzgebung Neuerungen beabsichtigt sind, und auch nur dort, wo ich diese als wesentlich erachte.

Frau Bundesrätin Sommaruga hat zum sachlichen Geltungsbereich bereits Ausführungen gemacht, wonach Überwachungen des Fernmeldeverkehrs nicht nur bei Strafuntersuchungen, sondern noch in zwei anderen Fällen denkbar sind, bei der Notsuche nach vermissten Menschen und bei der Fahndung nach verurteilten, flüchtigen Straftätern. In Artikel 2 geht es aber nicht um den sachlichen, sondern um den persönlichen Geltungsbereich des Gesetzes. Man kann, wenn man das geltende Gesetz und den Entwurf einander gegenüberstellt, relativ schnell herauslesen, dass die meisten mitwirkungspflichtigen Personen gemäss Artikel 2 bereits nach dem geltenden BÜpf zur Mitwirkung verpflichtet sind. Betroffen sind also insbesondere die Anbieter von Postdiensten, die Anbieter von Fernmeldediensten und die Betreiber von internen Fernmeldenetzen. Der persönliche Geltungsbereich wird mit dem neuen Gesetz auf zusätzliche Personenkreise erweitert, auf solche, die im Fernmeldeprozess intervenieren und Kommunikationsdaten besitzen können, die für die Strafverfolgungsbehörden von Interesse sind. Dabei handelt es sich um die Anbieter abgeleiteter Kommunikationsdienste. Wir werden bei den Anträgen Graber Konrad darauf zurückkommen.

Der Begriff der abgeleiteten Kommunikationsdienste bezeichnet verschiedene Arten von Internetanbietern wie reine E-Mail-Anbieter oder die Anbieter von Chat- und Dokumentenaustauschplattformen; diese sind unter dem Begriff «Cloud Services» bekannt. Der von diesem Gesetz betroffene Personenkreis bestimmt sich auch aufgrund der Zurverfügungstellung des Zugangs zu einem öffentlichen Fernmeldenetz. Das betrifft Institutionen, die Dritten einen Zugang zur Verfügung stellen, so Hotels, Cybercafés, Spitäler, Schulen und auch Private. Hier knüpft der Antrag Fetz an. Es geht um die Frage, ob auch private Personen dem persönlichen Geltungsbereich des Gesetzes unterstehen sollen, wenn sie solche Angebote nicht gewerblich anbieten. Der dritte zu erwähnende Personenkreis, der unter den Geltungsbereich fällt, sind die professionellen Wiederverkäufer von Karten und ähnlichen Mitteln, die den Zugang zu einem öffentlichen Fernmeldenetz ermöglichen und von Fernmeldediensteanbietern stammen.

Bevor Kollegin Fetz ihren Antrag begründen wird, bleibt noch festzuhalten, dass die Überwachungspflichtigen der verschiedenen Personen sehr unterschiedlich sind und dass je nach Kategorie auch die Mitwirkungspflichten unterschiedlich ausfallen. Grundsätzlich werden nur die Anbieter von Post- und Fernmeldediensten zu einem aktiven Verhalten verpflichtet werden können. Bei den übrigen werden sich die Pflichten vor allem darauf beschränken, dass sie Überwachungen und Datenlieferungen zu dulden haben.

So weit zum persönlichen Geltungsbereich. Wie bereits gesagt, gibt es hierzu noch einen Einzelantrag.

Fetz Anita (S, BS): Frau Bundesrätin, Sie haben vorhin rhetorisch gefragt, was denn die Alternative zu diesem Überwachungsgesetz sei. Ich glaube, in diesem Saal hat niemand

mit irgendeinem Wort gesagt, dass es kein Überwachungsgesetz brauche, sondern die Frage ist: Was sind die Grenzen dieser Überwachung, und was betrachtet man als verhältnismässig? Aus diesen Überlegungen resultiert mein Antrag. Ich möchte hier, dass Buchstabe e, «Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen», auf Personen beschränkt wird, die eine entsprechende wirtschaftliche Tätigkeit ausüben.

Ich nehme an, dass es darum geht. Es geht um die zunehmende Zahl von WLAN in Restaurants und Hotels oder auch in öffentlichen Gebäuden; dort geht es darum, dass jemand im Rahmen einer wirtschaftlichen Tätigkeit gezielt Dritten einen Internetzugang zur Verfügung stellt. Bei dieser Personengruppe, da bin ich vollkommen einverstanden, soll eine Unterstellung auch möglich sein. Aber es gibt auch den Fall, wo der Zugang persönlich Dritten zur Verfügung gestellt wird. In der Botschaft lese ich dann zur Erklärung dieses Artikels: «Unter diesen Buchstaben kann auch eine Privatperson fallen, deren Zugang Dritten absichtlich oder unabsichtlich offensteht.» So steht es auf Seite 2709 der Botschaft. Das heisst, wenn jemand unabsichtlich über mein WLAN einsteigt und ich davon keine Ahnung habe, darf ich auch überwacht werden.

Mir persönlich geht das zu weit. Ich finde, es sollte auf die wirtschaftliche Tätigkeit beschränkt sein. Dort sind ja auch – davon gehe ich einmal aus – die meisten Probleme, dort lohnt es sich, bezüglich einer Straftat zu überwachen.

Engler Stefan (CE, GR), für die Kommission: Die Kommission hat sich mit diesem Antrag nicht auseinandersetzen können. Allerdings hat die Kommission Kenntnis genommen von den Ausführungen in der Botschaft, in welcher ausdrücklich darauf hingewiesen wird, dass gerade auch private Personen unter bestimmten Voraussetzungen darunterfallen müssen. Man muss auch sehen, dass nicht damit zu rechnen ist, dass Privatpersonen dazu gezwungen werden könnten, ihre eigene und mitgenutzte Telekommunikation abhören zu lassen: Selbst in diesem Fall müsste nach dem Verhältnismässigkeitsprinzip entschieden werden und zuerst die Anordnung einer Staatsanwaltschaft und dann die Zustimmung durch ein Zwangsmassnahmengericht eingeholt werden.

Ich würde also dafür plädieren, diese Möglichkeiten der Strafermittlung offenzulassen. Für die rechtsanwendenden Behörden gilt, dass sie nur dann Überwachungsmassnahmen anordnen, wenn diese nötig, zweckmässig und verhältnismässig sind. Diese drei Voraussetzungen müssen immer erfüllt sein.

Bischof Pirmin (CE, SO): Ich bitte Sie, den Antrag Fetz abzulehnen. Der Antrag Fetz möchte den Geltungsbereich des Gesetzes auf Personen beschränken, die ihr Netz im Rahmen einer wirtschaftlichen Tätigkeit Dritten zur Verfügung stellen. Der Antrag würde also nicht nur eine Privatperson wie Sie oder mich ausschliessen, sondern auch alle grösseren Institutionen, die nicht gewerblich ihre Netze Dritten zur Verfügung stellen, das sind namentlich Schulen, Universitäten, Spitäler und andere. In diesen Bereichen scheint mir, wenn man den Sinn des Gesetzes bejaht, eine Überwachung notwendig zu sein. Sie müssen auch beachten, wenn Sie Artikel 29 lesen, der mit Artikel 2 verbunden ist, dass diese Personen nur eine Duldungspflicht übernehmen; d. h., es kann zwar bei diesen Schulen und Spitälern eine Überwachung vorgenommen werden, aber sie haben keine weiter gehenden Pflichten, wie sie Fernmeldeanbieter wie Swisscom oder Cablecom dann schon haben. Die Norm, wie sie Bundesrat und Kommission Ihnen vorschlagen, ist meines Erachtens genug eingeschränkt. Wenn Sie umgekehrt Artikel 2 im Sinne des Antrages Fetz annehmen würden, würde der Zweck der ganzen Überwachungsanlage aufgrund eines irrationalen Kriteriums, «wirtschaftliche Tätigkeit», eingeschränkt. Ich bitte Sie, den Antrag Fetz abzulehnen.

Sommaruga Simonetta, Bundesrätin: Frau Ständerätin Fetz beantragt bei Artikel 2 Buchstabe e, dass nur noch Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz «im Rahmen einer wirtschaftlichen Tätigkeit» Dritten zur Verfügung stellen, in den Anwendungsbereich des Gesetzes fallen, also zum Beispiel Restaurants, Hotels oder Spitäler. Sie beantragt weiter eine entsprechende Änderung von Artikel 29.

Dazu jetzt einfach Folgendes: Der Bundesrat schlägt vor, dass alle Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen, in den Anwendungsbereich des Gesetzes fallen. Wenn Sie den Antrag Fetz annähmen, müssten Privatpersonen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen – das könnten Sie alle sein, eben alle, die jemandem ihr Netz zur Verfügung stellen –, eine Überwachung durch den Dienst ÜPF gemäss Artikel 29 nicht mehr dulden. Sie müssten dem Dienst also keinen Zugang zu ihren Anlagen gewähren und ihm auch die zur Überwachung notwendigen Auskünfte nicht erteilen. Sie müssten auch die ihnen zur Verfügung stehenden Randdaten der überwachten Person nicht liefern.

Sie müssen sich vor Augen halten, dass eine Privatperson bei all diesen Pflichten, welche sie nach dem Entwurf des Bundesrates hätte, nicht die ganze Infrastruktur bereithalten oder etwas dafür tun müsste – es geht nicht um umfassende Überwachungspflichten. Sie müsste auch keine Randdaten speichern oder Echtzeitüberwachungen durchführen. Sie müsste einfach das liefern, was sie ohnehin hat – darum geht es. Das entspricht der Mitwirkungspflicht, die jeder Mann und jede Frau gemäss der Strafprozessordnung hat. Wenn Sie Unterlagen oder Gegenstände besitzen, die in einem Strafverfahren relevant sind, müssen Sie diese abliefern, dann müssen Sie diesen Beitrag leisten und können nicht sagen, das seien Ihre privaten Unterlagen. Wenn in der Strafverfolgung zum Beispiel solche Gegenstände oder Unterlagen von Relevanz sind, wenn sie dazu beitragen, Täter in einem Strafverfahren zu identifizieren, müssen Sie diese herausgeben; das ist die grundsätzliche Herausgabepflicht gemäss Artikel 265 der Strafprozessordnung. Warum soll man jetzt sagen, ausgerechnet hier gelte dieser Grundsatz nicht?

Sie haben bei Gegenständen und bei Unterlagen eine Herausgabepflicht und eine Mitwirkungspflicht; und hier hätten Sie diese nicht. Diese Einschränkung wäre also auch nicht mit der Strafprozessordnung vereinbar, es wäre nicht konsequent, man würde dort eine Lücke schaffen, ausgerechnet bei der Überwachung. Eine solche Einschränkung wäre am Schluss faktisch auch noch ein Anreiz für Kriminelle, die Fernmeldenetze von Privatpersonen zu nutzen. Das wollen wir nicht. Wir wollen, dass Privatpersonen, wie es in der Strafprozessordnung vorgesehen ist, ihren Beitrag leisten müssen bzw. eine Herausgabepflicht haben, aber – ich sage es noch einmal – nur für das, was sie ohnehin haben, was ohnehin vorhanden ist.

Von daher macht diese Ausnahme für Privatpersonen keinen Sinn. Ich bitte Sie deshalb, den Einzelantrag Fetz abzulehnen.

Fetz Anita (S, BS): Ich habe eine Frage: Heisst das, dass ich auch informiert werde? Bei Gegenständen werde ich ja informiert. Da heisst es: «Zeigen Sie mir bitte diesen Gegenstand, er ist für eine Strafverfolgung wichtig.» Wenn das der Fall ist, kann ich meinen Antrag zurückziehen, sonst nicht.

Sommaruga Simonetta, Bundesrätin: Ja, es sind genau die gleichen Regeln wie bei der Strafprozessordnung, Sie werden informiert.

Präsident (Germann Hannes, Präsident): Der Antrag Fetz ist zurückgezogen worden.

*Angenommen gemäss Antrag der Kommission
Adopté selon la proposition de la commission*

Art. 3–15*Antrag der Kommission*

Zustimmung zum Entwurf des Bundesrates

Proposition de la commission

Adhérer au projet du Conseil fédéral

*Angenommen – Adopté***Art. 16***Antrag der Kommission*

... beraten;

k. er führt eine Statistik über die Überwachungen.

*Antrag Fetz**Bst. k*

k. er führt eine Statistik über die Überwachungen. Der Bundesrat regelt die Einzelheiten.

Art. 16*Proposition de la commission*

... de collaborer;

k. il tient une statistique des surveillances.

*Proposition Fetz**Let. k*

k. il tient une statistique des surveillances. Le Conseil fédéral règle les modalités.

Fetz Anita (S, BS): Zuerst möchte ich der Kommission dafür danken, dass sie bei Buchstabe k die Statistik aufnimmt. Ich finde es ganz wichtig, dass das Gesetz das enthält. Ohne verlässliche Statistik kann man nicht beurteilen, ob das Gesetz richtig angewendet wird, und vor allem auch nicht, ob es wirksam ist. Deshalb möchte ich einen kleinen Zusatz: «Der Bundesrat regelt die Einzelheiten.» Ich möchte darauf hinweisen, dass ich mir in dieser Statistik zum Beispiel auch Aussagen wünsche über die Anzahl der nichtgenehmigten Überwachungen. Diese sollen auch erhoben werden. Ich möchte Aussagen über die Anzahl der nichtgenehmigten Verlängerungen der Überwachungen, über die Anzahl der Strafverfahren und Verurteilungen, die aufgrund der Überwachungen stattgefunden haben und nicht Zufallsfunde betreffen. Ich kann mir vorstellen, dass Sie das eh vorhaben. Aber mir geht es wirklich darum, hier auch sicherzustellen, dass nach Beendigung von Überwachungsmassnahmen den Betroffenen mitgeteilt wird, dass die Überwachung aufgehoben ist, vor allem dann, wenn sie nicht schuldig sind. Das sind Fragen, die wichtig sind für die Akzeptanz und für die Wirksamkeit dieses Gesetzes und auch für den Nachweis der Wirksamkeit.

Präsident (Germann Hannes, Präsident): Frau Fetz, Sie beantragen bei mehreren Artikeln die folgende Ergänzung: «Der Bundesrat regelt die Einzelheiten.» Ich nehme an, dass es sich um eine Art Systementscheid handelt. – Dem ist so.

Engler Stefan (CE, GR), für die Kommission: Vielleicht ein paar Ausführungen dazu, was die Gründe für die Kommission waren, den Katalog der Pflichten des Dienstes zu ergänzen: Als Folge der Anhörungen wurde das Pflichtenheft ergänzt. Demnach hat der Dienst über alle Überwachungen Buch zu führen. Diese Pflicht soll dazu dienen, genau so, wie es Frau Kollegin Fetz gesagt hat, sich ein Bild machen zu können, in welchem Ausmass und für welche Zwecke die Praxis von diesen Überwachungsmöglichkeiten Gebrauch macht. Gerade weil solche Überwachungen grundrechtsrelevant sind, muss es für uns als Gesetzgeber von Interesse sein, dass dieser Bereich einen höchstmöglichen Grad an Transparenz aufweist. Ich bin mit Ihnen einig, dass diese Statistik auch über die nichtbewilligten Gesuche Auskunft zu geben hat, auch über die erfolgten Mitteilungen an die Betroffenen, über die Beschwerden, die allenfalls erhoben worden sind, sowie die von Ihnen genannten Aspekte, die von Interesse sind.

Ihr Antrag, Frau Fetz, dass der Bundesrat die Einzelheiten in einer Verordnung zu regeln hat, ist nachvollziehbar und verständlich. Für das Überwachungsgesetz allerdings sehen die Übergangsbestimmungen in Artikel 43 eine Verordnungskompetenz des Bundesrates vor. Sie haben ja jetzt zuhanden der Materialien auch bekanntgemacht, was Sie von der Verordnung bezüglich Aussagen der Statistik erwarten. Für die übrigen Gesetze, die davon betroffen sind, die Strafprozessordnung und den Militärstraßprozess, macht Ihre Anregung, dass der Bundesrat in einer Verordnung die Einzelheiten und die Inhalte der Statistik festlegt, durchaus Sinn. Im Überwachungsgesetz könnte man nach meinem Dafürhalten darauf verzichten, weil die Verordnungskompetenz des Bundesrates bereits in den Schlussbestimmungen, in Artikel 43, definiert ist.

Sommaruga Simonetta, Bundesrätin: Ich kann mich den Ausführungen des Kommissionssprechers anschließen. Das Anliegen von Frau Fetz ist richtig und gut, wir unterstützen es. Es ist aber nicht nötig, diesen Zusatz in Artikel 16 Büpf anzubringen, weil es bereits mit Artikel 43 abgedeckt ist. In der Strafprozessordnung und beim Militärstraßprozess hingegen macht es auch aus unserer Sicht Sinn, diesen Zusatz zu machen. Wir danken Ihnen für diese Anregung und würden sie gerne unterstützen.

Fetz Anita (S, BS): Das ist für mich okay. Ich ziehe meinen Antrag zu Artikel 16 Buchstabe k also zurück. Die von mir beantragte Ergänzung in den anderen Artikeln halte ich aber aufrecht.

Präsident (Germann Hannes, Präsident): Der Antrag Fetz ist zurückgezogen worden.

*Angenommen gemäss Antrag der Kommission
Adopté selon la proposition de la commission*

Art. 17, 18*Antrag der Kommission*

Zustimmung zum Entwurf des Bundesrates

Proposition de la commission

Adhérer au projet du Conseil fédéral

*Angenommen – Adopté***Art. 19***Antrag der Mehrheit**Abs. 1–3, 5*

Zustimmung zum Entwurf des Bundesrates

Abs. 4

... während 6 Monaten aufbewahren.

Antrag der Minderheit

(Engler, Cramer, Levrat, Savary, Seydoux)

Abs. 4

Zustimmung zum Entwurf des Bundesrates

Art. 19*Proposition de la majorité**Al. 1–3, 5*

Adhérer au projet du Conseil fédéral

Al. 4

... durant 6 mois.

Proposition de la minorité

(Engler, Cramer, Levrat, Savary, Seydoux)

Al. 4

Adhérer au projet du Conseil fédéral

Engler Stefan (CE, GR), für die Kommission: Hier geht es um eine wichtige Bestimmung, nämlich um die Aufbewahrungspflicht für die sogenannten Randdaten, allerdings jene des Postverkehrs und nicht jene des Fernmeldeverkehrs. Bezüglich des Postverkehrs ist die quantitative Dimension der ganzen Problematik eine geringe. Ich würde vorschla-

gen, weil es um die grundsätzliche Frage geht, ob und wie lange Randdaten aufbewahrt werden sollen, dass wir in grundsätzlicher Hinsicht auch gerade Artikel 26 Absatz 5 mitbehandeln, denn die grundlegenden Fragen stellen sich sowohl bei den Randdaten des Postverkehrs wie auch bei den Randdaten des Fernmeldeverkehrs.

Es handelt sich um eine zentrale Bestimmung in dieser Vorlage. Sie wurde in der Eintretensdebatte auch von verschiedenen Kolleginnen und Kollegen angesprochen. Das Thema der Randdatenaufbewahrung, auch Vorratsdatenspeicherung genannt, ist aus verschiedenen Gründen grundrechtsrelevant, im gleichen Masse aber auch relevant für eine wirksame Strafverfolgung. Nicht ganz korrekt ist, wenn in diesem Zusammenhang davon gesprochen wird, es würden Daten flächendeckend auf Vorrat gesammelt. Korrekt ist: Die Daten sind bei den Fernmeldediensteanbietern gespeichert und werden erst im Einzelfall bei dringendem Tatverdacht – und auch dann nur, wenn der Verdacht auf eine schwere Tat im Raume steht – nach Anordnung durch die Staatsanwaltschaft und nach erfolgter Genehmigung durch das Zwangsmassnahmengericht an den Dienst übermittelt. Es ist also nicht etwa so, dass der Dienst Daten sammelt. Vielmehr ruft der Dienst im Einzelfall, wenn die Voraussetzungen, die ich genannt habe, erfüllt sind, bei den Fernmeldediensteanbietern und bei den Postdiensteanbietern die entsprechenden Daten ab.

Bei diesen Daten sprechen wir nicht von Echtzeitüberwachung. Es sind sogenannte Randdaten. Es ist in einem gewissen Sinne aber doch problematisch, dass diese, ohne dass ein Verdacht vorliegt, von wem auch immer aufbewahrt werden. Es handelt sich aber nicht um eine staatliche Kontrolle des Inhalts dieser Kommunikation, sondern um eine Registrierung des Kommunikationsvorgangs an sich. Solche Verbindungsranddaten verraten unter anderem, welcher Anschluss wann und wie lange mit welchem anderen Anschluss verbunden war und wo ein Mobiltelefon zu einem bestimmten Zeitpunkt benutzt wurde. Auf Ihrer Telefonrechnung finden Sie im Übrigen diese Angaben auch vor. Randdaten können heute sowohl beim Postverkehr wie auch beim Fernmeldeverkehr rückwirkend bis auf 6 Monate zurück verlangt werden. Deshalb müssen diese die Anbieter und nicht etwa der Dienst – wie schon unter dem geltenden Recht – vorrätig halten.

Zum Zugriff auf die Daten durch die Staatsanwaltschaft: Diese muss dem Richter nachweisen können, dass sie ein Strafverfahren gegen einen Beschuldigten wegen eines Verbrechens oder Vergehens führt und dass der Tatverdacht dringend ist. Spätestens mit Abschluss der Untersuchung muss sie dem Beschuldigten mitteilen, dass sie Daten erhoben hat. Dagegen kann der Betroffene nachträglich Beschwerde führen. Die Befürchtung gewisser Kreise, dass die Staatsanwaltschaften mit dem Zugriff auf die Vorratsdaten die Möglichkeit haben, den Fernmelde- oder Internetverkehr beliebiger Leute nachträglich dem Inhalte nach zu kontrollieren, ist hingegen unbegründet.

Es fragt sich, ob ein solches Speichern von Daten bei den Anbietern auf Vorrat zweckmässig, notwendig und verhältnismässig ist hinsichtlich der Unterstützung der Strafverfolgung. Diese Frage hat sich auch der Datenschutzbeauftragte gestellt. Zugegeben, in dieser Frage gehen die Meinungen auseinander. Europaweit wird das Thema kontrovers diskutiert, auch sind die Aufbewahrungsfristen für solche Randdaten des E-Mail- und Telefonverkehrs in den Nachbarländern unterschiedlich geregelt. Die EU-Richtlinie gibt als Dauer mindestens 6 und höchstens 24 Monate vor. So beträgt die Speicherdauer in Frankreich 12 Monate und in Italien, je nach Datentyp, zwischen 12 und 24 Monaten. Vor allem in Deutschland steht die Vorratsdatenspeicherung aber deutlich in der Kritik. Vor dem Gerichtshof der Europäischen Union ist ein Verfahren zur Grundrechtskonformität der EU-Vorratsdatenspeicherungs-Richtlinie hängig. Damit ist aber die Frage immer noch nicht beantwortet, ob die Aufbewahrung solcher Daten bei den Anbietern des Fernmeldeverkehrs zweckmässig, notwendig und verhältnismässig ist.

In der Tat, Frau Fetz, Sie haben Recht, es gibt in der Schweiz keine offiziellen quantitativen oder qualitativen Erhebungen über die Relevanz von Randdaten oder von deren Speicherung. Es ist in den meisten Fällen, die Bundesrätin hat es zutreffend gesagt, aber unmöglich zu sagen, die Randdaten seien eine *Conditio sine qua non* für eine Verurteilung und damit für einen Ermittlungserfolg verantwortlich gewesen. Allgemein kann jedoch gesagt werden, dass die Möglichkeit besteht, mittels Randdaten einen Anfangsverdacht zu erhärten oder zu entkräften, Hinweise auf weitere Verdächtige zu erhalten – Hinweise, die in der Folge eine Hausdurchsuchung oder eine Beschlagnahme legitimieren –, aber auch Beweise zu erhalten bei Straftaten, die über Internet verabredet bzw. dann auch begangen werden.

Das Ziel der Massnahme ist in der Regel – das sagt der Erste Staatsanwalt des Kantons St. Gallen, ein Spezialist dieser Materie, Herr Thomas Hansjakob –, Mittäter von Drogendealern zu identifizieren oder den Aufenthaltsort des Beschuldigten zum Zeitpunkt eines Tötungsdelikts, eines Raubs, eines Einbruchs oder einer Serie solcher Delikte zu ermitteln und die Kontaktpersonen zum heiklen Zeitpunkt zu identifizieren. Gerade in Drogenfällen gelingt es regelmässig, Lieferanten und Abnehmer des Beschuldigten zu ermitteln. In den anderen Fällen gelingt es häufig, die Anwesenheit des Beschuldigten am Tatort zu belegen oder, vor allem im Zusammenhang mit Tötungsdelikten, die Abwesenheit des Beschuldigten vom Tatort zu ermitteln und ihn deshalb auch zu entlasten.

Nach Auffassung der Strafverfolgungsbehörden ist deshalb das Mittel der Randdatenerhebung heute unverzichtbar, um solche Delikte aufklären zu können. Die Fälle, in denen eine Randdatenerhebung nicht beweisrelevant ist, seien relativ selten. Es kommt höchstens vor, dass ein bestimmtes Mobiltelefon nur kurz benützt wurde und die ausgelieferten Randdaten deshalb nicht den erhofften Zeitpunkt betreffen.

Nun noch etwas zur Verlängerung der Frist: Die Verlängerung der Frist von 6 auf 12 Monate ist einerseits vor allem deshalb erforderlich, um Verdächtige bei Tötungsdelikten, die längere Zeit nach der Tat ermittelt werden können, zu überprüfen. Nicht selten kann in solchen Fällen ein Verdächtiger nicht innerhalb von 6 Monaten nach der Tat ermittelt werden. Andererseits ist die Verlängerung der Frist dann erforderlich, wenn aus dem Ausland Hinweise auf Kinderpornografie eintreffen. Die Hinweise darauf, dass von einem bestimmten Internetanschluss aus Kinderpornografie heruntergeladen wurde, treffen häufig erst mit einer Verzögerung von mehreren Monaten in der Schweiz ein. Es könnte dann gar nicht mehr ermittelt werden, wer den fraglichen Anschluss benützte, wenn diese Daten nur für 6 Monate verfügbar wären.

Das sind die grundsätzlichen Überlegungen dazu, weshalb die Strafverfolgung auf Randdaten angewiesen ist und weshalb bei den Randdaten des Fernmeldeverkehrs eine Verlängerung der Aufbewahrungsfrist von 6 auf 12 Monate angezeigt ist.

Nun zu Artikel 19 Absatz 4: Da geht es um die Aufbewahrung der Randdaten des Postverkehrs. Die Aufbewahrungsdauer soll analog zu jener des Fernmeldeverkehrs einheitlich von bisher 6 auf neu 12 Monate erhöht werden. Ich habe es bereits gesagt: Im Vergleich zu den Randdaten des Fernmeldeverkehrs kommt diesen Randdaten eine deutlich geringere Bedeutung für die Strafverfolgung zu. Diese Randdaten beschränken sich ja im Wesentlichen auf Postsendungen mit Zustellnachweis, also auf eingeschriebene Sendungen. Im Unterschied zur Überwachung des Postverkehrs gibt das rückwirkende Auswerten der Randdaten Aufschluss darüber, mit wem Postsendungen ausgetauscht wurden. So gesehen stellt sich die Minderheit auf den Standpunkt, dass es zweckmässig, nötig und verhältnismässig ist, auch die Randdaten des Postverkehrs statt wie bisher während 6 Monaten neu 12 Monate lang aufzubewahren.

Damit habe ich in dieser Frage die Haltung der Minderheit vertreten.

Präsident (Germann Hannes, Präsident): Ich gratuliere Ihnen zum vollzogenen Hutwechsel in dieser Konstellation. *(Heiterkeit)*

Stadler Markus (GL, UR): Wegen des Hutwechsels sage ich hier, was ich eigentlich erst bei Artikel 26 zu sagen vorhatte. Zur Verlängerung der Aufbewahrungspflicht habe ich bereits beim Eintreten grundsätzliche Bedenken angemeldet. Es geht um verdachtsunabhängige Vorratsdatenspeicherung, also um die Speicherung von Daten von uns allen, wenn auch nur von Randdaten. Selbstverständlich kann man bereits aus diesen Randdaten, wenn sie systematisch bei den Anbietern aufbewahrt werden, einiges entnehmen, auch einiges über den Inhalt. Ich gehe davon aus, dass der Staat, wenn er in die Privatsphäre seiner Bürgerinnen und Bürger eindringen will, die Gründe darlegen und damit überzeugen muss. Er muss beweisen, weshalb es eine verlängerte Frist braucht, denn diese sollte nicht länger als unbedingt notwendig sein. Er sollte diesen Beweis vorlegen, auch wenn er schwierig ist. Eigentliche Beweise im Sinne der Wirksamkeit und der Verhältnismässigkeit habe ich aber in der Kommission nicht gesehen. Eine Verdoppelung der Aufbewahrungsfrist ist für mich deshalb zu lang.

Ich bitte Sie, hier der Mehrheit und bei Artikel 26, zu dem ich nicht mehr sprechen werde, der Minderheit zu folgen.

Savary Géraldine (S, VD): J'ai peu de choses à ajouter, puisque le président de la commission a présenté les arguments de la minorité dont la proposition est de revenir à la solution du Conseil fédéral. Si je prends l'exemple du canton de Vaud qui, comme d'autres, subit un certain nombre d'infractions et de délits criminels, en particulier des cyberattaques à raison de 200 à 300 par année. A chaque fois que ce type d'infraction a lieu, la procédure prend énormément de temps, cela a été dit, notamment parce qu'on doit avoir des commissions rogatoires auprès des pays comme les Etats-Unis, l'Allemagne, la France, etc. A chaque fois il faut faire des demandes qui prennent du temps. Il faut évidemment délimiter le périmètre de l'infraction. De ce point de vue, il est clair que 12 mois – cela a été dit par Monsieur Engler, rapporteur –, c'est une moyenne au niveau européen, d'après ce que constatent les praticiens. C'est le minimum pour pouvoir véritablement engager des poursuites sérieuses.

De ce point de vue là, je vous invite à soutenir la proposition défendue par la minorité. Cela permettrait véritablement d'identifier les auteurs des délits dans cet immense espace Internet.

Sommaruga Simonetta, Bundesrätin: Ich äussere mich zuerst zu beiden Artikeln, weil es hier ja um die Aufbewahrungsdauer für die Randdaten des Fernmeldeverkehrs, aber auch des Postverkehrs geht.

Herr Ständerat Stadler hat, glaube ich, schon zu Recht gefragt, warum gerade eine Verdoppelung von 6 auf 12 Monate vorgeschlagen wird. Das tönt in der Tat ein bisschen nach Willkür, denn man hätte auch eine Verdreifachung vorschlagen können, weil eine längere Aufbewahrungsdauer auch immer besser ist, oder man hätte sie bloss von 6 auf 8 Monate verlängern können.

Eine Verlängerung der Aufbewahrungsdauer für diese Randdaten ist aus Sicht des Bundesrates sinnvoll und nötig, weil es immer wieder Fälle gab, bei denen man gesehen hat, dass 6 Monate nicht genügen. Insofern ist Ihre Frage, weshalb wir keine Verdreifachung der Dauer vorsehen, berechtigt. Ich möchte Ihnen hier gerne aufzeigen, welche Überlegungen den Bundesrat dazu bewogen haben, die Dauer auf 12 Monate festzulegen. 12 Monate entsprechen den Forderungen von zwei Motionen, die Sie angenommen haben: Es ist einerseits die Motion Schweiger 06.3170 und andererseits die Motion Barthassat 10.4133. Beide Motionen sind vom Parlament angenommen worden, und beide Motionen halten

fest, dass die Randdaten des Fernmeldeverkehrs während 12 Monaten aufbewahrt werden müssen, damit die Strafverfolgungsbehörden ihre Arbeit korrekt erledigen können. Man hat also diese Überlegungen schon einmal gemacht. Es geht ja darum, dass die wichtigen Daten in einem konkreten Fall nicht verlorengehen.

Der Bundesrat ist im Übrigen bereits im Bericht vom 9. Juni 2006 in Erfüllung des Postulates der Sicherheitspolitischen Kommission des Ständerates 05.3006 vom Februar 2005 – es ist also schon eine Zeit lang her – zum Schluss gekommen, dass es eine Erhöhung dieser Aufbewahrungsdauer braucht. Man hat sich damals zwar noch nicht festgelegt, aber die Tatsache, dass es eine Verlängerung braucht, ist nicht brandneu, sondern wurde schon in jenen Jahren vom Bundesrat festgestellt.

Die vom Bundesrat vorgeschlagene Dauer von 12 Monaten stützt sich auch auf eine Richtlinie der Europäischen Union für die Randdaten des Fernmeldeverkehrs, die eine Aufbewahrungsdauer von mindestens 6 Monaten und im Prinzip bis zu höchstens zwei Jahren erlaubt. Viele Mitgliedstaaten der EU haben sich eben für eine Aufbewahrungsdauer von 12 Monaten entschieden, nämlich Dänemark, Spanien, Frankreich, die Niederlande und das Vereinigte Königreich. Wir haben also auch ein bisschen geschaut, was andere machen, und haben uns hier für einen Mittelweg entschieden, weil diese EU-Richtlinie sogar eine Aufbewahrungsdauer von bis zu zwei Jahren vorsieht.

Der Mehraufwand aufgrund der Verlängerung der Aufbewahrungsfrist für die Anbieter ist aus unserer Sicht nun wirklich vertretbar. Die Randdaten müssen ja wie gesagt bereits heute, gemäss geltendem Bupf, für 6 Monate aufbewahrt werden. Zudem muss man einen Teil dieser Daten sowieso während mindestens 12 Monaten aufbewahren, und zwar aus Gründen der Buchhaltung und der Rechnungsstellung. Ausserdem kann der Bundesrat bestimmte Anbieter von Fernmeldediensten von der Pflicht, die Randdaten aufzubewahren, befreien. Von dieser Pflicht können z. B. kleine Anbieter von Fernmeldediensten befreit werden, also namentlich jene, die Fernmeldedienste mit einer geringen wirtschaftlichen Bedeutung anbieten. Schliesslich wird der Bundesrat – wie heute – dafür zuständig sein, in der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs festzulegen, welche Randdaten für die verschiedenen Arten von Überwachung angemessenerweise aufbewahrt werden müssen. Sie sehen also, dass man durchaus noch Details präzisieren kann, um den unterschiedlichen Ausgangslagen gerecht zu werden.

Was die Aufbewahrungsfrist für den Postverkehr anbelangt, so hat der Kommissionssprecher bereits ausgeführt, dass wir der Meinung sind, es sollte für Postverkehr und Fernmeldedienste die gleiche Dauer sein, nämlich 12 Monate. Beim Postverkehr geht es um ein sehr kleines Volumen: Wir hatten dort 2012 nur gerade 13 rückwirkende Überwachungen. Es geht wirklich nur darum, für den Postverkehr die gleichen Voraussetzungen festzulegen. Wie der Kommissionssprecher gesagt hat, geht es hier um Postsendungen mit Zustellnachweis, natürlich nicht um den Briefversand insgesamt. Von daher macht es auch Sinn, die beiden Verkehrsmöglichkeiten gleich zu behandeln.

Ich bitte Sie, bei Artikel 19 die Kommissionsminderheit und bei Artikel 26 die Kommissionsmehrheit zu unterstützen.

Abstimmung – Vote

Für den Antrag der Mehrheit ... 19 Stimmen

Für den Antrag der Minderheit ... 19 Stimmen

(0 Enthaltungen)

Mit Stichentscheid des Präsidenten

wird der Antrag der Mehrheit angenommen

Avec la voix prépondérante du président

la proposition de la majorité est adoptée

Art. 20*Antrag der Kommission*

Zustimmung zum Entwurf des Bundesrates

Proposition de la commission

Adhérer au projet du Conseil fédéral

*Angenommen – Adopté***Art. 21***Antrag der Kommission**Abs. 1*

Zustimmung zum Entwurf des Bundesrates

Abs. 2

... und während der Dauer der Kundenbeziehung sowie während 12 Monaten nach deren Beendigung geliefert werden können.

Art. 21*Proposition de la commission**Al. 1*

Adhérer au projet du Conseil fédéral

Al. 2

... durant toute la durée de la relation commerciale ainsi que durant 12 mois après la fin de celle-ci.

Engler Stefan (CE, GR), für die Kommission: Es geht bei dieser Bestimmung, wie man das vielleicht meinen könnte, weder um den Inhalt einer Überwachung noch um Randdaten. Es geht einzig um Auskünfte über einen Anschluss, also darum, wer welchen Telefonanschluss hat. Die Daten, die damit gemeint sind, könnte man auch einem Telefonbuch entnehmen. Deshalb sind sie auch keinem besonderen Schutz unterstellt.

Der Entwurf des Bundesrates hatte den Fehler, dass die Informationen, um die es hier geht, mit der Beendigung des Vertragsverhältnisses gelöscht werden könnten. Wo aber laufend Abonnemente geändert werden, scheint es zweckmässig – um Lücken bei der Rückverfolgbarkeit zu verhindern –, die Frist für Auskünfte über die Kundenbeziehung auf 12 Monate zu befristen. Das dient auch der Kohärenz mit den Aufbewahrungsfristen für die soeben diskutierten Randdaten.

*Angenommen – Adopté***Art. 22***Antrag der Kommission*

Zustimmung zum Entwurf des Bundesrates

*Antrag Fetz**Abs. 2*

Der Bundesrat bestimmt, welche Angaben die Anbieter von Fernmeldedienststellen zum Zweck der Identifikation für einen Zeitraum von höchstens 5 Jahren bereithalten und liefern müssen. Sie müssen ...

*Antrag Graber Konrad**Abs. 4*

... Kommunikationsdienste, die Dienste von grosser Bedeutung für die Aufklärung strafbarer Handlungen oder Dienste von grosser wirtschaftlicher Bedeutung ...

Art. 22*Proposition de la commission*

Adhérer au projet du Conseil fédéral

*Proposition Fetz**Al. 2*

Le Conseil fédéral détermine les indications que les fournisseurs de services de télécommunication doivent, pour une période n'excédant pas 5 ans, posséder et livrer aux fins de l'identification. Ils doivent ...

*Proposition Graber Konrad**Al. 4*

... services de communication dérivés offrant des services d'une grande importance pour élucider des infractions ou des services d'une grande importance économique ...

Fetz Anita (S, BS): Mit diesem Antrag möchte ich die Frage nach der Maximaldauer der Aufbewahrung stellen. Ich habe nirgends Angaben dazu gefunden. Konkret geht es ja in Artikel 22 um das Abfragen von IP-Adressen. Da kann man bei Verdacht auf Straftaten über das Internet gewissermassen formlos die Informationen einholen. Laut Botschaft waren es im letzten Jahr 200 000 Abfragen. Das Problem, das ich sehe, ist folgendes: Wenn der Bundesrat bestimmen kann, dass diese Daten jederzeit verfügbar sein müssen, werden sie das natürlich auch sein, im Zweifelsfalle jahrzehntelang – Verjährungen treten gemäss StGB teilweise erst nach Jahrzehnten ein. Ich habe einfach einmal fünf Jahre vorgeschlagen und habe mich nach dem BWIS ausgerichtet. Dort müssen die Daten, die nachrichtendienstlich erfasst werden, nach fünf Jahren zwingend gelöscht werden. Eigentlich ist das auch eine lange Dauer, und letztendlich stelle ich hier die Frage nach der Maximalaufbewahrungsdauer.

Engler Stefan (CE, GR), für die Kommission: Ich kann nur meine Interpretation der Bedeutung von «jederzeit» wiedergeben. Eventuell muss dann die Frau Bundesrätin erklären, was sie bzw. was der Bundesrat damit gemeint hat.

Das jederzeitige Bereithalten betrifft ja nicht Daten, die dem Fernmeldegeheimnis unterstellt wären, sondern allgemein zugängliche Daten. Nach meiner Lesart kann «jederzeit» nur bedeuten: solange sie verfügbar sind bzw. solange ein Kundenverhältnis zwischen dem Anbieter und dem Kunden besteht. Das ist möglicherweise noch weniger lang, als Sie es jetzt mit fünf Jahren als Maximaldauer vorschlagen.

Ich bin gespannt zu erfahren, wie die Verwaltung bzw. der Bundesrat «jederzeit» interpretiert.

Sommaruga Simonetta, Bundesrätin: Der Bundesrat schlägt Ihnen hier vor, dass diese Daten, wie sie jetzt in Artikel 22 Absatz 2 definiert sind, jederzeit verfügbar sein müssen. Es handelt sich um Identifikationsdaten, also um Daten, wie sie auch im Telefonbuch stehen. Diese Daten sind keine sensiblen Fernmeldedaten. Deshalb meinen wir, dass es keinen Sinn macht zu sagen, diese Zurverfügungstellung müsse begrenzt werden. Es sind auch keine Daten, die dem Fernmeldegeheimnis unterliegen. Deshalb verstehen wir nicht, weshalb Sie die Dauer beschränken möchten. Die Daten nach Artikel 22 entsprechen zudem im Bereich Internet den Daten, die Gegenstand von Artikel 21 sind, das ist z. B. der Name des Inhabers eines Telefonanschlusses. Weil es eben nicht um sensible Fernmeldedaten geht, sollte man, so meinen wir, diese Daten dann nicht nur für höchstens fünf Jahre zur Verfügung stellen müssen, sondern vielmehr für die gesamte Dauer der Kundenbeziehung.

Vielleicht wäre es hilfreich und sinnvoll, wenn wir sagen, dass man für Artikel 22 Absatz 2 die gleiche Formulierung nimmt wie in Artikel 21 Absatz 2, wie das Ihre Kommission vorgeschlagen hat. Wir könnten uns vorstellen, dass wir dem Zweitrat einen entsprechenden Vorschlag unterbreiten. Dann hätten wir hier eine Präzisierung und eine Kohärenz, die jetzt unter Umständen nicht genügend gegeben ist.

Wenn Ihnen das helfen würde, schlagen wir vor, dass wir im Zweitrat eine entsprechende Formulierung einbringen. Aber generell zu sagen, dass Fernmeldedaten, die nicht sensibel sind und die Sie in jedem Telefonbuch finden, nicht zur Verfügung gestellt werden müssen, würde zu weit gehen.

Präsident (Germann Hannes, Präsident): Frau Fetz, sind Sie mit diesem Vorgehen einverstanden?

Fetz Anita (S, BS): Ich bin damit einverstanden. Ich habe mich einfach gewundert, dass man Daten, die sowieso jedem zur Verfügung stehen, in diesem Gesetz noch speziell benennen muss. Es ist für mich aber okay, wenn wir es so

machen wie vorgeschlagen und dies durch den Zweirat nochmals genau überprüfen lassen.

Präsident (Germann Hannes, Präsident): Der Antrag Fetz ist zurückgezogen worden.

Graber Konrad (CE, LU): Ich beziehe mich auf mein Votum in der Eintretensdebatte und halte mich sehr kurz. Es geht um eine Ergänzung, die vorsieht, dass man hier vor allem Dienstleistungen einbezieht, die von grosser Bedeutung für die Aufklärung von strafbaren Handlungen sind. Ich begründe meinen Antrag wie folgt: Anbieter abgeleiteter Kommunikationsdienste wie Datacenterbetreiber oder Hosting-Anbieter sollen nur mit den Fernmeldediensteanbietern gleichgesetzt werden, wenn ihre Dienstleistungen für die Aufklärung von strafbaren Handlungen generell eine grosse Bedeutung haben. Auf Seite 2736 der Botschaft schreibt der Bundesrat im zweitletzten Absatz: «Als Modell dienen dabei die Angaben, die von den Fernmeldediensteanbietern geliefert werden müssen.» Ich will mit meinem Antrag verhindern, dass namhafte Investitionen für Einrichtungen zur Überwachung getätigt werden müssen, die kaum oder nie zum Einsatz kämen oder bei der Aufklärung von strafbaren Handlungen nur eine untergeordnete Bedeutung hätten. Es geht mir letztlich also darum, dass man Fernmeldediensteanbieter und Anbieter abgeleiteter Kommunikationsdienste nicht über den gleichen Leisten schlägt, dass man eine Differenzierung vornimmt und unterscheidet, inwiefern die abgeleiteten Kommunikationsdienste effektiv einen Beitrag leisten können. Auf diese Weise möchte ich sicherstellen, dass keine unnötigen Investitionen getätigt werden.

Engler Stefan (CE, GR), für die Kommission: Kollege Graber spricht die Verhältnismässigkeit der Mitwirkungspflichten der Personenkreise an, die im Geltungsbereich dieser Gesetzgebung sind. Wenn Sie die Formulierung des Bundesrates lesen, sehen Sie, dass der Bundesrat die Mitwirkungspflichten im Einzelnen je nach Bedeutung, die diese Anbieter für die Strafverfolgung haben, differenzieren kann. Ich verstehe die Formulierung des Bundesrates so, dass er im Rahmen der Verordnung durchaus Abstufungen bezüglich der Mitwirkungspflichten der Beteiligten machen kann. Dass er die Relevanz für die Strafverfolgung als erstes Kriterium für diese Abstufung nimmt, ist dieser Bestimmung inhärent. Nach meinem Dafürhalten kann der Bundesrat das, was der Antrag Graber Konrad verlangt, in der Verordnung so regeln.

Sommaruga Simonetta, Bundesrätin: Ich möchte gerne noch etwas ausführen, was der Kommissionssprecher gesagt hat. Wir schlagen Ihnen vor, dass Anbieter von sogenannten abgeleiteten Kommunikationsdiensten verpflichtet werden können, alle oder einen Teil ihrer Angaben bereitzuhalten und zu liefern, Angaben, welche auch die klassischen Fernmeldediensteanbieter liefern müssen. Es geht hier also um reine E-Mail- oder Cloud-Service-Anbieter, die eben die gleichen Angaben bereithalten müssen wie zum Beispiel die Swisscom. Voraussetzung für eine solche Verpflichtung ist aber, dass diese Anbieter Dienstleistungen von grosser wirtschaftlicher Bedeutung oder Dienstleistungen für eine grosse Benutzerschaft anbieten.

Herr Ständerat Graber möchte jetzt noch ein weiteres Kriterium anfügen, wonach die angebotenen Dienstleistungen von grosser Bedeutung für die Aufklärung von strafbaren Handlungen sein müssen. Aus unserer Sicht ist das wirklich eine Selbstverständlichkeit. Wir müssen nämlich in der Verordnung, wie der Kommissionssprecher gesagt hat, definieren, was massgebend ist, damit eine Anbieterin abgeleiteter Kommunikationsdienste in eine Überwachungsinfrastruktur investieren muss; da gilt selbstverständlich das Verhältnismässigkeitsprinzip – das ist die Grundlage dieses Gesetzes für diese Massnahme. Die Bedeutung für die Strafverfolgung ergibt sich also bereits aus dem Zweck des Gesetzes und dem allgemeingültigen Verhältnismässigkeitsprinzip und muss deshalb nicht noch einmal erwähnt werden.

Das heisst, dass die von Herrn Ständerat Graber verlangte Ergänzung aus unserer Sicht wirklich unnötig ist. Ich muss aber auch einräumen, dass sie nicht schädlich wäre. Doch Sie alle mögen ja schlanke Gesetze, weshalb ich Ihnen in diesem Sinne beantragen möchte, diesen Einzelantrag abzulehnen.

Graber Konrad (CE, LU): Der Kommissionspräsident hat gesagt, der Bundesrat könne das in der Verordnung regeln; die Frau Bundesrätin hat gesagt, der Bundesrat werde das tun – so habe ich es verstanden. Dass das Verhältnismässigkeitsprinzip auch in diesem Fall gilt, scheint mir auch selbstverständlich. Ich kann mit diesen beiden Überlegungen meinen Antrag zurückziehen.

Präsident (Germann Hannes, Präsident): Der Antrag Graber Konrad ist zurückgezogen worden.

*Angenommen gemäss Antrag der Kommission
Adopté selon la proposition de la commission*

Art. 23–25

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Proposition de la commission

Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Art. 26

Antrag der Mehrheit

Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit

(Stadler Markus, Minder, Schmid Martin)

Abs. 5

... während 8 Monaten aufbewahren.

Antrag Graber Konrad

Abs. 6

... von Fernmeldediensten bezüglich Diensten von geringer Bedeutung für die Aufklärung strafbarer Handlungen oder Diensten von geringer wirtschaftlicher Bedeutung sowie Anbieter von Fernmeldediensten im Bildungsbereich von bestimmten gesetzlichen Pflichten befreien. Er befreit sie nicht ...

Art. 26

Proposition de la majorité

Adhérer au projet du Conseil fédéral

Proposition de la minorité

(Stadler Markus, Minder, Schmid Martin)

Al. 5

... durant 8 mois.

Proposition Graber Konrad

Al. 6

... ceux qui offrent des services de télécommunication de faible importance pour élucider des infractions, de faible importance économique ou dans le domaine de l'éducation. Il ne les dispense pas ...

Engler Stefan (CE, GR), für die Kommission: Wir haben in dieser Sache schon einlässlich diskutiert. Es geht um die Aufbewahrungsdauer für die Randdaten des Fernmeldeverkehrs. Wir haben die damit verknüpften Aspekte im Zusammenhang mit der Aufbewahrungsdauer für die Randdaten des Postverkehrs bereits behandelt. Beim Postverkehr, Sie erinnern sich, hat sich der Rat mit Stichentscheid des Präsidenten entschieden, es bei 6 Monaten Aufbewahrungsfrist zu belassen. In Zusammenhang mit den Fernmeldediensten stellt sich aber die Kommissionsmehrheit auf den Standpunkt, es sei zweckmässig, nötig und verhältnismässig, die

Aufbewahrungsdauer für die Randdaten von 6 Monaten auf 12 Monate zu erhöhen.

Präsident (Germann Hannes, Präsident): Der Antrag der Minderheit Stadler Markus ist bereits begründet worden.

Graber Konrad (CE, LU): Zu Absatz 6: Wenn die Frau Bundesrätin hier auch bestätigen kann – es handelt sich eigentlich um den gleichen Sachverhalt –, dass es vor allem um Dienste von geringer Bedeutung für die Aufklärung von strafbaren Handlungen geht, wäre ich der Auffassung, dass man die Investitionen nicht tätigen muss. Wenn das analog zu Artikel 22 Absatz 4 gehandhabt wird, könnte ich meinen Antrag zurückziehen, sonst würde ich ihn dann noch begründen.

Sommaruga Simonetta, Bundesrätin: Ich kann eigentlich bestätigen, dass dieser Absatz 6 eine gewisse Parallelität zu Artikel 22 Absatz 4 hat. Anbieter von geringer wirtschaftlicher Bedeutung sind rein statistisch gesehen für die Strafverfolgung selten von Interesse. Das Kriterium «Bedeutung für die Strafverfolgung» ergibt sich aus dem Zweck des Gesetzes und dem Verhältnismässigkeitsprinzip und muss auch hier nicht noch einmal eigens erwähnt werden. Es tritt jedoch in den Hintergrund, wenn es um den Schutz von kleinen Unternehmen geht. In diesem Sinne gibt es durchaus diese Parallelität.

Präsident (Germann Hannes, Präsident): Der Antrag Graber Konrad ist zurückgezogen worden.

Abstimmung – Vote

Für den Antrag der Mehrheit ... 22 Stimmen

Für den Antrag der Minderheit ... 14 Stimmen

(1 Enthaltung)

Art. 27

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Antrag Graber Konrad

Abs. 3

Der Bundesrat kann alle oder Teile der Anbieter abgeleiteter Kommunikationsdienste, die Dienste von grosser Bedeutung für die Aufklärung strafbarer Handlungen oder die Dienste von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten, allen oder einem Teil der in Artikel 26 genannten Pflichten unterstellen. Für die ...

Proposition Fetz

Abs. 3

Streichen

Art. 27

Proposition de la commission

Adhérer au projet du Conseil fédéral

Proposition Graber Konrad

Al. 3

Le Conseil fédéral peut soumettre l'ensemble ou une partie des fournisseurs de services de communication dérivés offrant des services d'une grande importance pour élucider des infractions ou des services d'une grande importance économique ...

Proposition Fetz

Al. 3

Biffer

Engler Stefan (CE, GR), für die Kommission: Es liegen zwei Anträge vor, nämlich der Antrag Fetz, Artikel 27 Absatz 3 zu streichen, und der Antrag Graber Konrad, Artikel 27 Absatz 3 zu ändern. Ich gehe aufgrund der vorhin zurückgezogenen Anträge allerdings davon aus, dass der Antrag Graber Konrad obsolet ist und somit nur noch der Antrag Fetz, Absatz 3 zu streichen, im Raum steht.

Dieser Antrag würde die Mitwirkungspflichten von Anbietern abgeleiteter Kommunikationsdienste einschränken und möglicherweise dazu führen, dass selbst der Ermittlungsstandard von heute nicht beibehalten werden könnte, wenn die zur Verfügung stehenden Randdaten des Fernmeldeverkehrs von den Anbietern abgeleiteter Kommunikationsdienste nicht abgerufen werden könnten. Ich sehe bei einer Streichung von Absatz 3 ein Problem, weil dadurch die Ermittlungsmöglichkeiten empfindlich eingeschränkt würden.

Präsident (Germann Hannes, Präsident): Herr Graber, nehmen Sie die Anregung des Kommissionspräsidenten auf?

Graber Konrad (CE, LU): Das vom Kommissionspräsidenten verwendete Wort «obsolet» gefällt mir natürlich nicht besonders. (*Heiterkeit*) Ich habe verstanden, dass mein Anliegen inhaltlich aufgenommen wird. Wenn das so ist, bin ich absolut einverstanden und ziehe auch diesen Antrag zurück.

Präsident (Germann Hannes, Präsident): Ich halte hier fest, dass die Meinung in Ihrem Sinne gedeutet wird, Herr Graber. Der Antrag Graber Konrad ist damit zurückgezogen.

Fetz Anita (S, BS): Absatz 3 von Artikel 27 ist für mich ein echter Innovationshemmer: Er wird sämtliche Start-ups im IT-Bereich behindern. Wie komme ich zu dieser Überlegung? Es geht ja hier um die Unterstellung bestimmter Anbieter abgeleiteter Kommunikationsdienste unter dieselben Mitwirkungspflichten, wie sie die ganz grossen Internetanbieter haben. Das heisst, dass dieser Absatz sehr weit reicht. Man muss dabei auch im Auge behalten, dass er allein und ausschliesslich schweizerische Anbieter treffen wird. Die wirklichen Big Shots in diesem Business haben bekanntlich alle ihren Hauptsitz im Ausland; sie alle werden nicht getroffen.

In der Kommission war dieser Artikel kein Thema – ich habe das in den Unterlagen überprüft. Vielleicht ist da auch nicht aufgefallen, welche Auswirkungen oder, besser gesagt, welche groben Nebenwirkungen er haben kann. Denn dieser Absatz erlaubt es dem Bundesrat, diesen Diensten exakt dieselben Mitwirkungspflichten wie den grossen Fernmeldediensteanbietern aufzuerlegen. Ich zähle jetzt nicht alle Artikel auf, die davon betroffen sind, sondern gehe vor allem auf etwas ein: Sie alle müssen den extrem teuren Nachweis der Auskunft- und Überwachungsbereitschaft nach den Artikeln 32 bis 34 erbringen, und zwar mit sämtlichen sehr teuren technischen Folgen, unter anderem auch mit der Kostenübernahmepflicht, und das alles unter Strafandrohung bis zu 100 000 Franken pro einzelne Verfügung! Das ist wie gesagt umso stossender, als es nur Schweizer Anbieter treffen kann. Das ist ein klassischer Wettbewerbsnachteil. Sie wissen, wer in diesem Bereich die grossen Player sind. Der Wettbewerb geht sehr stark zulasten der kleinen Anbieter. Darum nenne ich Absatz 3 auch einen Innovationskiller: Da wird nämlich eine Hintertür weit aufgesperrt für Massnahmen zulasten kleinerer Dienstleister, die auch mit den schweizerischen Giganten wie Swisscom, Sunrise und Orange auf die gleiche Stufe gesetzt werden.

Nehmen Sie einmal an, ein Instant Messenger wie beispielsweise das schweizerische Threema – das ist das schweizerische Whatsapp – hat ein paar Hunderttausend Benutzer. Pro App bezahlt man da nur einmal zwei Franken und keine Abonnementsgebühren. Die kommen auf einen Umsatz von vielleicht 200 000 bis 400 000 Franken im Jahr und müssen sich wie Sunrise, Swisscom usw. sämtlichen Vorgaben zu den technischen Ausstattungen unterwerfen. Ich finde das erstens unverhältnismässig, und zweitens wird in diesem Lande kein Start-up mehr leben können, weil damit derart hohe Kosten verbunden sind. Trotzdem kann das Unternehmen unter die Definition von Absatz 3 fallen, auch wenn es winzig ist, weil es eben einen abgeleiteten Kommunikationsdienst darstellt.

Ich bitte Sie sehr, hier die Verhältnismässigkeit zu wahren und die kleinen Anbieter nicht mit Kosten zuzudecken, die sie gar nicht stemmen können.

Sommaruga Simonetta, Bundesrätin: Ich muss das noch etwas präzisieren: Wenn Sie Absatz 3 anschauen, dann sehen Sie, dass es hier um die Anbieter abgeleiteter Kommunikationsdienste geht, die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten. Es geht also nicht um diese winzigen Start-ups, sondern um Anbieter, die grosse wirtschaftliche Bedeutung oder eine grosse Benutzerschaft haben. Wenn wir bei diesen Anbietern sagen, dass sie diese Randdaten z. B. nicht speichern müssen, dass sie von der Pflicht ausgenommen werden und dass sie auch keine Echtzeitüberwachungen durchführen müssen, dann nehmen wir hier wieder einen ganzen Teil heraus und schaffen eine Lücke in der Strafverfolgung, die man nicht begründen kann. Aber noch einmal: Es geht hier nicht gegen die Kleinen.

Es stimmt, was Frau Ständerätin Fetz sagt, dass viele grosse Internetdienste ihren Sitz und ihre Infrastruktur im Ausland haben. Es ist uns deshalb absolut bewusst, dass das nicht das Wundermittel ist, um z. B. Kinderpornografie im Internet zu bekämpfen. Es gibt kein Wundermittel. Es ist aber auch nicht nachvollziehbar, dass man Anbieter allein deshalb, weil sie abgeleitete Kommunikationsdienste anbieten, nicht gleich wie die klassischen Anbieter von Fernmeldediensten behandeln soll. Im Finanzsektor machen wir etwas Analoges längstens: Für die Unterstellung unter das Geldwäschereigesetz ist es unerheblich, ob es sich um eine klassische Bank oder um eine Spielbank handelt. Überall, wo Geldwäscherei vorkommen kann, unterstehen diese Unternehmen dem Geldwäschereigesetz.

Der technologische Fortschritt, die Telekommunikation und das Kommunikationsverhalten verändern sich dermassen stark, dass Kommunikation zunehmend über E-Mail, über Chat und über Apps stattfindet. Diese Dienste werden dann von einer Vielzahl von Unternehmen angeboten, die keine klassischen Fernmeldedienste erbringen. Wenn man sie hier einfach ausnimmt, indem sie nicht die gleichen Leistungen erbringen müssen, dann kann man das gar nicht begründen.

In diesem Sinne bitte ich Sie, hier den Einzelantrag Fetz nicht zu unterstützen. Aber auch hier gilt das Verhältnismässigkeitsprinzip. Gerade hier hat der Bundesrat ja explizit gesagt, dass es um Dienstleistungen geht, die eine grosse wirtschaftliche Bedeutung oder eine grosse Benutzerschaft haben. Es geht also nicht gegen die Kleinen, sondern es geht darum, dass diese abgeleiteten Dienste in grösserem Ausmass angeboten werden.

Abstimmung – Vote

Für den Antrag der Kommission ... 35 Stimmen

Für den Antrag Fetz ... 2 Stimmen

(3 Enthaltungen)

Art. 28

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Proposition de la commission

Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Art. 29

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Antrag Fetz

Abs. 1

Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz im Rahmen einer wirtschaftlichen Tätigkeit Dritten zur Verfügung stellen, müssen ...

Art. 29

Proposition de la commission

Adhérer au projet du Conseil fédéral

Proposition Fetz

Al. 1

Les personnes qui laissent leur accès à un réseau public de télécommunication à la disposition de tiers dans le cadre d'une activité économique tolèrent ...

Präsident (Germann Hannes, Präsident): Der Antrag Fetz ist im Rahmen der Behandlung von Artikel 2 zurückgezogen worden.

Angenommen gemäss Antrag der Kommission

Adopté selon la proposition de la commission

Art. 30–34

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Proposition de la commission

Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Art. 35

Antrag der Kommission

Abs. 1, 2, 4

Zustimmung zum Entwurf des Bundesrates

Abs. 3

... technische Geräte nach Artikel 269bis StPO ... würde. Sie führt eine Statistik über die Überwachungen nach Artikel 269bis StPO.

Art. 35

Proposition de la commission

Al. 1, 2, 4

Adhérer au projet du Conseil fédéral

Al. 3

... aux dispositifs techniques visés à l'article 269bis CPP ... difficile. Elle tient une statistique des surveillances visées à l'article 269bis CPP.

Engler Stefan (CE, GR), für die Kommission: Bei Artikel 35 Absatz 3 hat die Kommission eine kleine redaktionelle Anpassung vorgenommen, indem statt von «technischen Überwachungsgeräten» jetzt von «technischen Geräten» die Rede ist. Der neue Schlusssatz von Absatz 3 wurde bereits erklärt: Die Kommission wünscht, dass darüber eine Statistik erhoben wird.

Der Antrag Fetz erübrigt sich, weil wir immer noch im Bereich des Überwachungsgesetzes sind.

Angenommen – Adopté

Art. 36

Antrag der Kommission

Abs. 1, 3

Zustimmung zum Entwurf des Bundesrates

Abs. 2

Sie kann technische Geräte nach Artikel 269bis StPO und Informatikprogramme nach Artikel 269bis StPO einsetzen ... würde. Sie führt eine Statistik über die Überwachungen nach den Artikeln 269bis und 269ter StPO.

Art. 36

Proposition de la commission

Al. 1, 3

Adhérer au projet du Conseil fédéral

Al. 2

... aux dispositifs techniques visés à l'article 269bis CPP et aux programmes informatiques visés à l'article 269bis CPP lorsque ... difficile. Elle tient une statistique des surveillances visées aux articles 269bis et 269ter CPP.

Engler Stefan (CE, GR), für die Kommission: Bei Absatz 2 hat die Kommission eine Änderung vorgenommen. Es handelt sich um eine Ergänzung bezüglich der Fahndung nach verurteilten Personen analog der Notsuche nach vermissten

Personen. Zusätzlich zu den technischen Geräten wie dem IMSI-Catcher soll also subsidiär und nach Anordnung der Behörde und erfolgter Zustimmung durch das Zwangsmassnahmengericht dafür auch Govware eingesetzt werden können. Damit wird erreicht, dass mit diesen Massnahmen nicht nur nach Personen gefahndet werden kann, die im Ausland verurteilt wurden und auf der Flucht sind, sondern auch nach Personen, die im Inland verurteilt wurden und auf der Flucht sind.

Angenommen – Adopté

Art. 37

Antrag der Kommission

Abs. 1

... die Artikel 271, 272 und 274 bis 279 StPO sinngemäss.

Abs. 2, 3

Zustimmung zum Entwurf des Bundesrates

Art. 37

Proposition de la commission

Al. 1

... par les articles 271, 272 et 274 à 279 CPP.

Al. 2, 3

Adhérer au projet du Conseil fédéral

Engler Stefan (CE, GR), für die Kommission: Die Kommission hat Absatz 1 dahingehend ergänzt, dass die Bestimmungen zum Schutz des Berufsgeheimnisses und der Genehmigungspflicht durch das Zwangsmassnahmengericht – es geht um die Artikel 271 und 272 der Strafprozessordnung – auch für die Notsuche und für die Fahndung anwendbar sind.

Angenommen – Adopté

Art. 38

Antrag der Mehrheit

Abs. 1, 4

Zustimmung zum Entwurf des Bundesrates

Abs. 2

Streichen

Abs. 3

...

b. Streichen

Antrag der Minderheit

(Schmid Martin, Bischof, Engler, Häberli-Koller, Minder)

Abs. 2, 3 Bst. b

Zustimmung zum Entwurf des Bundesrates

Antrag Graber Konrad

Abs. 2

Die Mitwirkungspflichtigen erhalten vom Dienst eine Entschädigung, welche die Kosten der einzelnen Überwachung deckt.

Art. 38

Proposition de la majorité

Al. 1, 4

Adhérer au projet du Conseil fédéral

Al. 2

Biffer

Al. 3

...

b. Biffer

Proposition de la minorité

(Schmid Martin, Bischof, Engler, Häberli-Koller, Minder)

Al. 2, 3 let. b

Adhérer au projet du Conseil fédéral

Proposition Graber Konrad

Al. 2

Les personnes obligées de collaborer reçoivent du service une indemnité qui couvre les frais occasionnés pour chaque surveillance.

Engler Stefan (CE, GR), für die Kommission: Mit der Frage, wer für die Kosten der Überwachung aufzukommen hat – dieses Thema wurde in der Eintretensdebatte von verschiedener Seite angesprochen –, nämlich der Bund, die Kantone oder die Mitwirkungspflichtigen, haben wir einen der Casus Belli dieser Vorlage erreicht. Das kommt allein dadurch zum Ausdruck, dass zu dieser Frage drei unterschiedliche Vorstellungen bestehen und entsprechende Anträge vorliegen. Der Antrag der Kommissionsmehrheit, den Kollegin Savary anschliessend vertreten wird, will, dass die Kosten der Überwachung, und zwar sowohl diejenigen für die notwendigen Investitionen wie auch die variablen Kosten der Überwachung, die den Mitwirkungspflichtigen anfallen, von den Providern getragen werden sollen.

Der Einzelantrag Graber Konrad will etwas anderes: Wenn schon die Kosten der Investitionen von den Mitwirkungspflichtigen zu tragen sind, dann nicht auch noch die Kosten der Überwachung. Für diese sollen sie vielmehr kosten deckend entschädigt werden.

Zwischen diesen beiden Anträgen liegt jener des Bundesrates und der Minderheit, der an der heutigen Regelung, die eine Mittellösung darstellt, festhalten will. Die Anbieter kommen für die zur Überwachung benötigten Einrichtungen auf, erhalten aber eine angemessene Entschädigung für den mit der Überwachung verbundenen Aufwand.

Die Höhe der Entschädigung für die verschiedenen Überwachungsarten wie auch die Höhe der bei den Strafverfolgungsbehörden zu erhebenden Gebühren sind Gegenstand einer Verordnung. Dabei wird der Bundesrat einen Ausgleich der verschiedenen Interessen finden müssen. Gemeint sind das Interesse an einer wirkungsvollen Strafverfolgung, die finanzielle Belastung der Mitwirkungspflichtigen für Investitionen und Überwachung sowie der Kostendeckungsgrad beim Dienst des Bundes, der heute etwa 54 Prozent beträgt, was nichts anderes bedeutet, als dass sich der Bund schon heute zu einem wesentlichen Teil an den Kosten für die Strafverfolgung beteiligt.

Eine durch den Bund im Jahre 2012 bei der KPMG in Auftrag gegebene Studie – sie ist öffentlich – liefert Anhaltspunkte für die Höhe der Kosten bei den Anbietern im Zusammenhang mit der Überwachung. Für das Referenzjahr 2011 entstanden demnach dem Cluster der vier grossen Fernmeldediensteanbieter unter der bisherigen Gebührenverordnung jährliche Betriebskosten in der Höhe von 18,8 Millionen Franken. Den mittleren Fernmeldediensteanbietern entstanden ebenso wie den kleinen jeweils Kosten von rund 200 000 Franken. Die vorgenannten Zahlen zu den Betriebskosten werden unter anderem damit begründet, dass alle grossen Anbieter aufgrund der hohen Anzahl an Überwachungsfällen eigene Teams zur Durchführung von Überwachungen beschäftigen. Bei den mittleren und kleinen Anbietern wird die Überwachung überwiegend im Zug des Regelbetriebs durchgeführt, d. h. mit Mitarbeitern, die anteilig je nach anfallenden Aufträgen auch für die Überwachung tätig sind. Berücksichtigt man die dafür an die Fernmeldediensteanbieter bezahlten Entschädigungen, ergibt sich bei ihnen ein Deckungsgrad von ungefähr 50 Prozent bezüglich der variablen Kosten.

Der Antrag der Mehrheit wird von Kollegin Savary begründet. Der Antrag der Minderheit wurde von Kollege Schmid in seinem Eintrittsvotum begründet: Er hat erläutert, warum die Minderheit der Auffassung ist, es sei an der Mittellösung festzuhalten. Kollege Graber wird seinen Einzelantrag, wonach bei den Fernmeldediensteanbietern gar keine laufenden Kosten für die jeweiligen Überwachungen entstehen dürfen, ebenfalls noch begründen.

Savary Géraldine (S, VD): J'ajoute quelques mots sur la position de la majorité de la commission à l'article 38.

Tout d'abord, je rappelle que le Conseil fédéral a cherché un compromis sur la question des coûts, ce qui est à saluer. De plus, je reconnais aussi que la minorité de la commission a considéré que ce compromis était acceptable. Ce compromis consiste à considérer que les personnes obligées de collaborer, à savoir les opérateurs et les prestataires de services Internet, reçoivent une indemnité équitable – c'est le mot important par rapport à la proposition Graber Konrad – pour les frais occasionnés tant pour la surveillance téléphonique que pour le stockage des données secondaires.

Ce qui a incité la majorité à considérer que ce compromis était insatisfaisant, c'est que les représentants des opérateurs que nous avons reçus et écoutés n'ont pas donné de réponses satisfaisantes pour que l'on puisse considérer que cette indemnité équitable correspondait véritablement et à leurs besoins et à leurs investissements. La première question que nous nous sommes posée et à laquelle nous n'avons encore aujourd'hui toujours pas de réponse, c'est celle de savoir ce que coûtent réellement ces prestations fournies par les opérateurs. Nous avons posé les questions suivantes: combien de personnes faudra-t-il engager? Combien de temps cela prendra-t-il? Et les réponses à ces questions ne figurent pas dans le procès-verbal. Nous avons aussi demandé s'il y avait une comptabilité analytique, une comptabilité différenciée pour évaluer le coût des prestations. Nous n'avons pas obtenu de réponse. Le Bureau KPMG a été mandaté pour vérifier quel était le type de coûts et d'investissements que les opérateurs devraient consentir. Là aussi, nous savons que cela va augmenter mais pas dans quelle proportion. Ces réponses sont véritablement insuffisantes.

La deuxième question que nous nous sommes posée était la suivante: pourquoi chaque demande de fourniture de données secondaires adressée par les autorités de poursuite judiciaire coûte aujourd'hui environ 700 francs? Quelles prestations techniques faut-il fournir, avec quel type de personnel, avec quelle formation pour ce type de personnel? Evidemment, comparaison n'est pas raison, mais si on considère qu'en France cela coûte 40 euros, et qu'en Suisse le service est facturé 700 francs, j'aimerais qu'on m'explique pourquoi c'est aussi cher en Suisse, pourquoi dans d'autres pays, comme les Pays-Bas, il y a différents systèmes de forfait et pourquoi il est impossible d'en faire autant en Suisse.

La troisième question est plus fondamentale. Le débat porte sur les principes, par conséquent pourquoi certaines institutions, je pense en particulier aux banques, se soumettent gratuitement à des demandes de la part des autorités de poursuite quand il y a enquête, alors qu'on prévoirait des indemnités pour les opérateurs de téléphonie? En commission, il a été dit que cela pourrait créer un précédent. Les banques pourraient se demander pourquoi elles dépensent de l'argent pour répondre aux autorités et pourquoi les opérateurs touchent des indemnités. Cela pourrait faire tache d'huile.

Pour ce qui concerne Swisscom, je suis membre d'une formation politique qui défend cette société, qui défend la qualité des prestations et d'innovation de Swisscom. Je considère toutefois que la défense d'un opérateur public doit aller de pair avec un certain nombre de prestations, d'égards envers la collectivité. Nous avons réclamé des informations relatives à la protection de la jeunesse. Il a fallu des années pour que Swisscom prenne des mesures de protection de la jeunesse. Je trouve que c'est la même réflexion que nous devrions faire à l'égard de Swisscom concernant la criminalité. Il s'agirait de faire en sorte que les opérateurs de téléphonie, qui sont dans des situations financières malgré tout favorables, participent à la lutte contre la grande criminalité.

Ce que nous savons par contre – ce sont des chiffres qui sont consolidés –, c'est que la facture pour les cantons est très salée. Si je prends l'exemple du canton de Vaud, mais il y en a évidemment d'autres, celui-ci a dépensé 2 millions de francs par année pour 510 mesures actives et 1000 mesures portant sur les données secondaires. Le canton de Genève a dépensé 2,4 millions de francs en 2011 pour 692

surveillances téléphoniques. Le canton de Zurich a dépensé un peu près la même chose pour 654 mesures actives.

Vous avez toutes et tous reçu la position des cantons, qui rappelle à quel point la facture est élevée, et à quel point elle est opaque pour les autorités cantonales de poursuites judiciaires. Sur 700 francs payés pour les données secondaires, les opérateurs touchent 540 francs. Pour les écoutes directes, les opérateurs touchent 1330 francs sur 2410 francs. Donc je pense comme les cantons qu'il est important que la justice et la police travaillent à armes égales pour lutter contre la criminalité et je pense que les opérateurs et les prestataires de services Internet pourraient participer à cet effort.

Je vous invite à contribuer à ce que les mesures les plus efficaces soient prises et donc à avoir un débat franc et transparent sur cette question des coûts. Je rappelle que nous délibérons en tant que conseil prioritaire. Ce n'est pas impossible qu'ensuite il y ait d'autres propositions de compromis qui arrivent et je crois que nous devons pouvoir aussi adresser un message suffisamment clair auprès des acteurs de cette branche.

Schmid Martin (RL, GR): Ich teile die Auffassung des Kommissionspräsidenten, dass es sich bei diesem Artikel um einen wesentlichen Punkt dieser Revision handelt, der letztlich auch entscheidend sein wird für die Frage, ob dieses Gesetz einmal in Kraft gesetzt wird oder nicht. Wir haben verschiedene Varianten auf dem Tisch. Sie betreffen die Frage, ob die Fernmeldedienstleister in Zukunft eine volle Entschädigung erhalten sollen, wie das Kollege Graber beantragt, oder ob sie keine Entschädigung erhalten sollen, wie es die Mehrheit mit Kollegin Savary beantragt.

Ich bin der festen Überzeugung, dass es richtig ist, am geltenden Recht und an der geltenden Praxis festzuhalten. Das erste Argument ist ein staatspolitisches: Kann es sein, dass private Gesellschaften letztlich die Kosten der Strafverfolgung übernehmen müssen? Da habe ich eine klare Auffassung: Es kann nicht sein, dass im Ergebnis Privaten die Kosten übertragen werden für Tätigkeiten, welche hoheitlicher Natur sind. In diesem Falle müssten sie diejenigen Kosten der Strafverfolgung übernehmen, welche eigentlich die Kantone tragen müssten. Das wäre nämlich das Ergebnis, wenn Sie der Mehrheit folgen würden. Aus staatspolitischen Gründen bin ich der Auffassung, dass letztlich nicht die Handynutzer durch ihre Gebühren diese Kosten zu übernehmen haben. Ich bin nicht der Auffassung, dass es jemand anders sein sollte als die Kantone. Es sind entweder die Handynutzer oder die Steuerzahler, welche auch für die anderen Kosten der Strafverfolgung aufkommen müssen. Wie wir bei der Justiz und bei der Polizei nicht auf die Idee kommen, dass diese Aufgaben unbeteiligten Dritten übertragen werden können, muss man meines Erachtens auch hier zu diesem Ergebnis kommen.

Ein zweites Argument liegt auch in der Kooperation der Fernmeldedienstleister begründet. Wir wissen ja heute schon, dass ganz neue Entwicklungen auch im Bereich des Fernmeldewesens auf uns zukommen werden. Glauben Sie, dass diese Fernmeldedienstleister kooperieren, um entsprechende neue Technologien für die Strafverfolgungsbehörden aufzubauen, wenn sie keine Entschädigung erhalten, weder für die Einrichtung der Technologie noch für die Betriebskosten? Eine solche Regelung könnte sich ins Gegenteil wenden, sodass die Kooperationsbereitschaft der Fernmeldedienstleister gegen null geht und letztlich das Anliegen, die Strafverfolgung zu ermöglichen, sabotiert wird.

Ich frage Sie: Wie zwingen Sie als Gesetzgeber einen Fernmeldedienstleister, der in diesem Bereich nur Dienst nach Vorschrift macht, zur Kooperation? Sie können keine Beschlagnahmen vornehmen, und Sie können auch keinen Staatsanwalt in diese Abteilungen entsenden. Sie sind also letztlich darauf angewiesen, dass Ihnen die Gesellschaften auch in diesem Bereich ein Minimum an Kooperationsbereitschaft entgegenbringen.

Ich bin auch nicht der Meinung, dass der Vergleich mit dem Ausland gerechtfertigt ist. Wenn wir Deutschland nehmen,

mit 80 Millionen potenziellen Kunden, dann ist die Ausgangslage eine ganz andere. Das Gleiche gilt für Frankreich. Ich meine auch nicht, dass der Vergleich von Kollegin Savary richtig ist, die erwähnt, dass die Banken und Versicherungen entsprechende Dokumente vorlegen müssen. Es ist richtig, dass die Banken und Versicherungen das tun müssen, aber sie werden nicht verpflichtet, aktiv tätig zu werden. Fernmeldedienstleister müssen eben in Echtzeit Daten aktiv sammeln und den Strafverfolgungsbehörden zur Verfügung stellen. Es gibt also auch hier einen grossen qualitativen Unterschied.

Dass die Kantone, und ich möchte hier auf die KKKJPD verweisen, eine kostengünstige Lösung fordern, dafür habe ich ein gewisses Verständnis: Wenn man nur die Optik der Strafverfolgungsbehörden wählt, könnte man, aus diesem Blickwinkel und vielleicht noch mit Blick auf die Finanzsorgen der Kantone, zu diesem Ergebnis kommen. In einer Gesamtabwägung aber, in der auch die Interessen der Bürgersphäre gewahrt und die Interessen der Kantone sowie der Fernmeldedienstleister angeschaut werden sollen, komme ich zum Ergebnis, dass die Lösung, wie sie die Kommissionsminderheit und der Bundesrat vorschlagen, eine Konsenslösung, ein Kompromiss ist.

Ich bitte Sie, diesen Antrag der Kommissionsminderheit zu unterstützen. Ich bin folgender Überzeugung: Wenn wir jetzt gerade die Vorratsdatenspeicherung und die Möglichkeiten des Gesetzes gegenüber heute ausgeweitet haben, brauchen wir nun letztlich ein Korrektiv, damit diese Untersuchungsmassnahmen nicht inflationär angewendet werden, sondern nur in den Fällen, in denen Überwachungsmassnahmen auch wirklich angewendet werden sollten.

Graber Konrad (CE, LU): Ich halte mich relativ kurz, weil Herr Schmid meinen Antrag hervorragend begründet hat. All die Argumente, die er gebracht hat, sprechen eigentlich auch für meinen Antrag, nicht nur für den Minderheitsantrag, nur ist mein Antrag aus meiner Sicht vielleicht noch eine Nuance konsequenter.

Meine persönliche Überzeugung ist, dass es keinen sachlichen Grund dafür gibt, dass die Mitwirkungspflichtigen nur teilweise für ihren Aufwand für die Überwachung entschädigt werden sollen. Ich sehe keinen sachlichen Grund dafür. Normalerweise trägt derjenige, der den Auftrag gibt, die Kosten, sonst erteilt er keinen Auftrag, insbesondere, weil die Investitionskosten – das wurde jetzt eigentlich nicht berücksichtigt – gemäss Absatz 1 von den Mitwirkungspflichtigen getragen werden. Ich meine, die Investitionen sind praktisch so etwas wie das Grundangebot. Ich verstehe, dass die Fernmeldedienstleister hier eben ein Grundangebot leisten müssen, damit man diese Überprüfung überhaupt vornehmen kann. Diese Investitionen gehören zum Grundangebot und sollten deshalb auch von den Anbietern getragen werden. Bei den Leistungen selber, da ist es klar, ist es wie bei einem Auftrag: Wer den Auftrag erteilt, trägt die Kosten.

Frau Savary möchte ich sagen: Ich verstehe die Anbieter, wenn sie der Kommission ihre Betriebsbuchhaltungen nicht offenlegen. Aber die Kommission hat ja einen guten Weg gefunden. Sie hat die KPMG offensichtlich beauftragt, hier Klarheit zu schaffen. Es wurde Klarheit geschaffen, die Daten sind auf dem Tisch. Wie der Kommissionssprecher gesagt hat, sind die Ergebnisse klar.

Ich möchte nochmals betonen: Mir geht es darum, dass der Anbieter die Investitionen gemäss Absatz 1 trägt. Das ist für mich klar. Aber die variablen Kosten, dort, wo es um einen Auftrag geht, soll derjenige tragen, der den Auftrag erteilt hat. Wenn jemand einen Auftrag für eine Observation erteilt, dann ist ja auch klar, dass er die Kosten trägt. Wo ist der Unterschied? Ich sehe hier keinen Unterschied. Ich meine, es ist auch eine Frage der Transparenz und der Fairness, dass man hier Klarheit schafft und nicht irgendwie durch einen Kanal irgendwelche Aufträge separat finanzieren lässt. Herr Schmid hat es gesagt, letztlich tragen hier die Konsumentinnen und Konsumenten die Kosten. Wenn Sie hier festlegen, so, wie es die Mehrheit will, dass die Telekomanbieter diese Kosten vollständig tragen, dann wird das letztlich auf die

Handygebühren niederschlagen. Sie haben dann die Mitverantwortung dafür zu tragen, dass die Konsumentinnen und Konsumenten mit höheren Kosten konfrontiert sind.

Ich bitte Sie, meinen Antrag zu unterstützen.

Comte Raphaël (RL, NE): Les coûts dont nous parlons ici posent deux problèmes: d'une part ils sont excessifs, et d'autre part ils sont inexplicables.

Excessifs: vous avez lu la lettre de la CCDJP. Ce sont des coûts relativement élevés qui pèsent sur les budgets des cantons. Donc cela peut parfois freiner les autorités de poursuite lorsqu'elles veulent mener des investigations. Si les coûts étaient seulement excessifs, nous pourrions prendre acte de la situation, si encore nous pouvions expliquer le fait qu'ils soient si élevés. Il faut admettre que, lors des auditions, qui ont été longues et lors desquelles de nombreuses questions ont été posées aux opérateurs concernés, les réponses n'ont pas du tout été convaincantes. On nous a donné des réponses extrêmement vagues, peu claires, qui ne nous ont pas permis d'être persuadés que les propos qui nous étaient tenus reflétaient la réalité.

Ces coûts nous semblent d'autant plus inexplicables lorsque nous regardons au-delà des frontières et que nous voyons ce qui se pratique dans d'autres pays: les différences de prix sont encore plus criantes que pour le roaming! Nous pouvons bien admettre que la Suisse soit un îlot de cherté, mais il y a tout de même un certain nombre de limites à respecter. Ici, elles semblent clairement dépassées.

Le fait que ces coûts soient excessifs met en danger la poursuite pénale. Dans certains cantons, les crédits sont épuisés en août ou en septembre et il faut trouver des solutions dans l'urgence, parfois en renonçant à des mesures pour des raisons de coûts. Je ne crois pas que ce soit dans l'intérêt de la protection de la société. Si on apprenait qu'on a laissé courir des délinquants par manque de moyens, parce qu'on a renoncé à des mesures, nous pouvons tous imaginer le scandale que cela créerait! Cela crée aussi un sentiment de découragement au sein des autorités de poursuite judiciaire et des autorités de police.

Nous nous sommes trouvés en commission devant une situation assez simple: fallait-il croire plutôt les opérateurs de téléphonie ou les cantons? Nous nous sommes trouvés face à des affirmations contradictoires et, comme représentants des cantons, nous avons tout naturellement penché plutôt pour la parole des cantons.

Je vous invite en tout cas dans ce premier débat à donner un signal en faveur des cantons. Nous sommes le conseil prioritaire. Je reste persuadé qu'il y aura sans doute nécessité de trouver un compromis, que peut-être la solution de la majorité de la commission n'est pas encore la version définitive qui ressortira de nos travaux. Mais le Conseil national aura tout le loisir de reprendre ce point-là. Et peut-être que, cette fois-ci, les opérateurs concernés seront plus transparents et que cela permettra à la commission du Conseil national de corriger le projet dans le sens souhaité par les opérateurs.

Enfin, certains ont parlé de la responsabilité des autorités de poursuite de ne pas forcément prendre des mesures de manière trop large, certains ont dit qu'il fallait responsabiliser en mettant une partie des coûts à la charge des autorités. Je crois que nous pourrions évoquer ici la responsabilité des entreprises qui ont aussi à assumer un minimum de responsabilité sociale et n'ont pas que la responsabilité d'encaisser les prix de leurs abonnements.

Donc, au nom de la responsabilité sociale des entreprises et de l'intérêt de la poursuite pénale, je vous invite à soutenir la proposition de la majorité.

Sommaruga Simonetta, Bundesrätin: Ich habe am Anfang gesagt, dass in dieses Gesetz vieles hineingelesen wurde, und mein Eindruck war manchmal, dass ein Teil der Schaurmärchen, die man sich über dieses Gesetz erzählt hat, auch mit diesem Artikel zu tun hat. Ich erlaube mir diese Bemerkung.

Es liegen jetzt drei Anträge auf dem Tisch: Die Mehrheit Ihrer Kommission möchte, dass die Anbieter nicht mehr entschädigt werden für die Überwachungsdienste, die sie anbieten; die Minderheit möchte, wie auch der Bundesrat, dass die Anbieter eine «angemessene Entschädigung» erhalten; Herr Ständerat Graber möchte mit seinem Einzelantrag erreichen, dass die Anbieter voll entschädigt werden. Es gibt dieses Dreieck: Es gibt die Fernmeldediensteanbieter; es gibt die Strafverfolgungsbehörden, das sind insbesondere die Kantone; und es gibt den Dienst ÜPF, das ist die Bundeskasse. So viel einfach, damit klar ist, wer bezahlt. Die Kosten entstehen, die Frage ist nur: Wer bezahlt?

Ich möchte Ihnen nur ganz kurz ausführen, welches die Auswirkungen sind. Warum schlagen Ihnen der Bundesrat und die Kommissionsminderheit eine «angemessene Entschädigung» vor? Die Fernmeldediensteanbieter sollen die Infrastrukturen selber bezahlen müssen, und sie bekommen für jede einzelne Überwachung eine Entschädigung, die aber nicht die vollen Kosten deckt. Wir sind der folgenden Meinung:

1. Das war schon bisher so und hat sich eigentlich bewährt.
2. Ein Teil der Kosten muss tatsächlich von den Fernmeldediensteanbietern getragen werden: Sie sind in einem Bereich tätig, der mit Risiken verbunden ist, und sie müssen einen Teil dieser Risiken mittragen und abdecken.
3. Dass die Fernmeldediensteanbieter aber gar nicht mehr entschädigt werden, wie das die Kommissionsmehrheit will, ist aus unserer Sicht keine gute Lösung. Das Gleichgewicht – es ist ein sehr labiles Gleichgewicht – würde dann verlorengehen.

Wir haben auch keine Hinweise darauf – ich kann nicht bestätigen, was Herr Ständerat Comte gesagt hat –, dass einzelne Kantone die Überwachungen nicht mehr durchführen konnten, weil sie das nötige Budget nicht hatten. Wir sind der Meinung: Wer Aufträge erteilt, soll auch einen Beitrag leisten. Wir sind der Meinung, dass das nicht völlig kostenlos sein muss, dass es also gerechtfertigt ist, wenn die Strafverfolgungsbehörde einen Teil bezahlt. Wir sind der Meinung, dass auch die Bundeskasse über den Dienst ÜPF einen Teil dieser Überwachungsmaßnahmen finanzieren soll. Wir lehnen deshalb den Antrag der Kommissionsmehrheit ab.

Wir lehnen aber auch den Einzelantrag Graber Konrad ab. Stellen Sie sich vor, die Fernmeldediensteanbieter würden einfach für die vollen Kosten entschädigt. Das wäre unglaublich aufwendig. Sie müssten dann jedes Mal die vollen Kosten ermitteln. Die Anbieter hätten auch keinen Anreiz mehr, möglichst kostengünstig zu arbeiten. Sie könnten einfach die Rechnung schicken. Und wer würde die Rechnung bezahlen? Entweder die Kantone oder der Bund. Das geht so nicht. Ich denke, das ist wirklich keine Lösung. Wir sind wie gesagt der Meinung, dass die Fernmeldediensteanbieter auch einen Teil des Risikos mittragen müssen, dass hier eine vollständige Deckung der Kosten wirklich nicht gerechtfertigt ist.

Ich kann Ihnen sagen, wir haben lange geübt und deshalb auch diese Studie bei der KPMG verlangt. Wir haben vieles ausprobiert, vieles diskutiert, und wir sind zum Schluss gekommen, dass das, was wir heute im geltenden Recht haben, wahrscheinlich auch die mehrheitsfähigste Lösung ist, indem in diesem «Gleichgewicht des Schreckens» alle ihren Beitrag leisten müssen. Dabei ist klar, dass die Fernmeldediensteanbieter auch mitmachen müssen und dass sie eben einen Teil der Kosten selber tragen müssen.

Ich bitte Sie, bei diesem Gleichgewicht zu bleiben. Sie werden merken, dass sich, wenn dieses Gleichgewicht nicht mehr gewahrt ist, sehr schnell Kräfte formieren werden, die dieses Gesetz nicht wollen. Ich glaube, dass wir dann die schlechteste aller Lösungen haben.

Ich bitte Sie deshalb, die Kommissionsminderheit und den Bundesrat zu unterstützen.

Graber Konrad (CE, LU): Ich ziehe meinen Antrag zugunsten der Minderheit Schmid Martin zurück, wobei ich nochmals festhalten möchte, dass ich bei Absatz 1 nie gesagt

habe, dass alle Kosten der Justizbehörde übertragen werden. Absatz 1 wäre unverändert geblieben.

Abstimmung – Vote

Für den Antrag der Minderheit ... 27 Stimmen

Für den Antrag der Mehrheit ... 13 Stimmen

(1 Enthaltung)

Übrige Bestimmungen angenommen

Les autres dispositions sont adoptées

Die Beratung dieses Geschäftes wird unterbrochen

Le débat sur cet objet est interrompu

Schluss der Sitzung um 20.10 Uhr

La séance est levée à 20 h 10