13.025

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Änderung

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

Zweitrat – Deuxième 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)
Nationalrat/Conseil national 17.06.15 (Zweitrat – Deuxième Conseil)
Nationalrat/Conseil national 17.06.15 (Fortsetzung – Suite)

Antrag der Mehrheit
Eintreten

Antrag der Minderheit
(Vischer Daniel, Brand, Egloff, Reimann Lukas, Schwander, Stamm)
Nichteintreten

Antrag der Minderheit
(Vischer Daniel, Brand, Egloff, Kiener Nellen, Nidegger, Pardini, Reimann Lukas, Schwander, Stamm)
Rückweisung an den Bundesrat
mit dem Auftrag, eine Vorlage vorzulegen, welche keine Vorratsdatenspeicherung mehr kennt. Zudem sei beim Staatstrojaner und beim Imsi-Catcher der Deliktekatalog auf schwere Gewaltverbrechen zu beschränken. Es sei überdies sicherzustellen, dass die Daten einzig zu Zwecken der Strafverfolgung verwendet werden. Es sind schliesslich genügende Sicherheitsmassnahmen zu treffen, dass der Staatstrojaner auf zu überwachende Live-Kommunikation beschränkt bleibt.

Proposition de la majorité
Entrer en matière

Proposition de la minorité
(Vischer Daniel, Brand, Egloff, Reimann Lukas, Schwander, Stamm)
Ne pas entrer en matière

Proposition de la minorité
(Vischer Daniel, Brand, Egloff, Kiener Nellen, Nidegger, Pardini, Reimann Lukas, Schwander, Stamm)
Renvoyer le projet au Conseil fédéral
avec mandat de présenter au Parlement un projet qui ne prévoit plus la possibilité de conserver des données à titre préventif. En outre, il s'agira de limiter le recours à des chevaux de Troie et des IMSI-Catcher à la lutte contre les actes de violence criminelle uniquement ainsi que de garantir que les données récoltées soient utilisées exclusivement aux fins de la procédure pénale. Enfin, des mesures de protection suffisantes devront être prises afin de limiter le champ d'action des chevaux de Troie à la surveillance des communications directes.

Flach Beat (GL, AG), für die Kommission: Das geltende Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) stammt aus dem Jahr 1998 und wurde im Jahr 2000 in Kraft gesetzt. Partielle Änderungen erfuhr das Büpf insbesondere im Jahr 2007 mit der Einführung der bundesweit geltenden Strafprozessordnung. Das Büpf ist denn auch eine Ausführungsgesetzgebung zu den im Strafprozessrecht umschriebenen Überwachungsmassnahmen in Straffällen. Das Büpf gehört zum Verwaltungsrecht und regelt die Pflichten und Rechte der Personen, die mit Überwachungen beauftragt sind oder die gehalten sind, technische Hilfeleistungen für Überwachungen zur Verfügung zu stellen oder selber vorzunehmen.
Die Strafprozessordnung dagegen bestimmt, welche Überwachungsmassnahmen unter welchen Bedingungen zulässig sind. Die Strafprozessordnung sieht auch vor, dass eine Überwachung erst dann durchgeführt werden darf, wenn in einem Strafverfahren ein dringender Verdacht besteht, dass eine schwere Straftat begangen worden ist. Eine präventive Überwachung ist also ausgeschlossen und höchstens ein Thema des Nachrichtendienstgesetzes, das wir ja schon behandelt haben und das bald wieder zu uns zurückkommt, sie ist aber nicht Thema des Büpf. Ausserdem muss die Überwachung immer von einem Zwangsmassnahmengericht genehmigt werden.
Wir sind Zweitrat. Der Ständerat hat dem Geschäft am 19. März 2014 mit 30 zu 2 Stimmen bei 4 Enthaltungen zugestimmt. Ihre Kommission hat diese Vorlage während sieben Sitzungen intensiv und kontrovers beraten. Sie hat mehrfach Anhörungen durchgeführt, den für die Überwachung in diesem Bereich zuständigen Dienst besucht, vertiefte Abklärungen bei der Verwaltung veranlasst und im Rahmen der Detailberatung über rund 60 Anträge entschieden. Im Moment haben wir trotzdem noch 43 Minderheitsanträge auf der Fahne. Die Kommission folgte im Wesentlichen dem Ständerat, wich jedoch punktuell von ihm ab und konkretisierte die Vorlage an verschiedenen Stellen – wir werden in der Detailberatung darauf zurückkommen.
Die wichtigsten Punkte möchte ich in einer kurzen Übersicht vorweg etwas ausleuchten, da es ja ums Eintreten geht und es vielleicht hilfreich ist, wenn Ihnen die Eckpunkte, die die Kommission beraten hat, bekannt sind. Die Kommission ist mit 16 zu 6 Stimmen bei 3 Enthaltungen eingetreten und hat am Schluss für die Annahme des Entwurfes gestimmt.
Das Gesetz regelt die Überwachung des Post- und Fernmeldeverkehrs im Rahmen eines Strafverfahrens zum Vollzug eines Rechtshilfeersuchens, im Rahmen der Suche nach vermissten Personen oder im Rahmen der Fahndung nach Personen, die zu einer Freiheitsstrafe verurteilt wurden oder gegen die eine freiheitsentziehende Massnahme angeordnet, veranlasst und durchgeführt wurde.
Das Gesetz legt Mitwirkungspflichten und Duldungspflichten fest und regelt die Aufbewahrung von sogenannten Randdaten durch die Fernmeldedienstanbieter. Die Fernmeldedienstanbieter müssen weiterhin eine Infrastruktur zur Überwachung auf eigene Kosten aufbauen und betreiben. Die Entschädigung der einzelnen Leistungen erfolgt nach den Bestimmungen der entsprechenden Verordnung.
Kleine Fernmeldedienstanbieter müssen diese Infrastruktur nicht stellen. Kleine Fernmeldedienstanbieter müssen allerdings unter Umständen zulassen, dass sie ihre Infrastruktur für Überwachungszwecke zur Verfügung stellen müssen. Kleinere Anbieter, die eine geringere Kundenzahl bedienen, sind nicht Unternehmen, die grosse kommerzielle Zwecke verfolgen, oder Dienstleister, die Fernmeldedienste lediglich als Service zur Verfügung stellen. Das können Hotels sein, Restaurants, aber auch Internetcafés. Bei all diesen kleinen Dienstleistern ist eine wesentliche Voraussetzung die Pflicht zur Duldung von Überwachungsmassnahmen. Diese Massnahmen müssen aber immer verhältnismässig sein, und nach wie vor muss ein Zwangsmassnahmengericht den Eingriff in die Infrastruktur eines Dienstanbieters ausdrücklich bewilligen.
Der Hauptgrund für die Revision ist der Umstand, dass sich die Technologie der Kommunikationswege und Kommunikationsmittel seit der Entstehung des geltenden Büpf rasant verändert hat. Neben herkömmlicher Telefonie mittels Kabel auf analoger Basis ist die digitale Kommunikation auch in Verbrecherkreisen angekommen. Die Ermittlungsbehörden sehen sich vor das Problem gestellt, dass viele dieser neuen Kanäle, welche die digitale Revolution mit sich bringt, von

den Strafverfolgungsbehörden nicht mehr überwacht werden können, wenn sie für kriminelle Aktivitäten verwendet werden. Wenn sich zwei Straftäter also via Internetchat oder Internettelefonie zu einem Verbrechen verabreden, bleiben die Polizei, der Staatsanwalt, unsere Staatsmacht, aussen vor, weil das geltende Gesetz keine Mittel zulässt, um diese Kommunikation abzuhören. Dabei ist klar, dass es nicht um Bagatellfälle geht, sondern um schwere Straftaten, wie Gewaltverbrechen, Drogenhandel, Pädophilie, Menschenhandel, Terrorismus oder besonders schwere Fälle von Diebstahl durch Einzelpersonen oder auch durch kriminelle Vereinigungen.
Das Hauptziel des Entwurfs besteht also darin, die Möglichkeiten zur Überwachung des Fernmeldeverkehrs an die grossen technischen Entwicklungen der letzten Jahre anzupassen. Das Büpf schafft den Rahmen für die Umsetzung von Überwachungsmassnahmen, die in der Strafprozessordnung vorgesehen sind.

Schwaab Jean Christophe (S, VD), pour la commission: Les télécommunications ont évolué. Les criminels s'en sont aperçus et font usage des nouveaux moyens de communication. Ils utilisent des logiciels ou des applications cryptées. Ils planifient leurs mauvais coups par consoles de jeu interconnectées. Et lorsqu'ils se savent écoutés, la dernière chose qu'entendront les forces de l'ordre, c'est «finissons cette conversations sur Skype, sur Facebook Messenger ou sur World of Warcraft», ou encore sur un autre service crypté.
Parfois, ils n'ont même pas besoin de changer d'appareil. Avec ce simple téléphone intelligent, que nous sommes bon nombre à posséder dans cette salle, il n'y a qu'à changer d'application, à appuyer sur le logo bleu doté d'un «S» ou sur le logo bleu arborant un «F» au lieu du logo vert orné d'un combiné téléphonique pour passer d'un mode que les autorités de poursuite pénale peuvent écouter à un autre qu'il est actuellement impossible de surveiller, à part peut-être la NSA, mais je m'écarte du sujet.
Il n'est d'ailleurs pas certain que je m'en écarte autant que cela, car l'exemple de ce que peut – enfin, pouvait et pourra certainement bientôt de nouveau – faire la NSA est révélateur de la mauvaise compréhension qu'ont certains de la loi sur la surveillance de la correspondance par poste et télécommunication révisée et de ses instruments. Jusqu'à il y a peu, en effet, la NSA récupérait les données secondaires de télécommunications de la totalité de la population des Etats-Unis, sans aucun contrôle, si ce n'est celui d'un pseudo-tribunal secret. Comme nous le verrons plus tard, la différence entre le droit en vigueur et la loi révisée est de taille: ni la loi actuelle, ni la future loi sur la surveillance de la correspondance par poste et télécommunication n'autorisent une autorité étatique à stocker des données secondaires de l'entier de la population. Personne d'ailleurs ne peut conserver, encore moins utiliser à des fins de surveillance, les données de toute la population. Lorsque l'Etat peut les obtenir, ce n'est pas à des fins de surveillance préventive de n'importe qui, mais c'est pour mener une surveillance d'une personne soupçonnée d'un délit important, sous le contrôle d'un tribunal.
J'en reviens aux objectifs de la loi qui nous est soumise aujourd'hui. Un des objectifs de la révision que nous traitons aujourd'hui est de donner aux autorités de poursuite pénale les moyens d'écouter ces télécommunications actuellement inaudibles et de pouvoir pour cela faire usage des instruments adéquats. Ces instruments font peur. Peut-être est-ce à cause de leurs noms barbares: IMSI-Catcher, Govware, chevaux de Troie, «Vorratsdatenspeicherung». Mais c'est surtout à cause des craintes légitimes qu'ils provoquent dans la population, craintes renforcées par les récentes affaires d'espionnage et de surveillance massive des télécommunications par des services secrets étrangers.
Il y a aussi des craintes – légitimes là aussi – que ces instruments perturbent les télécommunications, en particulier les services d'urgence, voire permettent de mener de véritables perquisitions en ligne, de falsifier des contenus et donc des preuves. Le danger est en effet réel que ces instruments soient utilisés à tort et à travers pour surveiller les communications d'honnêtes citoyens, ou de personnes vaguement soupçonnées d'avoir commis un délit mineur.
La commission s'est donc penchée avec beaucoup d'attention sur ce problème. Le projet du Conseil fédéral contenait déjà des garanties solides. La commission les a renforcées, pour ne pas dire bétonnées, en particulier en ce qui concerne les «programmes informatiques spéciaux», nom juridique des chevaux de Troie ou Govware.
Comme nous le verrons lors de la discussion par article, le cadre légal que vous propose la commission, qui a passé beaucoup de temps sur ce point en particulier, est extrêmement étroit et toujours guidé par les principes élémentaires suivant:
– la subsidiarité: l'instrument n'est utilisé que lorsque d'autres, moins invasifs, ont échoué;
– la proportionnalité: on ne s'en sert pas pour traquer la petite criminalité;
– l'autorisation par un juge: la police ne peut mettre en oeuvre une surveillance invasive de sa seule initiative;
– l'inexploitabilité des preuves obtenues en dehors du cadre légal: si l'instrument de surveillance sert à autre chose qu'à surveiller la communication autorisée, les règles habituelles de la procédure pénale en matière d'exploitation des preuves s'appliquent;
– l'établissement d'un procès-verbal et le contrôle de chaque étape de la surveillance, afin de pouvoir garantir le respect des principes précédemment énumérés.
La mise en oeuvre de ces principes est un point important de la révision, car il faut bien admettre que les moyens de surveillance proposés constituent une atteinte grave aux droits fondamentaux. Il est donc capital que cette atteinte se fasse dans le strict respect des conditions de l'article 36 de la Constitution fédérale. La commission y a veillé, et la majorité est convaincue qu'elle y est parvenue. Le Conseil fédéral avait placé la barre très haut en matière de respect des droits fondamentaux, la commission l'a mise encore plus haut.
Il y a d'autres points où la révision de la loi vise à adapter les instruments de poursuite pénale à l'évolution des technologies. Il doit être désormais possible d'identifier les utilisateurs de télécommunications qui se servent de moyens aussi banals que des cartes SIM à prépaiement ou des réseaux sans fil mis à la disposition du public. Il va sans dire que cette obligation d'identification doit respecter le principe de la proportionnalité et qu'il n'est pas question d'accabler les particuliers ou les petites entreprises avec les charges qu'entraîne la mise sur pied de la surveillance. Ceux qui sont trop petits pour fournir les données eux-mêmes seront uniquement obligés de tolérer la surveillance qui sera effectuée par les autorités. Cette obligation de collaborer est précisée et échelonnée en fonction de qui est obligé de collaborer et sous quelles conditions.
Mais il ne s'agit pas seulement de surveiller ceux qui commettent des crimes graves dans le monde réel. Il s'agit aussi de combattre la criminalité en ligne: pédophilie, sextorsion, hameçonnage, etc. Là aussi, les criminels savent faire usage des moyens qui échappent à nos autorités par manque de bases légales. Combattre ces délits exige souvent des procédures longues, car ils ont souvent des ramifications internationales. Le projet en tient compte, notamment au niveau de la durée de conservation des données secondaires.
La nouvelle loi précise également l'utilisation des nouvelles technologies en cas de recherche d'une personne disparue en dehors d'une procédure pénale. Il ne s'agit cependant pas de supprimer le droit de tout un chacun à «disparaître des écrans radars» sans donner de nouvelles, si bon lui semble. Il s'agit plutôt de pouvoir tout mettre en oeuvre, y compris une surveillance des télécommunications, pour retrouver une personne disparue dont il y a lieu de croire qu'elle court ou qu'elle fait courir un danger sérieux. La nouvelle loi permet par ailleurs de rechercher une personne qui

doit effectuer une peine privative de liberté, mais qui a plutôt choisi de prendre la clé des champs.
Le projet de loi repose sur le principe de la neutralité technologique. Ses dispositions doivent s'appliquer quelle que soit la technologie appliquée. Nous sommes en effet à des lieues d'imaginer ou de pouvoir prédire l'évolution des technologies que les prochaines années, que dis-je, les prochains mois pourraient apporter. La télécommunication évolue en effet avec une célérité incroyable.
Moins de vingt ans après la fin du monopole public sur le téléphone, les acteurs qui sont aujourd'hui dominants – et leurs technologies – pourraient être remplacés demain par d'autres acteurs dont l'objectif premier n'est pas d'être un opérateur de télécommunication. Pensez à Facebook par exemple, à la base un réseau social, qui, outre le rachat de Whatsapp, développe désormais son propre instrument de communication instantanée.
Evoquer le géant de Palo Alto me permet d'évoquer l'obligation de collaborer des entreprises étrangères. Bon nombre des opérateurs actuels et futurs ne sont en effet pas suisses et n'y ont ni siège, ni succursale. Comment donc leur faire appliquer les règles que nous vous proposons d'adopter aujourd'hui? Comment éviter l'écueil de la territorialité du droit? Ce n'est pas facile. Je vous donne un exemple. Facebook, encore elle, clame partout qu'elle collabore avec les autorités de poursuite pénale de tous les pays. Mais voyons comment cela se passe en pratique. En pratique, Facebook collabore, mais exige pour cela une décision de justice; décision qu'il est souvent impossible d'obtenir si les conditions de l'entraide pénale internationale ne sont pas remplies. Le Tribunal fédéral vient de le rappeler. Dans ces conditions, si elles ne peuvent pas toujours compter sur la collaboration de ces nouveaux acteurs, nos autorités de poursuite pénale doivent pouvoir tout mettre en oeuvre, notamment les instruments qui permettent d'écouter des conversations en cas de soupçons de crimes graves, dans le respect des droits fondamentaux. C'est ce que permet la nouvelle loi. Et c'est aussi ce que contrôle la nouvelle loi.
La commission – cela a été dit par le rapporteur de langue allemande, Monsieur Flach – a fourni un travail conséquent. Nous nous sommes concentrés sur les aspects les plus controversés, dans notre conseil comme dans le grand public, que sont les données secondaires et les chevaux de Troie.
Nous nous sommes aussi penchés sur les développements judiciaires internationaux, notamment dans l'Union Européenne, où la conservation des données secondaires donne lieu à un débat juridique et politique nourri qui, s'il est mal compris, peut faire naître quelques fantasmes à propos de la constitutionnalité de nos propres règles.
La commission vous propose d'entrer en matière, par 15 voix contre 6 et 1 abstention. Une minorité Vischer Daniel vous demande de ne pas entrer en matière, ce qui est un peu contradictoire, car une autre minorité Vischer Daniel – la minorité IV, à l'article 19 alinéa 4 – propose de biffer la disposition qui prévoit de conserver les données secondaires, ce qui ne sera pas possible si nous n'entrons pas en matière aujourd'hui. En effet, la loi actuelle permet la conservation des données secondaires.
Une autre minorité Vischer Daniel propose de renvoyer le projet au Conseil fédéral. La commission a rejeté cette proposition, par 16 voix contre 6 et 3 abstentions, car elle trouve absurde de faire deux fois un travail que le Parlement peut faire lui-même à l'occasion du débat sur les données secondaires. La commission a déjà fait ce travail et la minorité s'est d'ailleurs ralliée à ce résultat, mais j'aurai l'occasion d'y revenir.
Au vote sur l'ensemble, la commission a soutenu le projet tel qu'elle l'a modifié et le présente aujourd'hui, par 15 contre 6 et 1 abstention. Je vous remercie d'en faire autant.

Vischer Daniel (G, ZH): Wir sind hier mit einem Gesetz konfrontiert, das die persönliche Freiheit der Bürgerin und des Bürgers eminent betrifft. Ich kann selbstverständlich sehr wohl zwischen einem Strafverfahren und einer geheimdienstlichen Vorfeldermittlung, wie wir sie beim Nachrichtendienstgesetz diskutiert haben, unterscheiden. Hier geht es um den Strafprozess; bei gerichtspolizeilichen Verfahren muss freilich auch die Überwachung Verhältnismässigkeitskriterien genügen.
Ich habe mit meiner Minderheit einen Nichteintretens- und einen Rückweisungsantrag gestellt. Den Nichteintretensantrag ziehe ich zurück und beschränke mich auf den Rückweisungsantrag. Er konzentriert sich auf zweierlei: Zum einen will ich mit meinem Rückweisungsantrag die Vorratsdatenspeicherung abschaffen. Zum andern soll der Staatstrojaner nur unter eingeschränktesten Voraussetzungen zulässig sein; diese sind auch nach langer Beratung nicht festgelegt worden. Herr Kollege Schwaab, dieser Antrag ist keineswegs absurd. Die Kommission hat es nämlich nicht zustande gebracht, die einschränkende Verwendung dieses Staatstrojaners tatsächlich zu regeln.
Kommen wir zur Vorratsdatenspeicherung: Sie ist bis jetzt im Gesetz enthalten, das stimmt. Sie ist aber ein Unding, denn es werden Daten aller Bürgerinnen und Bürger auf Vorrat gespeichert, ohne dass die einzelne Bürgerin oder der einzelne Bürger dazu einen Anlass bieten würde. Das ist eine Präventivüberwachung, deren Daten auf Zusehen hin, gegebenenfalls, gebraucht werden.
Nun kann man mit dem Argument, am Schluss würden ja nur wenige Daten gebraucht, das Problem der Vorratsdatenspeicherung um kein «My» entschärfen. Entscheidend ist, wann überwacht wird: Das geschieht in dem Moment, in dem gespeichert wird, nicht erst in dem Moment, in dem die Daten gelesen werden, weil ein Richter die Bewilligung hierzu gibt. Nicht von ungefähr hat der Europäische Gerichtshof diese Vorratsdatenspeicherung als mit dem Recht der persönlichen Freiheit – einem der höchsten Güter im Verfassungsstaat – unvereinbar erklärt. Er hat dies gerade auch deshalb getan, weil einfach aufs Geratewohl Daten gespeichert werden.
Unsere Verfassung kennt den Schutz der persönlichen Freiheit auch. Ich zweifle nicht daran, dass die Vorratsdatenspeicherung auch in der Schweiz verfassungsrechtlich nicht zulässig ist. Ich hoffe, dass ein entsprechendes Verfahren dies ergeben wird. Der Gesetzgeber ist aber das Verfassungsgewissen der Schweiz. Er muss also handeln, wenn Handeln nötig ist. Deswegen braucht es eine neue Vorlage ohne Vorratsdatenspeicherung.
Der Begriff Staatstrojaner – das ist ein eingebürgerter Begriff, in der Botschaft heisst es Govware – umschreibt eigentlich gut, worum es geht: Der Staat ist plötzlich in Ihrem Computer anwesend. Niemand bestreitet, dass der Staat griffige Instrumentarien zur Verbrechensbekämpfung braucht, aber sie müssen verhältnismässig und vor allem nützlich sein. Es darf nicht einfach etwas installiert werden, bei dem nicht einmal klar ist, wie es technisch gemacht werden soll. Die Kommissionsberatungen bezüglich Staatstrojaner waren von himmelschreiender Widersprüchlichkeit. Es ist nicht einmal entschieden, ob diese Staatstrojaner derzeit überhaupt mit einer Software betrieben werden könnten. Es ist nicht gelungen, hier einschränkende Bestimmungen ins Gesetz zu nehmen, damit diese Eckdaten des Computers nur zur Verbrechensbekämpfung und nur diesem Ziel gemäss überhaupt verwendet werden dürfen. Zudem haben wir bei dieser Bestimmung einen viel zu weit gehenden Deliktekatalog.
Es ist angezeigt, noch einmal über die Bücher zu gehen. Deswegen ist der Rückweisungsantrag meiner Minderheit die einzige adäquate Antwort zu dieser Vorlage.

Le président (Rossini Stéphane, président): Vous l'avez entendu, la proposition de non-entrée en matière de la minorité Vischer Daniel a été retirée.

Huber Gabi (RL, UR): Artikel 13 Absatz 1 der Bundesverfassung, Artikel 8 Absatz 1 EMRK und Artikel 17 Absatz 1 des Internationalen Paktes vom 16. Dezember 1966 über bürgerliche und politische Rechte garantieren das Recht auf Schutz der Korrespondenz wie auch der Beziehungen, die

mittels Post und Fernmeldediensten aufgenommen werden. Dieses Recht ist Bestandteil des Schutzes der Privatsphäre. Diesbezügliche Überwachungen stellen einen schweren Grundrechtseingriff dar. Gemäss Artikel 36 der Bundesverfassung und Artikel 8 EMRK muss die Einschränkung eines Grundrechts durch eine gesetzliche Grundlage gedeckt sein, im öffentlichen Interesse liegen und hinsichtlich des angestrebten Ziels verhältnismässig sein.
Die Totalrevision des Büpf liegt in diesem Spannungsfeld zwischen dem Eingriff in das Grundrecht auf Schutz der Privatsphäre einerseits und der Effizienz der Kriminalitätsbekämpfung durch die Strafverfolgung andererseits. Es geht, auf den Punkt gebracht, um die Frage, ob neue Technologien wie z. B. verschlüsselte Internettelefonie exklusiv den Kriminellen zur Verfügung stehen sollen oder ob diese Technologien auch von den Strafverfolgern zur Bekämpfung schwerer Verbrechen angewendet werden dürfen. Die Vorlage beantwortet diese Frage klar: Das Büpf und die Strafprozessordnung sollen an die technische Entwicklung der letzten Jahre und im Rahmen des Möglichen an die künftigen Entwicklungen in diesem Bereich angepasst werden. Das Ziel besteht ausdrücklich darin, nicht mehr, sondern besser überwachen zu können. Mit der Revisionsvorlage werden die Voraussetzungen für einen Grundrechtseingriff geschaffen und die entsprechenden Anforderungen erfüllt.
Die Antwort liegt ja bereits aufgrund der eigenen persönlichen Lebenserfahrung auf der Hand: Dass sich die Telekommunikation in den letzten Jahren enorm entwickelt und verändert hat, ist offensichtlich. Die technologischen Fortschritte sind ja in der Regel auch nützlich und werden in den allermeisten Fällen in legaler Weise genutzt. Aber sie können eben auch zur Begehung von Straftaten verwendet werden.
Daher ist es geradezu ein Gebot der Rechtsstaatlichkeit, dass auch die Methoden der Strafermittler technisch aufgerüstet werden, damit diese bei der Verbrechensbekämpfung nicht auflaufen, weil ihnen der Gesetzgeber nur mittelalterliche – um nicht zu sagen: vorsintflutliche – Methoden erlaubt. Denn wenn der Zugriff auf verschlüsselte Daten grundsätzlich abgelehnt würde, hiesse das zum Beispiel auch, dass der Zugriff auf verschlüsselte Daten von Pädokriminellen nicht möglich wäre.
Nicht genug betont werden kann, worum es in diesem Gesetz nicht geht: Es geht in diesem Gesetz weder um nachrichtendienstliche Tätigkeiten noch um flächendeckendes Bespitzeln und Ausspionieren unbescholtener Bürger. Es geht in diesem Gesetz einzig und allein darum, die Überwachung von Personen zu ermöglichen, gegen die ein dringender Verdacht auf Begehung einer schweren Straftat besteht. Zudem muss ein Gericht die Überwachungsmassnahme bewilligen.
Das öffentliche Interesse an der Verfolgung schwerer Verbrechen rechtfertigt eine Grundrechtseinschränkung im Rahmen der Gesetzesvorlage, denn ohne Sicherheit gibt es keine Freiheit. Wie bereits gesagt geht es hier nicht um mehr, sondern um eine bessere Überwachung. Wir müssen die Ermittler in Sachen Technologie quasi auf die gleiche Augenhöhe stellen wie die Kriminellen. Würde die Vorlage mit dem Auftrag der Minderheit zurückgewiesen, wäre sie an sich praktisch obsolet, was die Frau Bundespräsidentin in der Kommission mit eindrücklichen Beispielen der Staatsanwaltschaften belegte.
Was die Vorratsdatenspeicherung betrifft, welche die Minderheit Vischer Daniel mit dem Rückweisungsantrag aus der Vorlage streichen will, wird oft das Urteil des Europäischen Gerichtshofes zur EU-Richtlinie 2006/24 zitiert. Darin wird aber nicht gesagt, dass die Vorratsdatenspeicherung an sich verboten ist; es wird ausdrücklich gesagt, dass sie ein geeignetes Mittel zur Kriminalitätsbekämpfung ist. In diesem Urteil ging es vielmehr um die Frage der Verhältnismässigkeit bzw. die Schranken für die Verwendung der Daten oder den Zugang zu ihnen in der nationalen Gesetzgebung. Auch ist die Schweiz, nebenbei bemerkt, nicht der Rechtsprechung des Europäischen Gerichtshofes unterstellt. Abgesehen davon ist die Vorratsdatenspeicherung bereits im geltenden Recht bis zu sechs Monate erlaubt.
In diesem Sinne beantrage ich Ihnen namens der grossen Mehrheit der FDP-Liberalen Fraktion Eintreten auf die Vorlage und die Ablehnung des Rückweisungsantrages. In der Detailberatung werden wir die Minderheitsanträge ablehnen.

Guhl Bernhard (BD, AG): Das Ziel der Revision ist es, ganz kurz gesagt, die Überwachungsmöglichkeiten der Strafverfolgungsbehörden an die neuen technischen Gegebenheiten anzupassen. Die BDP-Fraktion ist klar der Meinung, dass wir den Strafverfolgungsbehörden moderne Mittel geben müssen, damit sie gegen die organisierte Kriminalität in den Bereichen Drogenhandel, Menschenhandel und Mafia ankämpfen können.
Herr Vischer hat den Rückweisungsantrag damit begründet, dass die Daten aller Bürger in der Schweiz erhoben werden – aber das ist nicht alles. Es werden die Daten aller Mobilgeräte, aller Kommunikationsmittel in der Schweiz erhoben, eben auch die Daten von denjenigen Geräten, die Verbrecher und Kriminaltouristen nutzen. Und das ist das Zentrale. Diese Daten gelangen zudem nicht irgendwohin und werden aufs Geratewohl ausgewertet, sondern sie werden nur dann, wenn ein konkretes Verbrechen vorliegt und ein Gericht entschieden hat, dass man diese Daten verwenden kann, an die Strafverfolgungsbehörden übermittelt. Es ist nicht so, dass quasi nachrichtendienstlich mit diesen Daten gearbeitet wird, wenn wir von Daten gemäss dieser Vorlage sprechen.
Folgende Punkte sind aus der Sicht der BDP wesentlich bei dieser Vorlage:
1. Das Büpf ist nicht das Nachrichtendienstgesetz. Es geht nicht ums Schnüffeln. Es geht um schwere Straftaten, und es braucht richterliche Anordnungen. Es kann also nicht einfach ein Polizist oder irgendeine Person hingehen und diese Daten verlangen und in diesen herumschnüffeln.
2. Als das Büpf erarbeitet wurde, gab es gerade einmal zehn Telekomanbieter. Heute haben wir über 300 Anbieter von Fernmeldedienstleistungen. Damals hatten noch zwei von zehn Personen ein Natel. Heute haben wir in der Schweiz über 10 Millionen Mobilfunkgeräte, also mehr Geräte als Personen. Damals wurde telefoniert, und es wurden SMS geschrieben. Heute werden Angebote wie Whatsapp und Skype genutzt, es wird also verschlüsselt kommuniziert. Und die Strafverfolgungsbehörden haben eben leider nicht die Möglichkeit, auf diese Daten zuzugreifen. Man kann da nicht mithören.
3. Die Suche nach vermissten Personen wird verbessert, und man kann neu auch nach flüchtigen Verurteilten fahnden. Das ist eine weitere Verbesserung, die diese Vorlage bringt.
Summa summarum, so findet die BDP, dürfen wir das Feld der neuen Technologien nicht nur den Kriminellen überlassen, sondern auch der Staat muss diese modernen Technologien nutzen können. Der Staat darf nicht vor der Kriminalität kapitulieren. Wer hier für Nichteintreten stimmt, unterstützt also ein Stück weit die Kriminellen.
Die BDP-Fraktion wird auf die Vorlage eintreten und den Rückweisungsantrag ablehnen. Wir bitten Sie, dasselbe zu tun.

Chevalley Isabelle (GL, VD): Cette révision est nécessaire, car nos autorités de poursuite pénale ont besoin d'un instrument de poursuite de la criminalité grave qui soit adéquat et adapté à l'évolution actuelle de la technique. Pour que la poursuite pénale des délits graves et très graves aboutisse, il est indispensable de disposer d'un outil de surveillance de la communication qui soit fonctionnel. Concernant les Govware, le principe de proportionnalité sera appliqué, car il ne pourra être utilisé que si les autres moyens de surveillance moins invasifs ont échoué.
Mais ce n'est pas pour autant que les autorités compétentes pourront écouter les conversations de n'importe qui sans raison. Les chiffres de 2013 montrent bien qu'il ne faut pas retomber dans la psychose des fiches. En ce qui concerne la

surveillance postale des criminels, il y a eu 65 mesures; pour les surveillances sur le réseau fixe de téléphonie fixe, il y en a eu 446; pour la téléphonie mobile, 9950; et pour la surveillance par Internet seulement 56 cas. Ces chiffres sont à relativiser par rapport aux millions de personnes qui utilisent ces moyens de communication en Suisse chaque année. De plus, les autorités de poursuite pénale ont ordonné 10 860 surveillances sur un total de 750 371 infractions. Elles ont donc estimé qu'une mesure de surveillance n'était nécessaire que dans 1,4 pour cent des infractions. Il faut aussi tenir compte du fait qu'une infraction donne souvent lieu à plusieurs mesures de surveillance, par exemple parce qu'il faut surveiller à la fois le téléphone mobile et le raccordement fixe d'un trafiquant de drogue présumé. Seuls environ 5 pour cent des surveillances n'aboutissent à aucun résultat et cela principalement parce que le raccordement surveillé n'est plus utilisé. Donc 95 pour cent des surveillances apportent des éléments à l'enquête.
Ne pas entrer en matière reviendrait à priver nos autorités d'outils nécessaires à l'accomplissement de leur tâche de sécurité dans notre pays. Selon la Conférence des procureurs de Suisse, dont notre commission a entendu les représentants, le trafic de drogue organisé ne peut presque plus être déjoué sans surveillance. Nous ne pouvons pas d'un côté reprocher à la police de ne pas résoudre des affaires de drogues, de pédophilie, de brigandage, de meurtre et autres, et de l'autre ne pas leur donner les outils pour le faire. Car, aujourd'hui, les personnes qui se font surveiller ont un coup technologique d'avance sur nos autorités.
Concernant la proposition de renvoi: celle-ci n'est pas nécessaire, car les critiques faites par les auteurs sont déjà présentées dans les différentes propositions soumises au conseil. De plus, la proposition de renvoi prévoit de limiter l'utilisation des Govware, ce qui réduirait drastiquement la possibilité de surveiller les trafiquants de drogue ou les réseaux du crime organisé par exemple. Ce n'est pas acceptable.
La majorité du groupe vert'libéral entrera en matière sur ce projet.

Fischer Roland (GL, LU): Wir stehen heute mit dem Büpf vor einer grossen Vorlage, welche wohl wie fast keine andere in dieser Session sämtliche Facetten der parlamentarischen Arbeit eindrücklich widerspiegelt. Es handelt sich einerseits um eine sehr technische Materie, und es geht, damit verbunden, um eine harte, langwierige und detaillierte Arbeit in der vorberatenden Kommission, für die ich im Namen der Grünliberalen herzlich danke. Es geht andererseits aber auch um grundsätzliche Fragen wie den Schutz der Privatsphäre, was Emotionen und kontroverse Diskussionen in der Öffentlichkeit und wohl in sämtlichen Fraktionen ausgelöst hat. Vor diesem Hintergrund wird es wohl niemanden gross erstaunen, dass diese Vorlage auch bei den Grünliberalen sehr intensiv und gründlich diskutiert worden ist und dass es sowohl zustimmende als auch kritische Stimmen gibt.
Wenn wir die technologische Entwicklung und unser persönliches Verhalten in den letzten Jahren anschauen, dann kommen wir mit Blick auf diese Vorlage aus dem Staunen nicht heraus. Freiwillig und oft bedenkenlos geben wir im Internet, in sozialen Medien und bei der Nutzung verschiedenster Applikationen unzählige persönliche Daten preis. Auch beim Einkaufen sind wir offenbar bereit, ohne mit der Wimper zu zucken, unser Kundenverhalten als Gegenleistung für Rabatte preiszugeben und zu tolerieren, dass private Unternehmen unzählige Daten über uns sammeln. Die Unternehmen wissen, wo ich mich jetzt aufhalte, welche Inhalte mich interessieren, wie viel Geld ich ausgebe und vieles, vieles mehr.
Weshalb beschleicht uns denn ein solches Unbehagen, wenn es darum geht, den Strafverfolgungsbehörden im Rahmen von schweren Straftaten gewisse Kompetenzen zu geben, um auf gewisse Daten zuzugreifen? Ich denke, es kommt daher, dass es einem liberalen Staatsverständnis entspricht, dass man gegenüber staatlichen Kompetenzen und den Möglichkeiten des Staates, in die Privatsphäre einzudringen, eine grundlegende Skepsis hat – und das ist gut so. Da besteht bei den Grünliberalen eine grundsätzliche Sorge über die zunehmende Datenflut, die zunehmende Überwachungstendenz in der Gesellschaft.
Wenn nun aber eine grosse Mehrheit der grünliberalen Fraktion trotz dieser Sorgen auf die Vorlage eintritt und die Rückweisung ablehnt, hat dies folgende Gründe:
Ein zentrales Element eines liberalen Staatswesens ist nicht nur der Schutz der Privatsphäre, sondern zentrale Elemente sind auch der Rechtsstaat und die Durchsetzung des Rechts. Das bedeutet, dass Straftaten verfolgt und geahndet werden müssen. Damit dies möglich ist, müssen wir aber bereit sein, den Strafverfolgungsbehörden unter Wahrung rechtsstaatlicher Grundsätze die entsprechenden Mittel verhältnismässig in die Hand zu geben. Wir dürfen zum Beispiel aus rechtsstaatlichen Gründen nicht einfach tatenlos zusehen, wenn das organisierte Verbrechen auf technologische Mittel ausweicht, zu denen die Strafbehörden heute keinen Zugang haben.
Beim Büpf geht es nicht um die generelle Überwachung von unbescholtenen Bürgerinnen und Bürgern, sondern um Instrumente der Strafverfolgung. Artikel 1 Absatz 1 des neuen Gesetzes umschreibt den materiellen Geltungsbereich und seine Einschränkung sehr klar: Das Gesetz gilt für die angeordnete Überwachung im Rahmen eines Strafverfahrens, zum Vollzug eines Rechtshilfeersuchens, im Rahmen der Suche nach vermissten Personen und im Rahmen der Fahndung. Somit besteht ein wesentlicher Unterschied zwischen dem Büpf und dem Nachrichtendienstgesetz, bei dem es um die präventive Überwachung geht. Dem Nachrichtendienstgesetz stehen wir Grünliberalen bekanntlich sehr kritisch gegenüber, wir fordern dafür massgebliche Verbesserungen gegenüber der ersten Lesung in unserem Rat. Mit dem Büpf hingegen wird die Strafverfolgung an die heutigen Technologien angepasst. Das Büpf regelt die Strafverfolgung bei dringendem Tatverdacht und erlaubt keine präventive Überwachung. Kritik und Unbehagen gegenüber einer zunehmenden Überwachung seitens des Staates sind aus der Sicht der Grünliberalen gerechtfertigt. Beim Büpf ist die Kritik jedoch gemäss einer grossen Mehrheit der Fraktion am falschen Ort.
Ich bitte Sie deshalb, einzutreten und den Rückweisungsantrag abzulehnen.

Vogler Karl (CE, OW): Sie haben es gehört: Unser Rat behandelt als Zweitrat die Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs und die in diesem Zusammenhang gleichsam notwendige Revision der Schweizerischen Strafprozessordnung und des Militärstrafprozesses.
Die Totalrevision des Büpf soll die Voraussetzungen dafür schaffen, dass der Post- und Fernmeldeverkehr, wenn der dringende Verdacht auf Begehung einer schweren Straftat besteht, zum Zwecke der Strafverfolgung besser – nicht mehr, aber besser – überwacht werden kann. Es geht darum, das Gesetz an die enormen technologischen Fortschritte der letzten Jahre anzupassen und damit eine effiziente Strafverfolgung zu gewährleisten. Anders gesagt: Der Gesetzgeber soll im Bereich der Strafverfolgung durch die rasanten technologischen Fortschritte nicht überholt werden.
Um es klarzustellen – es wurde bereits gesagt –: Bei der Revision des Büpf geht es nicht um eine flächendeckende präventive Überwachung der Bürgerinnen und Bürger oder um nachrichtendienstliche Tätigkeiten; es geht vielmehr um die Sicherstellung einer effizienten Kriminalitätsbekämpfung bei schweren und schwersten Delikten, beispielsweise im Bereich der organisierten Kriminalität, bei Kinderpornografie, bei Tötungs- oder schweren Vermögensdelikten.
Was macht dieses Geschäft, auch aus Sicht unserer Fraktion, schwierig und damit letztlich auch umstritten? Es sind dies gegenläufige Interessen, Spannungsfelder, die man nicht einfach auflösen kann, nämlich der legitime Schutz der Grundrechte, das heisst der Persönlichkeitsrechte auf der einen Seite und das öffentliche Interesse an einer wirksamen Kriminalitätsbekämpfung auf der anderen Seite. Diese Inter-

essen wiederum kollidieren mit den Interessen der Provider, die ihr Geschäftsmodell möglichst ungehindert, ohne weitere Kostenfolgen kommerziell anbieten wollen. In diesem mehrfachen Spannungsfeld befinden wir uns. Es gilt einen Weg zu finden, der es ermöglicht, im Rahmen des Gesetzmässigkeits- und Verhältnismässigkeitsprinzips gerade so viel wie nötig, aber so wenig wie möglich in die Grundrechte, aber auch in die Interessen der Fernmeldedienste einzugreifen.
Die Revision verläuft damit auch auf einem schmalen Grat zwischen dem, was technisch möglich ist, und dem, was rechtlich zulässig sein soll. Gerade der Einsatz der sogenannten Govware bzw. von Staatstrojanern macht den Konflikt deutlich: Nicht alles, was technisch möglich ist, soll rechtlich auch zulässig sein, und nicht alles, was rechtlich zulässig ist, ist technisch ohne Weiteres umsetzbar.
Ich habe es gesagt: Das vorliegende Geschäft betrifft die Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs sowie gleichzeitig die Revision der Strafprozessordnung und des Militärstrafprozesses.
Was sind die wichtigsten Änderungen? Das Büpf erweitert den persönlichen Geltungsbereich erheblich. Neu umfasst der Kreis der Mitwirkungspflichtigen sechs Kategorien mit entsprechenden, im Sinne der Verhältnismässigkeit klar definierten Pflichten, seien diese aktiver oder passiver Art. Das Büpf regelt weiter die Aufbewahrung der Daten und sieht eine Ausdehnung der Aufbewahrungspflicht von sechs auf zwölf Monate für die Randdaten vor. Geregelt werden schliesslich die Rechtsmittel gegen Verfügungen des Überwachungsdienstes. Das Büpf enthält ausserhalb des Strafverfahrens Bestimmungen betreffend die Notsuche für vermisste Personen und die Fahndung nach verurteilten Personen.
Mit den Änderungen in der Strafprozessordnung wird geregelt, unter welchen Voraussetzungen welche Überwachungsmassnahmen angeordnet werden können. Vorausgesetzt sind dabei ein dringender Verdacht und das Vorliegen eines schweren Delikts. Zudem müssen die bisherigen Untersuchungshandlungen erfolglos geblieben oder die Ermittlungen sonst aussichtslos sein, und schliesslich müssen diese Massnahmen durch das Zwangsmassnahmengericht genehmigt werden.
Umstritten ist dabei insbesondere auch die sogenannte Govware, landläufig unter dem Begriff «Staatstrojaner» bekannt. Unter strengen Voraussetzungen sollen damit verschlüsselte Daten mittels Einschleusen von besonderen Informatikprogrammen abgefangen werden. In diesem Kontext ist auch die gesetzliche Grundlage für den Einsatz der sogenannten Imsi-Catcher zu nennen, mit denen Gespräche mitgehört oder aufgenommen werden können.
Ich habe es eingangs gesagt: Wir bewegen uns in diesem Gesetz im Spannungsfeld verschiedener und entgegengesetzter Interessen, und mögliche Missbräuche können nicht ausgeschlossen werden. Allein deswegen die gesetzlichen Grundlagen für eine effektive und effiziente Strafverfolgung nicht zu schaffen und damit das Feld für die Kriminalität weiter zu öffnen wäre nicht zu verantworten.
Zusammengefasst lässt sich sagen, dass die Vorlage den sich ständig verändernden Bedürfnissen der Strafverfolgung Rechnung trägt. Sie beachtet die grundrechtlichen Anforderungen und schafft eine saubere gesetzliche Grundlage für notwendige Ermittlungen im Post- und Fernmeldeverkehr. Die CVP/EVP-Fraktion ist klar für Eintreten auf die Vorlage.
Erlauben Sie mir noch zwei, drei Hinweise zum Antrag auf Rückweisung. Natürlich ist es so – ich habe es gesagt –, dass das Gesetz Missbräuche nicht völlig ausschliessen kann. Das kann übrigens kein Gesetz. Die von Herrn Vischer geäusserten Bedenken können nicht einfach in den Wind geschlagen werden, aber es gilt eine Interessenabwägung zwischen möglichen Missbräuchen und dem öffentlichen Interesse an einer zeitgemässen Kriminalitätsbekämpfung vorzunehmen. Bei einer entsprechenden Abwägung dieser Interessen überwiegt für uns klar das letztere. Kriminalität ist allgegenwärtig, und wir müssen den Strafverfolgungsbehörden die notwendigen Instrumente für eine wirksame Strafverfolgung in die Hand geben. Das entspricht auch rechtsstaatlicher Notwendigkeit.
Der Rückweisungsantrag beinhaltet vier Forderungen, nämlich erstens keine Vorratsdatenspeicherung, zweitens die Einschränkung des Katalogs der Straftaten für Govware und Imsi-Catcher, drittens die Beschränkung der Verwendung von Informationen, die so erlangt wurden, auf die Strafverfolgung, und viertens verlangt dieser Rückweisungsantrag Sicherheitsmassnahmen, damit die Govware auf die Live-Kommunikation beschränkt ist.
Ohne im Detail auf diese Forderungen einzugehen, halte ich Folgendes fest: Würde man diesen Forderungen stattgeben, so würde man, was die ersten beiden Forderungen betrifft, die Möglichkeit der Kriminalitätsbekämpfung deutlich einschränken. Das wollen wir, wie gesagt, nicht. Was die dritte Forderung betrifft, so würde diese zu stossenden Ergebnissen führen. Beispielsweise dürfte man diese Methode bei der Fahndung nach einem flüchtigen Gefangenen nicht anwenden, weil es sich dabei nicht um eine Ermittlung, sondern um eine Fahndung handelt. Und würde man der vierten Forderung stattgeben, so hiesse das, dass damit auch die Erhebung von Randdaten ausgeschlossen würde. Diese Forderungen gehen zu weit. Wir lehnen sie ab.
Zusammengefasst: Ich ersuche Sie, auf die im Gesamten ausgewogene Vorlage einzutreten, und ich ersuche Sie um Ablehnung des Rückweisungsantrages.

Vischer Daniel (G, ZH): Für die Grünen ist dies eine sehr wichtige Vorlage. Wir sind im Bereich des Schutzes der persönlichen Freiheit und des informationellen Selbstbestimmungsrechtes. Es geht um Datenschutz, es geht darum, dass wir mit dem konfrontiert sind, was man in den Achtzigerjahren den Orwell-Staat nannte. Wenn ich es mir überlege: In den Achtzigerjahren wäre niemand auf die Idee gekommen, dass es einmal möglich sein würde, auf Vorrat Daten zu speichern, die dann plötzlich Verwendung finden, und dies, wie die Kommissionsmehrheit es will, über ein ganzes Jahr. In diesem Sinn knüpft die Vorlage an die damalige Diskussion an, auch an die Diskussion nach der Fichenaffäre, selbst wenn nicht einfach alles gleich ist – das ist völlig klar. Natürlich sind wir hier im Bereich des Strafverfahrens. Die Grünen wollen keinen «Huscheli-Staat», die Grünen wollen keine «Huscheli-Strafverfolger», die nicht in der Lage sind, effizient Verbrechen zu bekämpfen. Aber die Grünen wollen, dass ein verhältnismässiger Strafverfolgungsstaat obwaltet; sie wollen, dass nicht einfach Daten gespeichert werden können; sie wollen, dass bezüglich Staatstrojaner nicht einfach ohne Kontrollmöglichkeit in Computer eingedrungen werden kann.
Wir treten auf die Vorlage ein, weil das Gesetz mit der Rückweisung ja nicht geändert würde und weil es auch Verbesserungen enthält. Der Ständerat hat die Vorlage durchgewinkt. Das hatte auch einen Grund, denn der Diskurs über die Vorratsdatenspeicherung gewann eigentlich erst nach der Ständeratsdebatte flächendeckend Raum, nach dem nun schon mehrfach zitierten Entscheid des Europäischen Gerichtshofes. Das hat auch die Debatte verstärkt, in der gefordert wird, es sei grundsätzlich über diesen Typ der Überwachung nachzudenken. Nun gab es hier eine Parallelisierung zwischen dem Nachrichtendienstgesetz und dem Büpf. Wir wissen das auseinanderzuhalten – wie vielleicht nur wenige in diesem Saal. Es geht hier nicht um Geheimdienst, also geht es hier auch um andere Kriterien.
Wenn aber gesagt wird, wir seien hier nicht bei der präventiven Ermittlung, so ist dies in einem gewissen Sinn dennoch falsch. Das ist ja die Essenz des Entscheide des Europäischen Gerichtshofes: Bei der Vorratsdatenspeicherung wird ein neuer Typ von präventiver Überwachung eingeführt, bei dem man nicht mehr einfach sagen kann, die Überwachung geschehe auf Tatverdacht hin, denn – wie schon bei der Begründung des Rückweisungsantrags erwähnt – es kommt auf den Moment der Datenüberwachung und den Moment der Speicherung an und nicht auf den Moment, in dem die Daten gelesen werden. Ab dem Moment der Überwachung steht jede Bürgerin und jeder Bürger unter potenziellem

Straftatverdacht. Genau das wollen wir nicht, und das will auch der Europäische Gerichtshof nicht.
Ich ersuche Sie, diesen Rückweisungsantrag ernst zu nehmen. Die Kommission war überfordert damit, die Vorratsdatenspeicherung abzuschaffen und das Gesetz neu aufzubauen; die gleiche Bemerkung gilt bezüglich der Staatstrojaner.

Naef Martin (S, ZH): Kollege Vischer, ich bin inhaltlich weitestgehend Ihrer Meinung, was die Vorratsdatenspeicherung usw. betrifft. Was ich nicht verstanden habe: Warum verwirklichen Sie nicht, zusammen auch mit mir allenfalls, Ihre Vorstellungen einer gesetzlichen Lösung im Rahmen der Gesetzesberatung, sondern beantragen eine Rückweisung mit Auflagen? Das finde ich eigentlich nicht so schön. Können Sie mir das noch einmal ausführen?

Vischer Daniel (G, ZH): Sie haben Recht, Herr Naef, ich bin weiss Gott kein Fan von Rückweisungsanträgen. Wir sind zwar für Eintreten, aber hier haben wir ein Problem. Die Kommission kann nicht in einer Gesetzesberatung, bei der keine Klarheit über die Zielsetzung besteht, mit hundert Eventualfällen alles genau so legiferieren, dass immer alle möglichen Folgen bedacht werden. Sie sehen ja schon, wie viele Minderheitsanträge heute eingebracht werden. Wir wissen nicht, ob wirklich alles konsequent in der Folge so nachgezeichnet ist. Beim Staatstrojaner war es ja so: Je länger die Kommissionsberatung dauerte, desto grösser wurden die Unklarheiten. In letzter Minute wurden noch Verbesserungen formuliert. Aber ich bin sicher, dass die Verwaltung bei einer klaren Stossrichtung tatsächlich ein griffiges, gutes Gesetz machen würde. Überfordern Sie also nicht den Gesetzgeber, wenn er selbst nicht mehr weiterkommt, sondern bauen Sie auf die Vernunft der Verwaltung, vor der ich Hochachtung habe.

Glättli Balthasar (G, ZH): La loi sur la surveillance de la correspondance par poste et télécommunication autorise déjà maintenant la surveillance de toutes les citoyennes et tous les citoyens intègres et au-dessus de tout soupçon. La révision, qui vise à doubler la durée de conservation des données de communication, est disproportionnée. D'après une étude de l'Institut Max Planck, elle n'apporterait absolument pas les résultats escomptés. Il faut donc corriger ce défaut, et non l'accentuer! Le groupe des Verts demande par conséquent le renvoi du projet dans le but de l'améliorer.
La durée de conservation de données de communication ne doit pas passer à douze mois. Tout au contraire: la Confédération devrait pouvoir stocker des données uniquement lorsqu'il y a un soupçon concret d'un acte délictueux. La loi doit d'ailleurs garantir que les données ne seront utilisées qu'aux fins de l'enquête pénale. La destruction des données doit être effective une fois le délai écoulé, et il faut aussi à tout prix éviter que les données stockées puissent ensuite être utilisées à des fins commerciales ou frauduleuses.
En outre, le catalogue des délits prévoyant le recours à des chevaux de Troie étatiques – des logiciels espions – doit être restreint aux crimes graves et violents. Sans ces modifications, le groupe des Verts rejettera le projet de révision lors du vote final.
Une surveillance accrue et généralisée des citoyens ne respecte pas le principe fondamental d'un Etat de droit: la présomption d'innocence. Le dispositif de surveillance qui nous est proposé part au contraire du principe que chacun d'entre nous est potentiellement un criminel. Cela est inacceptable et constitue un viol de la vie privée que les Verts ne peuvent pas défendre.
Es ist, wenn man nach Europa schaut, nicht einfach eine Debatte zwischen links und rechts, nicht einfach eine Debatte zwischen Leuten, die den Staat nicht ernst nehmen, und anderen, die möglichst hart durchgreifen wollen. Wenn wir nach Europa schauen, wenn wir nach Deutschland schauen, wenn wir in die anderen europäischen Länder schauen, wo die Debatte um die Vorratsdatenspeicherung – ich möchte doch sagen – schon etwas länger und auch sehr vertieft geführt wird, dann sehen wir, dass es gerade auch die liberalen Kräfte sind, die sich dagegen wehren, dass aus einer Entwicklung der technischen Möglichkeiten die Rechtfertigung abgeleitet wird, eine Generalüberwachung einzuführen. Es ist kein Linker, sondern der frühere Bundesinnenminister Gerhart Baum von der FDP, der angekündigt hat, dass er diese Frage vor das Bundesverfassungsgericht ziehen würde, wenn die grosse Koalition die Vorratsdatenspeicherung in Deutschland wieder einführen würde. Ich denke, er hat Recht, wenn er sich darüber beklagt, dass die Unschuldsvermutung schon dann verletzt wird, wenn diese Daten gespeichert werden.
Wenn man sich gegen eine Überwachung auf Vorrat wehrt, hilft es nichts, wenn dann argumentiert wird, diese Daten könnten nur ab einem bestimmten richterlichen Entscheid eingesehen werden. Im Gegenteil, der Schutz des Privatlebens, der Privatsphäre, der freien Kommunikation hat dort anzusetzen, wo die Leute in der freien Ausübung ebendieser Rechte behindert werden.
Ein grosser Teil der Gewalttaten findet in den Haushalten statt. Sie sind oft schwierig aufzuklären, weil Aussage gegen Aussage steht. Würden Sie dann mit der gleichen Argumentation, mit der man uns hier die Vorratsdatenspeicherung verkauft, dafür plädieren, dass man in allen Wohnräumen Mikrofone aufstellt und diese Daten mal auf Vorrat, zugänglich halt natürlich nur bei richterlichem Beschluss, irgendwo speichert? Das ist eben eine Verletzung der Privatsphäre, die auch dann stattfindet, wenn die Freigabe der Daten erst auf richterlichen Beschluss hin erfolgt.
In dem Sinn: Haben Sie – das richtet sich vor allem an die Liberalen, mit grünem Flügel oder ohne – als Liberale Mut, und stehen Sie zu den liberalen Freiheitsrechten, auch wenn Ihnen dann mal ein Lüftchen entgegenwehen könnte! Es ist einfach, die Freiheitsrechte zu verteidigen, wenn es um nichts geht und wenn es unbestritten ist. Man muss sie dann verteidigen, wenn sie wirklich bedroht sind.

Lüscher Christian (RL, GE): Monsieur Glättli, je vous félicite tout d'abord pour votre maîtrise impressionnante de la langue française. Ensuite, j'ai une question par rapport à votre intervention. Vous avez dit que le présent projet de loi devrait être renvoyé au Conseil fédéral afin qu'il l'améliore. Savez-vous combien de séances et d'heures de commission ont été consacrées à cet objet? Pouvez-vous expliquer pourquoi les améliorations que vous demandez aujourd'hui n'ont pas été proposées en commission?

Glättli Balthasar (G, ZH): Wir haben verschiedene Anträge, die jetzt als Minderheitsanträge vorliegen, auch in der Kommission eingebracht. Ich kenne die lange Geschichte dieses Geschäfts. Aber wie Daniel Vischer vorher auf eine ähnliche Frage ausgeführt hat, bedingen eine Abschaffung der Vorratsdatenspeicherung und ein allfälliger Ersatz zum Beispiel durch ein Quick-Freeze-Verfahren, aber auch die Limitation des Deliktekatalogs, vor allem aber das Erste, grössere Änderungen am Gesetz. Wenn man ein alternatives Verfahren einführen will – wir sind ja nicht dafür, die Strafverfolgung einfach zu schwächen –, ein neues Verfahren, das einen schnellen Zugriff ermöglicht, wenn es nötig ist, aber nicht eine präventive Überwachung schafft, dann ist das ein neuer gesetzgeberischer Auftrag. Ein solcher ist idealerweise nicht durch die Kommission aufgrund eines Minderheitsantrages zu erarbeiten, sondern durch die Administration vorzubereiten.

Jositsch Daniel (S, ZH): Worum geht es? Wir kommunizieren heute alle täglich, stündlich via Natel, mit unserem Computer usw. Leider ist es so, dass auch Kriminelle moderne Kommunikationsmittel brauchen, und deshalb ist die Überwachung der Telekommunikation in der modernen Strafverfolgung zentral. Deshalb gibt es auch das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Es existiert bereits. Was diese Vorlage will, ist einzig und allein, das Büpf der modernen Telekommunikation anzupassen.

Es ist für den normalen Bürger und die normale Bürgerin wahrscheinlich kaum verständlich, aber es ist tatsächlich so: Unser Gesetz erlaubt es der Strafverfolgungsbehörde nicht, die modernen Telekommunikationsmittel zu überwachen. Wenn ich also als Strafrechtsprofessor nicht unbescholtene Studierende unterrichten, sondern ein Seminar für Kriminelle machen würde, dann wäre das für mich ein ganz zentraler Themenblock: ihnen zu erklären, wie sie untereinander kommunizieren können, ohne dass die Strafverfolgungsbehörde sie überwachen kann. Das ist ein Missstand, bei dem wir unbedingt Abhilfe schaffen müssen. Deshalb sind wir heute hier und beraten über dieses Gesetz.

Nun wird uns vorgegaukelt – Sie haben es gehört –, es gehe um die Verteidigung gegenüber dem Überwachungsstaat. Mit diesem Gesetz werde der unbescholtene Bürger überwacht, und es finde eine präventive Überwachung statt. Das ist definitiv nicht so. Es geht hier einzig und allein um die Überwachung im Rahmen der Strafverfolgung. Damit also eine entsprechende Überwachung stattfinden kann, muss zuerst einmal ein Tatverdacht vorliegen, und es muss ein Strafverfahren eröffnet sein; es muss geprüft werden, ob ein Delikt vorliegt, das so schwer wiegt, dass die Überwachung stattfinden kann, und es muss eine entsprechende Bewilligung vorliegen, damit sie durchgeführt werden kann. Nur wenn das alles gegeben ist, nur dann kann die Überwachung stattfinden. Das heisst, es besteht keine Gefahr, dass der unbescholtene Bürger überwacht wird. Es besteht keine Gefahr, dass Leute ausserhalb des Strafverfahrens zu präventiven Zwecken überwacht werden.

Die Ironie respektive das Erstaunliche besteht darin – darauf hat selbst Herr Vischer vorher hingewiesen –: Die ganze Grundrechtsdebatte, die wir hier führen, hätten wir vor kurzer Zeit, als wir das Nachrichtendienstgesetz beraten haben, tatsächlich führen können; denn gemäss Nachrichtendienstgesetz findet die Überwachung im präventiven Bereich statt. Hier aber geht es nur um die Überwachung in Rahmen von Strafverfahren.

Man kann im politischen Prozess ja verschiedener Ansicht sein. Sie können, wie das beispielsweise Herr Vischer macht oder Herr Reimann macht oder Herr Schwander macht, grundsätzlich dagegen sein und konsequenterweise das Nachrichtendienstgesetz und das Büpf ablehnen. Sie können konsequenterweise dafür sein, wie es andere sind. Was Sie aber nicht machen können, ist, das Nachrichtendienstgesetz unterstützen und das Büpf ablehnen – das macht definitiv keinen Sinn!

Und wenn ich schaue, wer diese Position offenbar einnimmt, dann muss ich sagen – und da schaue ich zur SVP-Fraktion –: Es hat offenbar mit dem zuständigen Bundesrat zu tun, dass Sie im einen Fall zustimmen und in diesem Fall jetzt ablehnen wollen. Das ist aber weiss Gott kein Grund, ein Gesetz abzulehnen! Oder es hat damit zu tun, dass Sie der Telekommunikationsbranche nahestehen, die das Gesetz nicht will.

Deshalb ersuche ich Sie, einzutreten – das scheint unbestritten zu sein – und den Rückweisungsantrag der Minderheit Vischer Daniel abzulehnen.

Reimann Lukas (V, SG): Herr Kollege Jositsch, Sie haben bei der Debatte über das Nachrichtendienstgesetz gehört, dass es dort um weniger als zehn Fälle pro Jahr geht. Um wie viele Fälle pro Jahr geht es beim Büpf?

Jositsch Daniel (S, ZH): Es geht beim Büpf um wesentlich mehr Fälle, und der Grund ist evident. Wir haben Gott sei Dank in unserem Land weniger Terrorverdächtige als Leute, die sich einer strafbaren Handlung verdächtig gemacht haben. Ich nehme an, Sie wollen mit Ihrer Frage darauf hinweisen, dass diese Vorlage aufgrund der Zahl der Überwachungen nun wesentlich wichtiger sei. Wichtiger ist sie, weil wir uns natürlich in allererster Linie mit dem Strafverfahren auseinandersetzen müssen. Nichtsdestotrotz ist aber der Unterschied evident, und deshalb ist es wichtig, dass Sie mir die Gelegenheit geben, das noch einmal kurz zu erläutern.

Im Nachrichtendienstgesetz geht es um den präventiven Bereich, und deshalb muss man wesentlich einschränkender sein. Deshalb haben wir im Nachrichtendienstgesetz auch sehr viel mehr Hürden eingebaut. Hier aber haben wir mit dem Strafverfahren einen wesentlichen Bereich, in dem wir aber grundsätzlich die Hürde haben, dass die Überwachung im Rahmen eines laufenden Strafverfahrens erfolgen muss; ausserhalb eines Strafverfahrens bestehen diese Überwachungsmöglichkeiten im Rahmen des Büpf nicht.

Leutenegger Oberholzer Susanne (S, BL): Ich spreche für eine knappe Mehrheit der SP-Fraktion, die für die Rückweisung dieser Vorlage ist, und zwar aus grundrechtlichen Überlegungen. Wir sind klar der Meinung, dass auch im Namen der Strafverfolgung bzw. der Sicherheit nicht jeder Grundrechtseingriff gerechtfertigt werden kann. Die Vorratsdatenspeicherung ist ein Grundrechtseingriff. Was hier so harmlos daherkommt, ist in der Realität ein Archiv unserer gesamten Telefon- und Internetkommunikation der letzten Monate oder des letzten Jahres. Wer meint, erst der Zugriff auf die Inhalte sei ein Grundrechtseingriff, der liegt falsch. Bereits die Sammlung dieser Daten ist ein Eingriff in die Grundrechte, zumal die Sammlung ohne Verdacht auf eine strafbare Handlung erfolgt. Das ist ein Verstoss gegen die persönliche Freiheit, verletzt den Schutz des privaten Familienlebens und insbesondere das informationelle Selbstbestimmungsrecht. Wir haben diese Debatte eigentlich erst nach dem Urteil des Europäischen Gerichtshofes vom 8. April 2014 geführt. Interessanterweise haben wir sie aber nicht à fond geführt. Die Dimension der geplanten Datensammlung übersteigt die seinerzeitige Fichenaffäre bei Weitem. Damals wurden 900 000 Bürgerinnen und Bürger fichiert. Ich wurde ebenfalls fichiert und habe meine Fiche im Hinblick auf diese Debatte noch einmal angeschaut. Da wurden auch nur Rahmendaten erfasst: Mit wem habe ich telefoniert, wohin bin ich gegangen. Nicht erfasst war der Inhalt der Kommunikation.

Bei der Speicherung der Rahmendaten geht es um Milliarden von Kommunikationen, um die Verbindungen von weit über 10 Millionen Kommunikationseinheiten. Stellen Sie sich vor, wie viele Handys, wie viele Festnetzverbindungen, wie viele Computer wir haben. Alle Verbindungen über diese Geräte werden erfasst. Rechtlich braucht es für jeden Grundrechtseingriff eine Rechtsgüterabwägung, eine Rechtfertigung; darin sind sich nicht nur die Juristen einig, sondern auch alle Bürgerinnen und Bürger. Zu prüfen sind dabei nicht nur die Gesetzmässigkeit und die Wahrung des Grundgehalts, sondern auch die Verhältnismässigkeit: absolut und in Bezug auf die Ziel-Mittel-Relation und das öffentliche Interesse.

Ich möchte mich nicht zur Wahrung des Grundgehalts äussern, aber zum öffentlichen Interesse und zur Verhältnismässigkeit. Es wurde behauptet, wir bräuchten das; Frau Chevalley, Frau Huber und Herr Vogler haben das betont. Das Max-Planck-Institut kommt in einer Untersuchung aus dem Jahr 2011 klar zum gegenteiligen Schluss.

Ich möchte Ihnen nahelegen, eine Plausibilitätsüberlegung zu machen. Die Wahrscheinlichkeit, aufgrund der weit über 10 Millionen – wahrscheinlich sind es 20 Millionen – erfassten Kommunikationseinheiten einen Straftäter zu finden, liegt im Promillebereich. Heute werden 5000 bis 6000 solcher Kommunikationseinheiten für ein Strafverfahren angefordert. Wenn Sie es hochrechnen: Sie haben insgesamt vielleicht 10 bis 20 Millionen Kommunikationseinheiten, 5000 bis 6000 davon werden inhaltlich überprüft. Sie können sich ausrechnen, dass das im Promillebereich liegt. Das belegt doch ganz klar: Das öffentliche Interesse an dieser massiven Verletzung der Grundrechte bzw. die Verhältnismässigkeit ist zu verneinen. Das Verfahren kostet sehr viel Geld – das Geld zu verbrennen wäre wahrscheinlich effizienter als diese flächendeckende Fichierung unserer Bürgerinnen und Bürger.

Ich komme noch kurz auf die Staatstrojaner zu sprechen. Es ist interessant, wie sich die Diskussion in der Kommission entwickelt hat. Ich verweise nochmals auf das Grundsätzli-

che. Wir haben immer noch keine befriedigende Antwort auf die Frage, was mit dem Einsatz von Govware verändert werden kann und wer den Einsatz kontrolliert. Für mich entscheidend ist: Die Staatstrojaner können eingeschleust werden, sie können Programme zerstören, sie können Computersysteme zerstören. In der Botschaft des Bundesrates wird auf Seite 2775 vermerkt: «Aus Sicht der kontaktierten Fachleute aus dem wissenschaftlichen Bereich ist es jedoch nicht möglich, Govware zu entwickeln und in Betrieb zu halten, die unter allen Umständen korrekt funktioniert, d. h. keinen Einfluss auf andere Programme oder Funktionen hat.» Das wäre vielleicht auch meine Antwort an Herrn Naef. Auch in der Kommission konnten wir diese Frage nicht klären, trotz aller Abklärungen.
Zum Schluss: Es stellt sich doch auch beim Büpf ganz grundsätzlich die Frage, ob beim Staat der Einsatz aller Überwachungsmittel geheiligt werden kann. Unter dem Siegel der Verfolgung von kriminellen Straftaten könnte man alles bewilligen. Jede und jeder im Saal muss eine Rechtsgüterabwägung vornehmen. Ich bitte Sie um eines: Sorgen Sie mit dem gesunden Menschenverstand für eine Rückweisung des Gesetzes. Helfen Sie mit, die Kommunikationsüberwachung auf ein rechtsstaatlich vertretbares Mass zurückzustutzen. Dazu gehört auch eine Überprüfung der geltenden Praxis der Rahmendatenspeicherung; deswegen ist auch die Rückweisung wichtig. Die Rahmendatenspeicherung ist nämlich in Bezug auf die Grundrechtsfrage bislang noch nicht überprüft worden, vor allem nicht von unserem Parlament.
Ich danke Ihnen für die Rückweisung.

Reimann Lukas (V, SG): Ich nehme es vorweg: Die SVP-Fraktion beschloss mit einer Zweidrittelmehrheit, mit 22 zu 11 Stimmen, die Rückweisung dieses Geschäftes zu unterstützen. Der liberale Freiheitsdenker Roland Baader schrieb in seinem bemerkenswerten Buch «Freiheitsfunken»: «Das einzig wahre Menschenrecht ist das Recht, in Ruhe gelassen zu werden – von jedem, den man nicht eingeladen hat oder den man nicht willkommen heisst.» Genau über dieses Recht debattieren wir heute. Es geht heute nicht darum, ob ein Terrorist überwacht wird oder nicht, sondern es geht darum, ob Sie alle überwacht werden oder nicht. Es geht darum, auch wenn heute das Gegenteil behauptet wurde, ob unbescholtene Bürger bespitzelt werden oder nicht. Nur darum geht es, wenn auf Vorrat alle Daten von allen Bürgern erhoben werden. Zudem gibt es immer wieder Menschen, die über Jahre bespitzelt und beschattet wurden und die am Schluss unschuldig waren und freigesprochen wurden. Denken wir nur an den Fall Holenweger.
Der Staat hat kein Recht, welches die Bürger nicht auch gegenüber dem Staat hätten. Lässt sich der Staat überwachen? Nein! Die Verwaltung beschliesst in Hinterzimmern, der Bundesrat ebenso. Der Staat soll doch die Bürger schützen und sie nicht allgemein verurteilen. Was ist das eigentlich für ein negatives Menschenbild, das hier gepflegt wird? Was ist das für ein Rechtsverständnis, das die Menschen kriminalisiert, bevor sie schuldig gesprochen wurden? Dieses enorme Misstrauen gegenüber den Bürgern seitens des Staates ist absolut unschweizerisch. «Einen Staat, der mit der Erklärung, er wolle Straftaten verhindern, seine Bürger ständig überwacht, kann man als Polizeistaat bezeichnen.» Dies sagte Ernst Benda, der ehemalige Präsident des Bundesverfassungsgerichtes. Ja, heute entscheiden wir tatsächlich, ob die Schweiz weiterhin ein Land der Freiheit und der Bürgerrechte sein will oder ob sie zu einem Polizei- und Überwachungsstaat verkommt.
Was sind die Kennzeichen eines Überwachungsstaates? Im Überwachungsstaat sollen die Erkenntnisse aus der Überwachung laut ihren Fürsprechern hauptsächlich zur Verhinderung und Ahndung von Gesetzesverstössen verwendet werden. Die Prävention von Straftaten und anderen unliebsamen Verhaltensweisen der Bürger findet im Überwachungsstaat durch einen hohen Überwachungsdruck statt. In diversen überwachenden Staaten waren bzw. sind präventive Festnahmen überwachter Personen vor Veranstaltungen üblich, um das öffentliche Erscheinungsbild der Veranstaltung zu beeinflussen. Der Überwachungsstaat zeichnet sich durch die Einschränkung des Datenschutzes, der Privatsphäre und der informationellen Selbstbestimmung aus.
Als Beispiele für rechtliche Massnahmen eines Überwachungsstaates werden immer wieder Telekommunikationsüberwachung und Vorratsdatenspeicherung genannt. Es war nie das Schweizer Staatsverständnis, dass man alle Bürger überwacht. Der Bürger in der Schweiz ist Kunde, und der Staat handelt im Interesse der Bürger, nicht gegen die Interessen der Bürger. Der Bürger ist nicht der Untertan, den man überwachen kann, wie man will. Frei sein und frei bleiben, das ist die Tugend, die in der Schweiz gilt und der Schweiz über Jahrhunderte Erfolg gebracht hat.
Was ich heute wieder gehört habe und nicht mehr hören kann: Wer nichts zu verbergen hat, der kann ja die Rechte zum Schutz der Privatsphäre aufgeben. Ja, und wer nichts zu sagen hat, kann auch das Recht auf freie Meinungsäusserung aufgeben – das wäre etwa gleich dumm.
Worum geht es bei der Revision des Büpf? Das Büpf sieht eine massive Ausweitung der staatlichen Überwachung vor: die Speicherung von personenbezogenen Daten aller unbescholtenen Bürger auf Vorrat, rückwirkend auf zwölf Monate; die Speicherung sämtlicher Verbindungsdaten Ihrer Telefonate und E-Mails ohne – ohne! – irgendeinen Verdacht; das Einschleusen von Programmen auf Ihre Computer, sogenannte Staatstrojaner, um unbemerkt Inhalte, Bilder, Texte, Aussagen mit- oder auszulesen sowie Ihre Kamera zu steuern, vorläufig nur im Verdachtsfall.
Kommen wir zum Kosten-Nutzen-Verhältnis: Derart weitgehende Eingriffe sollten doch mehr Nutzen als Kosten mit sich bringen. Sie wissen, dass die Revision des Büpf Millionen von Franken kostet. Zu beachten ist dabei, dass jede Datensammlung im Ausmass mehrerer Petabytes Kosten verursacht, welche schlussendlich auf die Allgemeinheit überwälzt werden. Die betroffenen Provider werden ihre Telekommunikations- und Internetangebote entsprechend verteuern, der Konsument zahlt mehr. Bereits heute müssen Provider die Verbindungsdaten der letzten sechs Monate speichern und sie den Ermittlungsbehörden auf richterlichen Beschluss hin übergeben; es stehen also bereits ausreichend Daten zur Verfügung. Im Berichtsjahr 2014 betrafen gerade einmal 0,8 Prozent der durch das Büpf erlaubten Anfragen Terrorverdachtsfälle – in jedem Votum hörte ich heute das Wort «Terror» –, und nur bei 41 von 10 000 überwachten Personen ging es um Kinderpornografie.
Die Ausweitung der Vorratsdatenspeicherung auf zwölf Monate bietet keinen Mehrwert. Das zeigt ganz klar auch die Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Sie verglich nämlich die Aufklärungsquoten von Staaten mit Vorratsdatenspeicherung und von Staaten ohne Vorratsdatenspeicherung. Es ist schlicht kein Mehrwert zu erkennen. Die Programmierung von Staatstrojanern wird ebenfalls Millionen verschlingen. Dort, wo effektiv Investitionen nötig wären, nämlich beim Personal, das die Daten auswertet, und bei den Auswertungstools für diese riesigen Datenmengen, werden mit Sicherheit noch weitere Kosten für Personal und Infrastruktur anfallen. Es käme am Schluss zu einem Kontroll- und Freiheitsverlust ohne Mehrwert.
Die Privatsphäre ist ein Grundrecht jedes Bürgers in einer Demokratie. Die elektronische Datensammlung birgt weit grössere Risiken als einst die Fichensammlung. Es ist eine grosse Datensammlung, es ist wie bei Schleppnetzfängen. Zahlreiche Informationen, die beispielsweise für fremde Geheimdienste, kommerzielle oder politische Zwecke ausgeschlachtet werden könnten, fallen an. Es stellt sich die Frage: Wer überwacht denn die Datensammler und die Datenauswerter? Und wer stellt sicher, dass der möglicherweise im Ausland programmierte Staatstrojaner nicht zum Vollstreckungsgehilfen anderer Nationen wird? Schon heute gibt es klare Anzeichen dafür, dass auch ausländische Geheim- und Nachrichtendienste auf die in der Schweiz auf Vorrat gespeicherten Daten Zugriff haben.

Die systematische Überwachung von unschuldigen Menschen ist einer Demokratie unwürdig. Eine Überwachungskultur ist in ein Gesetz gegossenes Misstrauen. Die Revision des Büpf löst keine Probleme, sie schafft aber neue. Die wirklichen Probleme der Staatssicherheit und der Strafverfolgungsbehörden, die fehlenden personellen und technischen Ressourcen zur Auswertung der in vielen Fällen bereits vorhandenen Daten, werden damit nicht gelöst.
Ich bin daher klar der Auffassung, dass die Änderung des Büpf nicht zu einer wirksamen Terrorprävention oder Strafverfolgung beiträgt, sondern eine überdimensionierte staatliche Überwachung nach sich zieht. Dagegen hilft einzig die Rückweisung. Es ist klar, dass wir für harte Strafen und einen funktionierenden Strafvollzug sind. Aber bürokratische Auflagen und Millionen an Mehrkosten und einen ganzen Industriezweig als verlängerten Arm des Staates zu beschliessen geht zu weit. Das geht insbesondere deshalb zu weit, weil Nutzen und Kosten in keinem Verhältnis zueinander stehen. Sie haben gesehen, der Mehrwert ist gering, und es geht hier – im Gegensatz zum Nachrichtendienstgesetz – um Tausende, ja um Zehntausende von Personen, die überwacht und bespitzelt werden. Es ist klar, dass wir ein revidiertes Gesetz brauchen – deshalb sind wir auch für Eintreten – und dass das Gesetz mit der Zeit und mit der technologischen Entwicklung gehen sollte. Die Botschaft und die vorliegende Vorlage gehen aber in die falsche Richtung. Sie führen primär zu einem erheblichen bürokratischen Mehraufwand für die Wirtschaft und erhöhen deren Aufwände, ohne dass die Massnahmen wirksamer wären.
Es braucht ein besseres Verhältnis von Kosten und Nutzen; deshalb empfehle ich die Rückweisung der Vorlage.

Badran Jacqueline (S, ZH): Herr Kollege Reimann, Sie benutzen das Internet; wir alle hier drin benutzen Google, wir benutzen Facebook, wir benutzen Twitter, wir benutzen alles Mögliche – so, wie ungefähr 95 Prozent der Bevölkerung. Kommerzielle globale Grosskonzerne wissen, was wir essen; sie wissen, wohin wir in die Ferien gehen; sie kennen unsere Präferenzen, sogar bis hin zu den sexuellen Präferenzen derjenigen, die im Internet solche Sachen konsumieren.
Wenn Sie das anschauen: Finden Sie das nicht ein bisschen unverhältnismässig im Vergleich zu einer kontrollierten – absolut kontrollierten – Situation, wie wir sie hier jetzt anstreben? Und was genau tut die SVP gegen diese gigantische Vorratsdatenspeicherung von kommerziellen Anbietern?

Reimann Lukas (V, SG): Ja, das ist ein grosser Unterschied. Jeder einzelne Nutzer kann sich schützen. Ich kann meine Daten verschlüsseln, wenn ich mit Ihnen kommuniziere. Das ist auch ein grosses Problem der Vorlage. Jeder Schwerkriminelle, den wir erwischen wollen, wird seine Daten verschlüsseln. Er wird diese Kommunikationsmittel sicher so verwenden. Man wird immer kommunizieren können, ohne dass der Staat einen Zugriff auf die Daten hat. Auch der einzelne private Nutzer hat die Möglichkeit, seine Daten zu verschlüsseln, damit zumindest die privaten Anbieter und die sogenannten Grosskonzerne nicht die Möglichkeit haben, alles mitzuverfolgen, was er am Computer macht.

Chevalley Isabelle (GL, VD): Monsieur Reimann, au sein de la commission dont nous sommes tous les deux membres, nous avons entendu les représentants de la Conférence des procureurs de Suisse qui nous ont clairement dit que sans ces outils que sont les Govware et les IMSI-Catcher, les procureurs ne pouvaient pas résoudre les affaires de trafic de drogue. Aujourd'hui, ils ont besoin de ces outils. Dès lors, comment envisagez-vous de résoudre le problème des trafiquants de drogue sans ces outils?

Reimann Lukas (V, SG): Ich bin auch der Meinung, dass wir den Drogenhandel bekämpfen müssen. Sie werden mit diesem Gesetz mehr Kleindealer erwischen; da bin ich mit Ihnen einverstanden. Aber diejenigen Dealer, die ganz oben sind, werden ihre Daten verschlüsseln. Da helfen andere Mittel, da hilft der Schutz der Grenzen. Was nützt es, die besten Überwachungsgesetze zu haben, wenn die Grenze offen ist und jeder frei hereinkommen und hinausgehen kann, wie er will? Das nützt gar nichts. Da müssen wir ansetzen. Wir müssen bei härteren Strafen, bei der wirksameren Ausweisung von Drogendealern und Drogenhändlern ansetzen. Die ganze Bevölkerung zu überwachen und einzelne Drogendealer, die vielleicht nicht verschlüsselt kommunizieren, herauszufischen ist unverhältnismässig.

Guhl Bernhard (BD, AG): Herr Reimann, Sie haben mit Ihrer Antwort auf die Frage von Kollegin Badran eigentlich genau das Hauptargument für diese Vorlage geliefert.
Meine Frage lautet: Ist in der Vorlage hier vorgesehen, dass die Strafverfolgungsbehörden bei schweren Kriminalfällen die Möglichkeit erhalten, mit sogenannter Govware jenen Kriminellen, welche verschlüsselte Technologien verwenden, auf die Spur zu kommen? Oder sind diese Möglichkeiten nicht vorgesehen?

Reimann Lukas (V, SG): Diese Möglichkeit ist in der Vorlage enthalten. Es ist aber sehr umstritten, wie diese Möglichkeit funktioniert. Sie kennen die Debatte aus der Kommission: Wo wirkt die Software, wo wirkt sie nicht? Was kann die Software, was kann sie nicht? Das war in der Debatte sehr umstritten.

Leutenegger Oberholzer Susanne (S, BL): Es gibt eine grosse Verwirrung, deswegen stelle ich Ihnen jetzt eine grundsätzliche Frage zum Geltungsbereich der Rahmendatenspeicherung: Teilen Sie meine Auffassung, dass mit der Rahmendatenspeicherung – vielleicht mit Ausnahme der ganz kleinen – sämtliche Kommunikationseinheiten, also Natel, Festnetzanschlüsse und Computeranschlüsse, sowie die Häufigkeit der Kommunikation erfasst werden und dass wir deshalb sagen, es sei eine anlasslose Vorratsdatenspeicherung, d. h. eine ohne strafrechtlichen Verdacht, ohne irgendwelche Anhaltspunkte für eine widerrechtliche Handlung? Teilen Sie diese Auffassung?

Reimann Lukas (V, SG): Diese Auffassung teile ich.

Vogler Karl (CE, OW): Sie haben ja gesagt, mit diesem Gesetz würde die ganze Bevölkerung überwacht. Ist Ihnen bekannt, dass bereits heute die Randdaten gespeichert werden? Was wird denn neu überwacht?

Reimann Lukas (V, SG): Das ist mir bekannt, das habe ich in meinem Votum auch erwähnt. Bereits heute werden die notwendigen Daten, die die Strafverfolger brauchen, erfasst. Was wollen Sie denn mehr? Was braucht es denn zusätzlich, wenn diese Daten bereits erfasst werden? Sie übertreiben in diesem Bereich mit diesen zusätzlichen Massnahmen.

Fischer Roland (GL, LU): Herr Kollege Reimann, Sie haben jetzt breit dargelegt, wie stark Sie gegen eine allgemeine Bespitzelung der Bevölkerung sind und dass deshalb zwei Drittel Ihrer Fraktion das revidierte Büpf – bei dem eine Strafverfolgung für die Überwachung erforderlich ist – ablehnen. Weshalb hat dann die Fraktion das Nachrichtendienstgesetz geschlossen akzeptiert, mit dem wir ohne Verdachtsfälle Kabelaufklärung betreiben und die Leute, ohne irgendwelche Verdachtsmomente zu haben, bespitzeln können? Ist das nicht ein Widerspruch?

Reimann Lukas (V, SG): Es ist genauso ein Widerspruch, wenn Sie das Nachrichtendienstgesetz ablehnen, hingegen dem Büpf zustimmen. Die Gesetze hängen ja in verschiedenen Bereichen zusammen. Der Nachrichtendienst kriegt auch Zugriff auf die Daten, die durch das Büpf erhoben werden. Es gibt aber einen grossen Unterschied zwischen dem Nachrichtendienstgesetz und dem Büpf, und zwar ist das die Anzahl der Fälle. Wir sprechen beim Büpf von mehreren zehntausend Fällen, während wir beim Nachrichtendienst-

gesetz von maximal zehn Fällen pro Jahr sprechen, wie Herr Bundesrat Maurer gesagt hat. Das ist ein grosser Unterschied zwischen den beiden Vorlagen. Es wurde heute oft von Terrorbekämpfung gesprochen – Entschuldigung: Einen Terroranschlag müssen Sie bekämpfen, bevor er passiert ist, und nicht erst dann, wenn der Terrorist tot ist. Dafür ist das Nachrichtendienstgesetz da und nicht das Büpf. Das Büpf kommt erst dann zur Anwendung, wenn der Terroranschlag schon passiert ist und der Terrorist noch lebt, aber entwischt ist.

Sommaruga Simonetta, Bundespräsidentin: Was schlägt Ihnen der Bundesrat mit dieser Vorlage eigentlich ganz genau vor? Es sind im Wesentlichen zwei Neuerungen: Erstens geht es darum, die Randdatenspeicherung, die es heute schon gibt, von sechs Monaten auf zwölf Monate zu erhöhen. Zweitens geht es darum, dass wir die rechtlichen Grundlagen dafür schaffen, dass wir Kommunikation, die verschlüsselt ist, ebenfalls überwachen können – überwachen können in dem Fall, in dem es einen konkreten Verdacht auf eine schwere Straftat gibt. Ist das eine massive Ausweitung der Überwachung?
Herr Nationalrat Reimann hat es gesagt: Jeder Schwerkriminelle wird seine Daten verschlüsseln. Ja, das ist so. Die Polizei hat mir erzählt, wie das heute am Telefon tönt. Schwerkriminelle sagen: «Wir wechseln jetzt auf Skype, denn da kann man uns nicht überwachen.» So einfach ist das. Jetzt gibt es Kräfte in diesem Parlament, die sagen: «Dann lassen wir den Schwerkriminellen diesen geschützten Raum, damit sie in Ruhe kommunizieren können und keine Angst haben müssen, dass sie überwacht werden können, wenn sie verschlüsselt kommunizieren.»
Es geht also bei dieser Vorlage in erster Linie darum, dass wir die Mittel, die es in der Kommunikation gibt und die wir alle brauchen, die wir alle auch geniessen, für die Strafverfolgung im Falle von schwerer Kriminalität so anpassen, dass sie adäquat sind und mit den technologischen Entwicklungen übereinstimmen. Wir reden hier von potenziellen Dschihadisten, wir reden von Terroristen; vorher wurde gesagt, es sei zu spät, wenn der Terrorist schon tot sei. Der Terrorismus wird finanziert von irgendjemandem, und darum geht es in diesem Gesetz auch. Wir sprechen hier von Pädokriminellen, von einem Thema, bei dem Sie gerne heftig sind, vehement sind, das Strafrecht verschärfen, das Tätigkeitsverbot ausweiten. Hier geht es darum, die Mittel dafür zu schaffen, dass diese Pädokriminellen gefunden werden, damit sie nachher bestraft werden können.
Wir reden hier auch von Ermittlungsmethoden, die nur dann eingesetzt werden können, wenn bereits ein Strafverfahren eröffnet worden ist. Dazu muss ich jetzt doch das eine oder andere klarstellen. Verdachtsunabhängige Überwachung ist kein Thema des Büpf, sondern das ist das Thema des Nachrichtendienstgesetzes, das Sie in der letzten Session doch mit beträchtlicher Mehrheit angenommen haben. Ich lese Ihnen gerne aus der Strafprozessordnung vor – einfach damit es gesagt ist, weil Sie vielleicht die Strafprozessordnung heute nicht dabeihaben. Dort ist nämlich ganz konkret festgehalten, in welchen Fällen überhaupt die Überwachung der Telekommunikation möglich ist. Es muss erstens einen dringenden Verdacht geben; es muss eine schwere Straftat sein, und die bisherigen Untersuchungsmethoden müssen erfolglos geblieben sein. Das sind die Voraussetzungen, damit überhaupt die Anwendung einer Überwachungsmethode infrage kommt. Dann muss die Strafverfolgungsbehörde einen Antrag stellen. Dieser muss vom Zwangsmassnahmengericht bewilligt werden. Sprechen Sie von «verdachtsunabhängig» am richtigen Ort, aber beim Büpf ist das kein Thema; diese Aussage ist schlicht und einfach falsch.
Eine Minderheit Ihrer Kommission möchte diese Vorlage zurückweisen – übrigens nicht an die Verwaltung, sondern an den Bundesrat; sie möchte, dass der Bundesrat diese Vorlage noch einmal überarbeitet. Mit dieser Rückweisung verlangt die Minderheit erstens, dass die Randdaten nicht mehr gespeichert werden dürfen. Einige von Ihnen haben es bereits gesagt: Die Randdaten werden heute schon gespeichert, und zwar während sechs Monaten. Das Einzige, was wir hier vorsehen, ist, dass die Randdatenspeicherung auf zwölf Monate verlängert wird. Dazu habe ich heute auch ein paar abenteuerliche Sachen gehört; das muss ich Ihnen sagen. Wer speichert eigentlich diese Randdaten? Es sind die Fernmeldedienstanbieter, die diese Randdaten speichern. Es geht dabei unter anderem um die Frage: Wer hat mit wem wie lange telefoniert? Diese Daten werden von der Swisscom, von Salt, von verschiedensten Fernmeldedienstanbietern gespeichert. Warum tun sie das? Damit sie Ihnen am Ende des Monats eine Rechnung stellen können. Nicht der Staat speichert diese Daten, sondern private Anbieter.
Was wir in diesem Gesetz regeln, ist die Frage, unter welchen Voraussetzungen die Strafverfolgungsbehörde das Recht hat, diese Randdaten zu überwachen respektive einzuholen, um bei Verdacht auf eine schwere kriminelle Handlung die Möglichkeit zu haben, den Täter zu finden; darum geht es in diesem Gesetz. Hören Sie also auf zu sagen, der Staat würde hier Daten speichern – es sind die Privaten, die das tun. Denjenigen, die sich darüber ärgern und die es stört, dass ihre Daten gespeichert werden, möchte ich vielleicht sagen: Ja, machen Sie den Vorschlag, dass die Fernmeldedienstanbieter diese Daten auch nicht mehr speichern dürfen! Oder stört es Sie nicht, wenn ausgerechnet private, kommerzielle Unternehmen Ihre sensiblen Daten speichern? Also ich bitte Sie, hier diese Unterscheidung zu machen.
Warum wollen wir diese Erhöhung von heute sechs auf neu zwölf Monate bei der Randdatenspeicherung? Weil die Erfahrung gezeigt hat, dass es bei der Ermittlung von Straftaten oft eine gewisse Zeit braucht! Damit diese Zeit auch vorhanden ist, zum Beispiel wenn es um Rechtshilfeersuchen, um komplexe Fälle geht, möchten wir eine Erhöhung auf zwölf Monate. Sie haben ja gesehen, dass zuerst auch anders ermittelt werden muss. Diese Daten können erst angefordert werden, wenn es sich gezeigt hat, dass andere Ermittlungsmethoden nicht zum Resultat geführt haben. Dann kann es eben sein, dass diese sechs Monate nicht reichen, und deshalb möchten wir diese Zugriffsmöglichkeiten auf zwölf Monate erhöhen.
Wenn es Sie dermassen stört, dass der Staat, die Strafverfolgungsbehörde während zwölf Monaten auf diese Daten zurückgreifen kann: Stört es Sie dann nicht, wenn Private diese Daten während zehn Jahren speichern? Darüber sprechen wir! Die Banken speichern übrigens jede Ihrer Bankbewegungen während zehn Jahren, und das sind bekanntlich ja auch sensible Daten. Stört Sie das nicht? Und wenn es eine Strafverfolgung gibt, hat die Strafverfolgungsbehörde Zugriff auf diese Daten. Bei einem Strafverfahren gibt es die Herausgabepflicht; es gibt die Editionspflicht. Wenn Sie also bezüglich Ihrer Randdaten in der Telekommunikation sensibel sind, müssten Sie doch auch sensibel sein, wenn es um Ihre Bankbewegungen geht. Ich bitte Sie einfach, hier diese Unterscheidung zu machen. Wir sprechen von schweren Straftaten, wir sprechen von eröffneten Strafverfahren, und nach der Bewilligung durch das Zwangsmassnahmengericht ist die Möglichkeit vorhanden, dass auf diese Daten zurückgegriffen wird.
Ich sage Ihnen noch, welche Folgen ein Verzicht auf die Erhebung von Randdaten haben kann. Der Verzicht darauf würde bedeuten, dass Sie dann in einem Strafverfahren oder eben auch im Falle einer Kindesentführung – ja, das gibt es leider auch in unserem Land – die Möglichkeit nicht mehr haben, auf die Randdaten zurückzugreifen. Den Zugriff auf die Randdaten haben wir ja auch hierfür vorgesehen. Ich möchte dann das nächste Mal, wenn ein Kind entführt wird, sehen, wenn man sagt, leider habe das Parlament entschieden, dass man nicht auf diese Randdaten zurückgreifen kann; man habe deshalb diese Möglichkeit leider nicht zur Verfügung, obwohl vielleicht gerade solche Daten helfen könnten, ein entführtes Kind zu finden.
Es gibt aber noch eine weitere Folge der Entscheidung, die Randdatenspeicherung nicht mehr zu ermöglichen respektive den Zugriff für die Strafverfolgungsbehörden zu verwei-

gern. Wenn ein Verurteilter aus dem Gefängnis entweicht, suchen wir ihn mit allen Mitteln. Dann kann der Zugriff auf diese Randdaten ebenfalls dazu dienen, den entwichenen, verurteilten Straftäter zu finden. Wenn Sie die Randdatenspeicherung, hier den Zugriff auf die Randdatenspeicherung, verweigern, haben Sie in diesem Fall die erwähnte Möglichkeit nicht.
Ich komme noch zum Entscheid des Europäischen Gerichtshofes, der hier immer wieder zitiert worden ist. Ich sage Folgendes dazu: Dieser Entscheid, der jetzt offenbar die höchste aller Massnahmen und Entscheide ist, sagt nicht, dass die Randdatenspeicherung generell unzulässig sei. Der Entscheid des Europäischen Gerichtshofes verlangt jedoch, dass es eine konkrete rechtliche Grundlage braucht. Diese schaffen wir in diesem Gesetz. Wir schaffen Klarheit, wer unter welchen Voraussetzungen auf diese Daten zugreifen kann. Genau das ist in dieser Vorlage geregelt. Es sind eben die Strafverfolgungsbehörden, es ist nicht irgendwer, der darauf zugreifen kann, und zwar – wie ich es bereits gesagt habe – erst nach dem Entscheid eines Gerichtes, das eine solche Massnahme bewilligen muss.
Ich sage Ihnen mal, wer heute in Europa eine solche Vorratsdatenspeicherung hat und wie lange sie dauert: Belgien ein Jahr, Dänemark ein Jahr, Finnland ein Jahr, Frankreich ein Jahr, Italien bis zu zwei Jahre, Niederlande ein Jahr, Portugal ein Jahr, Spanien und Grossbritannien ein Jahr. Deutschland ist daran, diese Frage ebenfalls zu regeln, Österreich ebenfalls. Der Europäische Gerichtshof hat verlangt, dass die Voraussetzungen geklärt sein müssen, dass sie restriktiv sein müssen und dass sie gesetzlich geregelt sein müssen – genau das, was Sie heute beschliessen können.
Im Übrigen sieht auch die Cybercrime-Konvention des Europarates einen Minimalstandard vor, nämlich dass die verfügbaren Randdaten für Zwecke der Strafverfolgung beigezogen werden können, weil das bei der Bekämpfung von Cyberkriminalität etwas Wichtiges für die Strafverfolgungsbehörden ist.
Noch etwas zum Persönlichkeitsschutz: Wir haben in diesem Gesetz dem Persönlichkeitsschutz grosse Bedeutung beigemessen. So muss die überwachte Person über die Überwachung informiert werden. Damit verhindern wir, dass die Strafverfolgungsbehörden einfach möglichst oft und breit überwachen lassen, weil sie wissen, dass ihre Massnahmen nicht nur vor einem Gericht bestehen müssen, sondern allenfalls auch von der betroffenen Person beurteilt werden.
Ich komme jetzt noch zu einem zweiten Punkt des Rückweisungsantrages, den ich, das muss ich Ihnen sagen, ebenfalls schwer nachvollziehen kann. Es wurde bereits gesagt: In der letzten Session haben Sie mit 119 zu 65 Stimmen das Nachrichtendienstgesetz angenommen. Sie haben damit entschieden, dass der Nachrichtendienst in Zukunft präventiv mit den sogenannten Staatstrojanern in Computer eindringen kann, um zum Beispiel – Sie haben das gesagt – potenziellen Dschihadisten auf die Spur zu kommen. Heute entscheiden Sie, ob die Strafverfolgungsbehörden, falls sich der Verdacht des Nachrichtendienstes bestätigt hat, ihre Arbeit überhaupt aufnehmen können, um diese potenziellen Täter dann auch vor Gericht bringen zu können. Der Nachrichtendienst kann nicht vor Gericht gehen. Dazu braucht es eine Strafverfolgungsbehörde, dazu braucht es einen Staatsanwalt. Da müssen Sie doch den Strafverfolgungsbehörden die gleichen Instrumente in die Hand geben, die Sie vorher dem Nachrichtendienst in die Hand gegeben haben, sonst kommt es so weit, dass die Strafverfolgungsbehörde die entsprechenden Beweismittel nicht hat. Stellen Sie sich das einmal vor! Da entdeckt der Nachrichtendienst einen potenziellen Täter. Das Gericht muss den Täter laufen lassen, weil die Strafverfolgungsbehörde die Beweismittel nicht beibringen konnte. Stellen Sie sich einmal eine solche Absurdität vor! Das sind die Folgen, wenn Sie heute im Büpf den Einsatz der Govware ablehnen.
Ich sage gerne noch etwas zu den Staatstrojanern. Ohne sie hat die Strafverfolgung keinen Zugriff auf die verschlüsselte Kommunikation. Das heisst ganz simpel und einfach, Kriminelle, Schwerverbrecher, Pädokriminelle, Dschihadisten, Drogenbosse können sicher sein, dass es keine Überwachungsmöglichkeit gibt, wenn sie über die verschlüsselte Kommunikation kommunizieren. Diese verschlüsselte Kommunikation ist nicht irgendetwas, was nur wenige kennen. Sie alle in diesem Saal, kommunizieren vermutlich auch verschlüsselt, indem Sie nämlich Skype verwenden, indem Sie Whatsapp verwenden, indem Sie mit Ihrem i-Phone über Facetime telefonieren. Das heisst, ohne diese Staatstrojaner gibt es keinen Zugang der Strafverfolgungsbehörden zu dieser Kommunikation. Das ist eigentlich eine Einladung an die Kriminellen, sich auf diesen Kanälen auszutauschen.
Ich möchte noch etwas zu den Staatstrojanern sagen. Sie wurden in unserem Land schon mehrmals angewendet, mit der Genehmigung des zuständigen Zwangsmassnahmengerichtes. Man kann sich darüber streiten, ob es heute schon eine gesetzliche Grundlage für die Verwendung von Govware durch die Strafverfolgungsbehörde gibt. Der Vorschlag des Bundesrates enthält aber nicht nur eine explizite rechtliche Grundlage für die Verwendung von Govware, sondern auch die entsprechenden Bestimmungen und, damit verbunden, enge Schranken. Es wird also der Tatsache Rechnung getragen, dass die Überwachung mittels Govware besonders sensibel ist. Ich würde eigentlich sagen: All diejenigen unter Ihnen, die hier sehr kritisch sind, müssen doch ein Interesse daran haben, dass jetzt in diesem Gesetz die rechtlichen Schranken gesetzt werden. Sie sind eng, die rechtlichen Schranken. Und Sie müssten auch ein Interesse daran haben, dass dieser Schwebezustand – ob die Govware dann halt angewendet wird, je nach Ansicht, ob dafür die gesetzlichen Grundlagen bestehen oder nicht –, dass diese Unsicherheit beseitigt wird, indem Sie, der Gesetzgeber, sagen, was gemacht werden darf und was nicht.
Ich komme zum Schluss. Der Antrag auf Nichteintreten ist zurückgezogen worden. Der Rückweisungsantrag besteht nach wie vor. Ich sage es Ihnen noch einmal, in aller Deutlichkeit: Wenn Sie auf die Vorratsdatenspeicherung verzichten wollen, wie das die Kommissionsminderheit will, dann verzichten Sie darauf, dass die Strafverfolgungsbehörden überhaupt die Möglichkeit haben, Straftätern auf die Spur zu kommen. Und ich sage all denjenigen, die dem Nachrichtendienstgesetz zugestimmt haben – es sind auch hier viele –, noch einmal: Wenn Sie hier dem Rückweisungsantrag zustimmen, dann ist das, was Sie beim Nachrichtendienstgesetz beschlossen haben, nämlich der Zugriff auf die Randdaten, auch weg; dann können Sie beim Nachrichtendienstgesetz die präventive Überwachung auch vergessen, da Sie im Nachrichtendienstgesetz explizit auf das Büpf verwiesen haben. Passen Sie also auf! Wenn Sie dem Nachrichtendienstgesetz zugestimmt haben und jetzt den Rückweisungsantrag unterstützen, torpedieren Sie das, was Sie beim Nachrichtendienstgesetz unterstützt haben.
Ich bitte Sie, auf die Vorlage einzutreten und den Rückweisungsantrag abzulehnen. Wenn Sie Feinkorrekturen machen wollen, weil Sie mit gewissen Dingen nicht einverstanden sind, dann tun Sie das in der Detailberatung – dort haben Sie die Möglichkeit dazu.

Leutenegger Oberholzer Susanne (S, BL): Frau Bundespräsidentin, Sie haben mich gefragt, ob es mich nicht störe, dass private Unternehmungen meine Rahmendaten speichern würden. Frau Bundespräsidentin, es stört mich sehr. Es stört mich genau so, wie es mich gestört hat, dass ich – wie 900 000 Bürgerinnen und Bürger – fichiert worden bin. Ich frage Sie jetzt: Haben Sie zur Kenntnis genommen, dass der Rückweisungsantrag genau den Verzicht auf die Rahmendatenspeicherung verlangt? Deswegen unterstütze ich den Rückweisungsantrag – weil die Rahmendatenspeicherung wesentlich in meine Grundrechte eingreift, weil sie eben anlasslos erfolgt, ohne Verdacht auf eine Straftat.

Sommaruga Simonetta, Bundespräsidentin: Vielen Dank, Frau Leutenegger Oberholzer! Das ist eine sehr wichtige Frage, weil ich damit auch noch etwas klären kann. Wenn es Sie stört, dass die privaten Fernmeldedienstanbieter Ihre

Daten speichern, wenn Sie das nicht mehr wollen, dann müssen Sie das ins Fernmeldegesetz schreiben und nicht ins Büpf. Dann müssen Sie nicht im Büpf sagen, dass die Strafverfolgungsbehörde nicht mehr auf diese Daten zugreifen können; dann müssen Sie das Fernmeldegesetz ändern. Ich vermute einfach, dass in der Minderheit, die hier für die Rückweisung eintritt, nicht ganz alle der Meinung sind, dass im Fernmeldegesetz den Fernmeldedienstanbietern verboten werden muss, ihre Daten zu speichern – ich müsste dann auch noch fragen, wie sie denn Rechnung stellen sollen.
Zu dem, was Sie über die Fichierung sagen, Frau Leutenegger Oberholzer: Damals hat der Staat Daten gesammelt, nicht die Privaten! Hier geht es um die Strafverfolgung. Es geht darum, dass man, wenn ein Strafverfahren eröffnet worden ist, auf Daten Zugriff hat, die bereits gesammelt worden sind. Bei der Fichierung gab es aber keine Strafverfahren – das war ja das Problem bei der Fichenaffäre! –, sondern damals wurden Leute fichiert, obwohl eben keine Strafverfahren gegen sie eröffnet worden waren.

Wasserfallen Christian (RL, BE): Frau Bundesrätin, ich bin ja auch der Meinung, dass man den Strafverfolgungsbehörden im Online-Zeitalter solche Mittel in die Hände geben muss. Es darf auch nicht sein, dass der Datenschutz zum Täterschutz wird.
Wenn der Gesetzgeber bestimmt, mit welchen Daten und wie die Rand- und Vorratsdatenspeicherung erfolgen soll, und wenn diese Aufgaben von Privaten ausgeführt werden, stellt sich aber schon noch eine Frage: Teilen Sie nicht die Meinung, dass die Kosten durch den Bund statt von den Privaten getragen werden müssen, wenn solche hoheitlichen Aufgaben auf die Privaten zukommen?

Sommaruga Simonetta, Bundespräsidentin: Vielen Dank, Herr Wasserfallen, Sie sprechen die Kosten an. Das ist ein sehr interessantes Thema. Wir werden uns darüber in der Detailberatung sicher noch unterhalten können. Ich habe auch gelesen, es würden mit dieser Vorlage 120 Firmen in den Ruin getrieben. Ich muss Ihnen sagen: Das ist schlicht und einfach falsch. Sie sehen dann bei den entsprechenden Gesetzesartikeln, dass bei vielen Anbietern, gerade bei den kleinen, nur eine Duldungspflicht besteht. Das heisst, sie müssen dulden, dass man auf die Daten zugreift. Es kostet sie nichts, sie müssen auch die Infrastruktur nicht selber zur Verfügung stellen und aufbereiten.
Noch etwas zu den Kosten: Die Kommission des Ständerates und auch Ihre Kommission haben die Anbieter angehört und ihnen gesagt, sie sollten einmal die Kosten aufzeigen. Schauen Sie einmal nach, was in den Hearings herausgekommen ist. Leider ist es nicht gelungen, die Kosten – die sehr hohen Kosten, wie jetzt zum Teil behauptet wird – auch nur annäherungsweise nachzuweisen.
Zur Kostenverteilung erarbeiten wir ja eine Verordnung, und wir haben Ihnen gesagt, wie wir das tun werden: Wir werden die Kosten so aufteilen wie bis heute, das heisst, es gibt für niemanden zusätzliche grosse Kostenblöcke.

Schwander Pirmin (V, SZ): Frau Bundespräsidentin, Sie haben gesagt, die Banken würden ihre hochsensiblen Bankkundendaten auch zehn Jahre lang aufbewahren. Meine Frage: Haben die Banken heute keine gesetzliche Verpflichtung mehr, ihre Daten zehn Jahre lang aufzubewahren?

Sommaruga Simonetta, Bundespräsidentin: Schauen Sie, Herr Schwander: Hier sprechen wir nicht davon, wie lange jemand die Daten aufbewahren muss, sondern davon, wie lange der Zugriff für die Strafverfolgungsbehörden garantiert werden muss. Darum geht es. Heute müssen die Fernmeldedienstanbieter während sechs Monaten garantieren, dass ein Zugriff möglich ist; deshalb müssen sie die Daten so lange aufbewahren. Neu müssen sie sie zwölf Monate aufbewahren. Ich kann Ihnen aber sagen, dass die Fernmeldedienstanbieter die Daten heute länger aufbewahren; dies wegen der Telefonrechnungen, bei welchen es manchmal Reklamationen gibt. Bei den Banken ist im Bankengesetz geregelt, wie lange sie Daten aufbewahren müssen; das regeln wir nicht hier. Die Banken müssen die Daten ohnehin herausgeben. Sie kennen die Editionspflicht in der Strafprozessordnung: Die Banken müssen diese Daten herausgeben, unabhängig davon, ob sie das wollen oder nicht.

Keller Peter (V, NW): Frau Bundesrätin, Sie halten hier ein Plädoyer für mehr Mittel und Möglichkeiten für die Strafverfolgung, was man auf der einen Seite absolut auch nachvollziehen kann. Auf der anderen Seite wären Sie glaubwürdiger, wenn Sie als Justizministerin auch durch Ihre eigene Arbeit überzeugen würden. Sie sprechen hier von Pädokriminellen, Drogenbaronen, Kindesentführern, Dschihadisten, Schwerkriminellen usw. Wie sieht es dann nachher aus, wenn diese Leute gefasst sind, wenn es um den Strafvollzug geht? Wie sieht es aus, wenn es um die Umsetzung von Volksinitiativen geht, die genau die Bestrafung dieser Leute wollen – wenn es um die Unverjährbarkeit geht, wenn es um die Verwahrung geht, wenn es um ein Berufsverbot für verurteilte Pädophile geht und wenn es um die Ausschaffung von kriminellen Ausländern geht? Wo bleiben Ihr Job und Ihre Verantwortung?

Sommaruga Simonetta, Bundespräsidentin: Was war genau Ihre Frage? *(Teilweise Heiterkeit)*

Schwaab Jean Christophe (S, VD), pour la commission: Il y a eu certaines inexactitudes dans ce qui a été dit précédemment, ce qui montre que certains n'ont pas toujours mené une étude attentive, tant du projet de loi qui nous est soumis que du message y relatif.
Monsieur Glättli a dit tout d'abord, à propos des données secondaires, que la Confédération stockait ces données. Non, Monsieur Glättli, la Confédération ne stocke pas les données, ni même les autorités de poursuite pénale d'ailleurs, qui ne font que demander à un juge l'autorisation de recevoir certaines données au cas où il y aurait un soupçon concret d'un crime grave. Ce n'est pas l'Etat qui stocke les données, ce sont les opérateurs, cela a été dit.
Une autre erreur fréquemment entendue, c'est le jugement de la Cour de justice de l'Union européenne qui aurait interdit la collecte des données secondaires. Là encore, c'est inexact de le prétendre. Cette cour n'a pas interdit en principe l'usage et la conservation des données secondaires. Elle a annulé une directive européenne qui ne respectait pas le principe de proportionnalité, mais elle n'a jamais dit que par principe la conservation des données secondaires était contraire aux principes constitutionnels. Pour la Suisse, il y a une décision sur laquelle nous aurons peut-être l'occasion de revenir. Certes, ce n'est qu'une décision du Service «Surveillance de la correspondance par poste et télécommunication», qui n'a pas encore été validée par le Tribunal administratif fédéral, ni même par le Tribunal fédéral. Mais, en Suisse, une instance judiciaire s'est posé la question de la constitutionnalité de l'actuelle possibilité de sauvegarder les données secondaires, et sa réponse est: «Oui, c'est conforme à la Constitution.»
La dernière erreur entendue lors des débats est de Monsieur Reimann qui a prétendu que les chevaux de Troie seraient utilisés pour modifier le contenu des ordinateurs, pour mener des perquisitions en ligne. Alors il est vrai qu'en principe c'est possible, et cela la commission ne le nie pas. Mais si on lit le texte de loi, soit l'article 269bis du Code de procédure pénale, on constate que les programmes informatiques spéciaux ne peuvent pas être utilisés pour ce genre de choses, mais uniquement pour surveiller une télécommunication, donc ni pour mener une perquisition en ligne, ni pour aller modifier ce qui se trouverait à l'intérieur du disque dur, ni pour créer des portes dérobées à l'intérieur des logiciels visés. Cela est garanti par le nouvel article 269quater alinéa 1 proposé à l'unanimité par la commission, qui prévoit que seuls les «programmes informatiques spéciaux qui génèrent un procès-verbal complet» puissent être utilisés afin

que l'on puisse vérifier que le cheval de Troie a seulement surveillé une télécommunication et n'a rien fait d'autre.
J'en viens maintenant à la proposition de renvoi de la minorité Vischer Daniel. Je pense qu'il vaut la peine de relire attentivement cette proposition de renvoi dont le but est le renvoi du projet non pas à l'administration comme cela a été dit, mais au Conseil fédéral, ce qui lui confère une portée tout de même un petit peu plus importante.
La demande vise à un renvoi au Conseil fédéral pour recommencer les travaux qui ont déjà été faits sur deux points. Le premier point consiste à ne plus prévoir la possibilité de conserver des données secondaires. Cette position est tout ce qu'il y a de plus légitime, c'est un débat que nous devons mener et que nous allons d'ailleurs mener. Mais pourquoi demander au Conseil fédéral de recommencer les travaux sur ce point? Celles et ceux qui ne souhaitent pas que soit prévue la conservation des données secondaires n'ont pas besoin d'attendre que le Conseil fédéral revienne à la charge, puisqu'il suffit d'accepter – certes ce n'est pas ce que va vous recommander la commission – les propositions de minorité IV et V (Vischer Daniel) aux articles 19 et 26. Il ne s'agit que de votes, c'est vite fait, c'est facile et cela évite de recommencer les travaux de zéro.
Le second point visé par la proposition de renvoi au Conseil fédéral concerne l'obtention de garanties supplémentaires sur l'emploi des chevaux de Troie. Là encore, à mon avis et de l'avis de la majorité de la commission, il n'est pas nécessaire que le Conseil fédéral recommence à zéro des travaux qui ont été menés en commission. La commission vous propose l'introduction de l'article 269quater du Code de procédure pénale, article non contesté qui contient justement les garanties demandées par Monsieur Vischer. Ce dernier, d'ailleurs, ne s'y oppose pas puisqu'il a accepté la proposition de la commission qui, en l'espèce, a pris sa décision à l'unanimité.
Reste la question de l'exploitation des preuves qui auraient été obtenues frauduleusement par un usage interdit des chevaux de Troie. Je vous demande ici de considérer l'article 141 alinéa 2 du Code de procédure pénale en vigueur qui répond justement à cette question, puisqu'il y est écrit que «les preuves qui ont été administrées d'une manière illicite ou en violation de règles de validité par les autorités pénales ne sont pas exploitables, à moins que leur exploitation soit indispensable pour élucider des infractions graves». «Ne sont pas exploitables»: je crois que ces quatre mots sont absolument capitaux. Ce que demande la minorité Vischer Daniel par sa proposition de renvoi, c'est que le Conseil fédéral planche à nouveau sur quelque chose qui existe déjà dans la législation. Et même si ce quelque chose ne devait pas convenir au conseil, il aurait toujours la possibilité, sans passer par la case renvoi, d'accepter la proposition de la minorité Vischer Daniel à l'article 269quater.
Je vous invite à rejeter la proposition de renvoi au Conseil fédéral, comme le suggère la majorité de la commission.

Flach Beat (GL, AG), für die Kommission: Der Rückweisungsantrag Vischer Daniel lag der Kommission vor. Wir haben sehr lange, an mehreren Sitzungen, über all diese Fragen diskutiert. Ich möchte Sie bitten, diesen Rückweisungsantrag abzulehnen, wie das auch die Kommission gemacht hat; die Kommission hat den Antrag im Übrigen mit 16 zu 9 Stimmen abgelehnt.
Worum geht es? Es geht nicht einzig darum, dass man hier ein neues Konzept machen soll. Vielmehr müssen Sie sich im Klaren darüber sein, dass Sie mit dem Rückweisungsantrag eine Sammlung an Aufträgen übernehmen. Der Rückweisungsantrag beantragt nicht nur, dass es keine Vorratsdatenspeicherung mehr geben soll, sondern auch, dass der Imsi-Catcher und die sogenannte Government Software nur noch bei schweren Gewaltverbrechen eingesetzt werden können.
Sie haben es vorhin gehört, auch Frau Bundespräsidentin hat es ausgeführt: Die Rückweisung hätte zur Folge, dass sehr viele Delikte dann nicht mehr erfasst wären. Es gibt im Strafgesetzbuch ja keinen Deliktekatalog für besonders schwere Gewaltverbrechen. Das Bundesamt für Statistik unterscheidet bei all diesen vielen Delikten zwischen Raub, Vergewaltigung, Geiselnahme usw., die alle zu diesen schweren Gewaltverbrechen gehören. Doch was gehörte dann nicht mehr zu dieser Gruppe? Es wären beispielsweise das Verbreiten von Falschgeld oder die Flucht nicht dabei – wir haben es gehört –; das Verbreiten von Kinderpornografie, Cyberkriminalität, auch schwere Fälle von Betrug würden nicht dazugehören.
Damit komme ich auch gleich auf die Randdatenspeicherung zu sprechen. Wenn Sie auf die Randdatenspeicherung verzichten – ich erinnere daran, dass wir sie heute haben, und zwar für sechs Monate –, dann verliert die Strafverfolgungsbehörde ein sehr, sehr wichtiges Instrument. Es wurde ausgeführt, dass das gar nicht so wichtig und für die Strafverfolgung von wenig Belang sei. Das ist nicht so. Es gibt schliesslich nicht nur die schweren Fälle, sondern auch ganz Profanes. Da müssen Sie mir schon erklären, weshalb Sie diese nicht verfolgen wollen. Die Staatsanwaltschaften haben uns verschiedene Fälle vorgestellt: Ich erinnere beispielsweise an die Bande der Enkeltrickbetrüger, welche alte Frauen abgezockt hat. Da hat irgendeine Person an der Türe einer alten Frau geklingelt und behauptet, er sei im Namen ihres Enkels gekommen, um das Geld abzuholen, das der Enkel leider nicht persönlich abholen könne, worauf die alte Frau mit dem Betrüger zur Bank gegangen ist. Wenn man diese Person dann befragt hat, hat sie gesagt, dass sie nichts mit der Sache zu tun habe und nur gebeten worden sei, das Geld abzuholen. Wenn man über die Randdaten verfügt, kann man feststellen, dass die Verdächtigen sehr wohl miteinander in Kontakt gestanden sind, sodass man den Fall aufklären kann.
Dann muss ich noch etwas anderes sagen: Diese Randdaten dienen nicht nur dazu, jemanden, der in einem Strafverfahren angeklagt ist, zu überführen – dazu braucht es viele kleine Indizien –, sondern sie können auch helfen, jemanden zu entlasten. Stellen Sie sich vor, Sie haben einen schweren Autounfall, und zwei oder drei Monate später taucht ein Zeuge auf, der sagt: Ich habe Sie gesehen, Sie waren am Telefonieren, als der Unfall passierte. Sie können dann schon behaupten, Sie hätten nicht telefoniert; vielleicht sind Sie dann aber wirklich froh, wenn Sie auf solche Randdaten zurückgreifen und belegen können, dass zumindest mit Ihrem Handy zu jenem Zeitpunkt nicht telefoniert wurde.
Die ganze Diskussion kommt mir ein klein wenig vor, als spiele sie sich hundert Jahre früher ab, als hätten wir gerade die Einführung des Automobils erlebt und würden nun sagen: Jetzt haben zwar auch Verbrecher Autos, aber der Polizei geben wir keine, um die Verbrecher zu verfolgen, denn diese sind sowieso zu schlau und zu schnell; wir verzichten darauf, die Polizei soll weiterhin mit Pferden auf Verbrecherjagd gehen.
Noch eine Bemerkung betreffend Staatstrojaner: Im Rückweisungsantrag wird gefordert, dass Staatstrojaner sicher sein müssen, dass Sicherheitsmassnahmen zu treffen sind und dass die erhobenen Daten nicht für andere Zwecke gebraucht werden. Wir sind hier im Strafprozessrecht; es gibt in der Strafprozessordnung ganz klare Regeln, wie man mit sogenannten Zufallsfunden umzugehen hat. Das gilt hier ebenso wie an andern Orten. Es ist ganz klar, dass es hier nicht um ein Ausschnüffeln irgendwelcher Leute geht, gegen die kein Verdacht besteht. Es geht darum, in einem eröffneten Strafverfahren nach der Genehmigung durch ein Strafmassnahmengericht eine Government Software einzuführen.
Herr Vischer hat ausgeführt, dass in der Kommissionsberatung nicht klar herausgekommen sei, wie es dann funktioniere. Es ist tatsächlich so, dass wir hier ein Gesetz machen, das nicht nur auf den Status quo zielt, sondern auch in die Zukunft gerichtet ist. Die digitale Kommunikation und die digitale Welt sind eine Realität. Ich habe mir in den vergangenen Wochen einen Spass daraus gemacht, im Umfeld und bei Kollegen zu schauen, was für kleine Apps sie auf ihren Handys haben und welche Funktionen sie diesen zugestehen. Ich kann Ihnen sagen, dass es auch in diesem Saal

Leute gibt, die auf ihrem Handy kleine Spiele installiert haben und diesen Spielen in den Einstellungen den vollen Zugriff auf die Kamera und auf ihre Position erlauben. Ich habe keine Ahnung, weshalb das einem Staatsanwalt verwehrt sein soll, wenn er in einem Strafverfahren ermitteln will, in dem klar ein schweres Verbrechen vorliegt.
Ich bitte Sie namens der Kommission, auf die Vorlage einzutreten und den Rückweisungsantrag abzulehnen.

Le président (Rossini Stéphane, président): La proposition de non-entrée en matière de la minorité Vischer Daniel a été retirée.

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

Le président (Rossini Stéphane, président): Nous votons maintenant sur la proposition de renvoi de la minorité Vischer Daniel.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 092)
Für den Antrag der Minderheit ... 50 Stimmen
Dagegen ... 128 Stimmen
(7 Enthaltungen)

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
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Titre et préambule
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Le président (Rossini Stéphane, président): La discussion par article a été divisée en trois blocs. Un document présentant la composition des blocs et fournissant les indications utiles sur le déroulement des débats vous a été distribué.

Block 1 – Bloc 1
Randdaten
Données secondaires

Reimann Lukas (V, SG): Ich muss mich wirklich kurzhalten – fünf Minuten für viele Minderheitsanträge.
Bei Artikel 2 Buchstabe c geht es um eine Ausweitung des Geltungsbereichs auf sogenannte Anbieter abgeleiteter Kommunikationsdienste. Das würde heissen, dass sich Tausende von kleinen Anbietern von Internetdiensten, die auch nur einen Mailserver für ein paar Freunde oder ein Forum für den lokalen Handballverein betreiben, zum verlängerten Arm der Strafverfolgungsbehörden würden und das Ganze mitmachen müssten. Aufgrund des Territorialitätsprinzips kann das Gesetz allerdings genau jene ausländischen Anbieter nicht umfassen, die heute diese Märkte dominieren und den grössten Teil der entsprechenden Kommunikation übermitteln, wie GMX, Skype, Whatsapp, i-Message und weitere. Damit ist die massive Ausdehnung des Geltungsbereiches auf ganz kleine Anbieter schlicht unnütz, weil der grösste Teil sowieso über ausländische Anbieter läuft.
Bei Artikel 8 Buchstabe b geht es darum, dass die technischen Merkmale der Randdaten ausgedehnt werden. Neu sollen auch Verbindungsversuche als Randdaten erhoben werden. Das wird heute von den Telekommunikationsanbietern nicht gemacht; es würde Millionen kosten, um diese Daten zusätzlich zu erheben. Das bringt keinen Mehrwert für die Strafverfolgungsbehörden, aber ganz viele Kosten für die Wirtschaft und das Gewerbe, was in diesem Sinne nichts bringt.
Bei Artikel 26, den Pflichten der Anbieter von Fernmeldediensten, sind wir der Meinung, dass eine präventive Überwachung sämtlicher Bewohner durch Erhebung und Speicherung der Kommunikations- und Lokationsdaten mit einem Rechtsstaat nicht vereinbar ist. Es wurde vorhin schon bei der Eintretensdebatte auf die Studie des Max-Planck-Instituts verwiesen, welche übrigens im Auftrag des deutschen Bundesamtes für Justiz ausgestellt wurde und nicht, beispielsweise, im Auftrag der Piratenpartei. Es ist nicht nachgewiesen, dass die Vorratsdatenspeicherung einen grossen Mehrwert für die Strafverfolgungsbehörden bringt. Deshalb sind wir der Meinung, dass das geändert werden muss, beispielsweise mit dem Quick-Freeze-Verfahren.
Von Frau Bundespräsidentin Sommaruga wurde auf Deutschland und Österreich verwiesen. In Deutschland hat etwa die FDP-Justizministerin und in Österreich haben sogar sämtliche Parteien in einem gemeinsamen Ausschussverfahren vorgeschlagen, man solle doch zu diesem Quick-Freeze-Verfahren übergehen.
Zu Artikel 27, den Pflichten der Anbieter abgeleiteter Kommunikationsdienste: Hier ist eine Einschränkung auf eine Auskunftspflicht betreffend die bereits vorhandenen Randdaten beantragt. Das Dulden von darüberhinausgehender aktiver Überwachung würde bedeuten, kurzfristig und ohne sorgfältige Test- oder Sicherheitsanalysen Änderungen an laufenden Systemen vorzunehmen, die darum die Sicherheit und die Stabilität des angebotenen abgeleiteten Kommunikationsdienstes gefährden. Die Schweiz darf nicht als Standort für die Erbringung von geschäftskritischen Dienstleistungen ungeeignet gemacht werden. Gerade heute ist die Schweiz ein Standort für die Informatik, wegen ihrer Informatiksicherheit und ihrer Sicherheit vor Überwachung. Das darf nicht dazu führen, dass der Standort Schweiz in dieser Zukunftsbranche geschwächt wird.
Es sollen nur Unternehmen für eine Auskunft herbeigezogen werden können, die eine wirtschaftliche Bedeutung haben und zugleich viele User haben. Von den Pflichten ausnehmen möchten wir Privatpersonen und nichtkommerzielle Vereine sowie die Hotels, die Gastronomie, Spitäler, Schulen, Bibliotheken usw. Wenn jedes Restaurant und jedes Hotel, das seinen Gästen z. B. den kostenlosen Internetzugang anbietet, auch erfasst wird, dann führt das zu enormen Kosten für die Anbieter, für die Gastronomie, für den Tourismus und bringt für die Strafverfolgung wenig.
In diesem Sinne sind das Anträge, die das Kosten-Nutzenverhältnis, das von uns bemängelt worden ist, etwas verbessern möchten und die die Anbieter von zusätzlichen Massnahmen, von zusätzlichen Kosten und zusätzlicher Bürokratie befreien möchten.

Leutenegger Oberholzer Susanne (S, BL): Die Minderheit I verlangt bei Artikel 19 Absatz 4, dass die Randdaten des Postverkehrs maximal während sechs Monaten aufbewahrt werden müssen. Das entspricht dem Beschluss des Ständerates. Es handelt sich hier um ganz wenige Fälle. Bereits die sechs Monate sind, wenn man sich die Fallzahlen vor Augen führt, an der Grenze der Verhältnismässigkeit. Es handelt sich hier vor allem um Postsachen mit Zustellnachweis, z. B. die LSI-Zustellungen. Es macht aber weder sicherheitstechnisch noch ökonomisch Sinn, eine längere Aufbewahrungsfrist zu verlangen.
Ich bitte Sie deshalb – für den Fall, dass die Aufbewahrung nicht generell gestrichen wird –, mit der Minderheit die Verhältnismässigkeit zu wahren und mit dem Ständerat auf sechs Monate zurückzugehen; das genügt.

Schneider Schüttel Ursula (S, FR): Ich spreche zuerst zu meinem Minderheitsantrag zu Artikel 19 Absatz 4, zu Artikel 26 Absatz 5 und zu Artikel 39 Absatz 1 Buchstabe b

Büpf. Der Antrag bezweckt die Löschung der Daten nach Ablauf der in den gleichen Artikeln geregelten Aufbewahrungsfrist.
In der Kommission hat uns der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, Herr Hanspeter Thür, erklärt, dass von den Grundsätzen des Datenschutzrechts zur Datenminimierung her die Löschung vorgenommen werden müsse, wenn kein entsprechender Zweck mehr bestehe. Nach seiner Ansicht ist die Löschung dann zu machen, wenn ein Fernmeldedienstanbieter nach bezahlter und akzeptierter Rechnung keine Gründe mehr hat, diese Randdaten aufzubewahren.
Ich habe in diesem Zusammenhang auch den Bundesgerichtsentscheid 139 IV 98 studiert, der die Frage behandelt hat, ob bei den Anbietern noch vorhandene Daten durch die Justizbehörden erhoben werden könnten. In diesem Zusammenhang wurde auch auf Artikel 80 der Fernmeldedienstverordnung verwiesen. Dieser lautet in dem Sinne, dass die Anbieter von Fernmeldediensten die persönlichen Daten der Kundinnen und Kunden bearbeiten dürfen, soweit und solange dies für den Verbindungsaufbau, für die Erfüllung ihrer Pflichten nach dem Büpf und für den Erhalt des für die entsprechenden Leistungen geschuldeten Entgelts notwendig ist. Auch daraus folgt, dass die Daten eben nicht länger als nötig aufbewahrt werden dürfen.
Angesichts der Tatsache, dass die Löschung der Daten, die die Anbieter für eine gewisse Zeit aufbewahren müssen, bereits geregelt ist, ziehe ich meinen Minderheitsantrag zurück.
Ich habe den Antrag der Minderheit I (Schwaab) zu Artikel 26 Absatz 5 übernommen. Hier geht es um die Vorratsdatenspeicherung. Die Minderheit I beantragt, dass die Randdaten des Fernmeldeverkehrs von den Anbietern von Fernmeldediensten während sechs Monaten aufbewahrt werden müssen, also weniger lang als während der vom Bundesrat im Entwurf und von der Kommissionsmehrheit vorgeschlagenen zwölf Monate. Die sechsmonatige Frist entspricht dem heutigen Recht. Wir lehnen also die Verlängerung dieser Frist ab.
Als Argument für die Verlängerung der Frist wurde vorgebracht, dass die sechsmonatige Frist zu kurz sei, um schwere Verbrechen wie Kinderpornografie, Gewaltdelikte oder Cyberkriminalität rechtzeitig aufklären zu können, namentlich wenn Rechtshilfegesuche aus dem Ausland vorlägen oder bei grenzüberschreitenden Tatbeständen. Dieses Argument hat uns nicht überzeugt. Natürlich ist es immer möglich, dass einzelne Straffälle durch die Maschen des Netzes fallen, weil die Frist eben sechs statt zwölf Monate beträgt. Aber Gleiches könnte man wohl auch sagen, wenn die Frist nun zwölf Monate betragen würde und ein Antrag für eine Frist von fünfzehn Monate vorliegen würde. Es ist eine Frage der Verhältnismässigkeit, wie lange eine solche Verpflichtung zur Speicherung bestehen soll. Es gab bei den Anhörungen in der Kommission sogar Voten, die sagten, dass nur für gewisse Ausnahmen eine relativ lange Frist von zwölf Monaten vorgesehen werden könnte, dass also in der Regel sechs Monate genügen sollten.
Wie gesagt, die Gründe, die für eine längere Frist vorgebracht wurden, sind nicht überzeugend. Ich ersuche Sie daher, dem Antrag der Minderheit I (Schwaab) für eine Aufbewahrungsdauer von sechs Monaten zuzustimmen.

Le président (Rossini Stéphane, président): Vous l'avez entendu, la proposition de la minorité II (Schneider Schüttel) aux articles 19 alinéa 4, 26 alinéa 5 et 39 alinéa 1 lettre b a été retirée.

Vischer Daniel (G, ZH): Ich habe hier zwei Minderheitsanträge zu vertreten. Mit dem ersten, mit meinem Minderheitsantrag V bei Artikel 26 Absatz 5, soll nun die Vorratsdatenspeicherung abgeschafft werden. Es wurde mir ja, nicht zuletzt von Leuten aus der SP, gesagt, sie seien für die Abschaffung der Vorratsdatenspeicherung, aber nicht für die Rückweisung. Das ist jetzt der Moment, wo wir handeln müssen, nachdem Sie die Rückweisung nicht beschlossen haben.
Die Argumente über die Vorratsdatenspeicherung wurden ausgetauscht. Ich habe nicht ganz begriffen, was Herr Schwaab meinte, als er vorhin darlegte, warum dieser Entscheid des Europäischen Gerichtshofes für uns nicht anwendbar und massgebend sein soll. Vor allem habe ich nicht begriffen, was kritisiert wird, wenn wir sagen, der Hauptgrund des Entscheides sei gewesen, dass eine Präventivüberwachung stattfindet, bei der keine Kriterien obwalten, welche Personen nach welchen Kriterien überwacht werden. Wie schon gesagt, entscheidend ist das Moment des Beginns der Überwachung und der Speicherung und nicht das Moment des rückwirkenden Zugriffs auf Daten nach dem richterlichen Entscheid.
Sie wissen, welche Profile über diese Randdaten erstellt werden können. Und nun ist es in der Tat ein Abwägen. Es hat keinen Sinn, jetzt so zu tun, als seien diejenigen, die gegen die Vorratsdatenspeicherung sind, gegen die Verbrechensbekämpfung. Gut, ich würde diese Schiene auch fahren, wenn ich Bundesrat wäre und diese Vorlage zu vertreten hätte; da muss man natürlich mit den Beispielen kommen, die alle im Land dann an einer «Arena»-Sendung hellhörig machen: «Ja gut, wenn ihr die Vorratsdatenspeicherung nicht wollt, dann wollt ihr keine Dschihadisten-Verfolgung, dann wollt ihr die Pädophilie nicht bekämpfen.» Aber es ist durch das Gutachten des Max-Planck-Institutes eben gerade nicht nachgewiesen worden, dass über die Vorratsdatenspeicherung tatsächlich eine effizientere Verbrechensbekämpfung erfolgt.
Die Schweiz hat – obwohl sie die Vorratsdatenspeicherung kennt – gerade in den vorgenannten Bereichen keine grösseren Fahndungserfolge als beispielsweise Deutschland. In Deutschland gibt es heute, nachdem der SPD-Parteichef den Justizminister aus seiner Partei genötigt hat, die Vorratsdatenspeicherung einzuführen, auch in SPD-Kreisen eine immer breitere Diskussion über die Vorratsdatenspeicherung. Die ehemalige Justizministerin, eine ausgewiesen liberale Person, Frau Leutheusser-Schnarrenberger, ist eine der profiliertesten Kritikerinnen dieses Instruments. Es ist eigentlich die gleiche Diskussion, wie wir sie hier führen. Es ist eine Diskussion über die Frage: Welche Eingriffe in den Grundrechtsschutz sind uns potenzielle Verbrechensbekämpfungserfolge wert? Da sagen wir: Es muss schon ein plausibler Nachweis da sein, dass grössere Erfolge möglich sind, bevor wir einem solchen Eingriff zustimmen.
Mein zweiter Minderheitsantrag will die Vorratsdatenspeicherung nicht abschaffen, sondern sie auf drei Monate reduzieren. Das ist gewissermassen die Eventualargumentation. Sie hat auch ein bisschen damit zu tun, dass man sagen kann: Okay, diese Daten werden eh gespeichert, also kommt es jetzt darauf an, wie lange sie gespeichert werden dürfen. Da meinen wir eben, dass drei Monate eine vertretbare Obergrenze sind, ab der die Verhältnismässigkeit nicht mehr gewahrt ist.
Es ist übrigens ein qualitativer Unterschied mit Bezug auf das informationelle Selbstbestimmungsrecht, ob ich einfach gedankenlos über weiss ich was für Karten und Beteiligungen an weiss ich was für Aktionen von Facebook bis weiss ich wohin mich freiwillig einlogge oder ob ich unabhängig davon, wie ich mich verhalte, dulden muss, dass Daten zugunsten des Staates zwangsgespeichert werden. Das ist ein qualitativer Unterschied; ich bitte Sie, diesen zu beachten. Das macht die Vorratsdatenspeicherung letztlich suspekt. In diesem Sinne war die Frage von Frau Badran bestenfalls gut gemeint, aber sie zielte eben genau an dieser qualitativen Unterscheidung vorbei.
Ich ersuche Sie mithin, hier nun Farbe zu bekennen und entweder die Vorratsdatenspeicherung abzuschaffen oder die Speicherung nur für drei Monate zu bewilligen. Hier zeigt es sich, wer rechtsstaatliche Erwägungen in den Vordergrund stellt und wer nicht.

Le président (Rossini Stéphane, président): Les propositions de la minorité Schwaab sont présentées par Madame Ruiz.

Ruiz Rebecca Ana (S, VD): Le but des propositions de minorité Schwaab aux articles 19 et 26 est d'améliorer le respect des droits fondamentaux liés à la conservation des données secondaires. Concrètement, il s'agit de faire en sorte que leur stockage se fasse ici en Suisse. On s'assurerait ainsi que leur conservation soit conforme aux règles en matière de protection des données et de la sphère privée prévalant dans notre pays. Alors qu'il s'agit de données passablement sensibles puisqu'elles permettent d'identifier quand ont eu lieu des télécommunications, quelle a été leur durée et où se trouvaient les personnes lors de ces échanges, il paraît pertinent de pouvoir les conserver ici. Les raisons sont assez simples.
Si on décidait de ne pas inscrire dans la loi cette nécessité, nous prendrions le risque que le stockage se fasse dans d'autres pays à travers des entreprises qui, bien que soumises au droit suisse, pourraient faire appel à des services de «cloud computing». De quoi s'agit-il concrètement? Il s'agit d'infrastructures dans lesquelles le stockage est géré par des serveurs à distance auxquels on se connecte de manière sécurisée, via Internet. On pourrait alors imaginer que les pays qui hébergeraient ces infrastructures de «cloud computing» n'aient pas les mêmes standards de protection des données que ceux que prévoit notre législation. On pourrait aussi imaginer qu'une entreprise stockant des données soit rachetée par une entreprise soumise à un droit étranger peu soucieux de la protection des données, tel que par exemple le droit américain. On sait en effet que le matériel informatique et les logiciels qui servent au stockage de données et à gérer les réseaux informatiques d'entreprises proviennent en grande partie de sociétés américaines. Le problème qui se poserait alors réside dans le fait que les entreprises américaines peuvent être obligées de fournir la totalité des données en leur possession aux services secrets, sans en informer les titulaires. Il s'agirait donc de se prémunir contre ce type de risque qu'on ne peut, hélas, exclure.
Je vous donne un exemple qui concerne mon canton et qui illustre bien la problématique. En février de cette année, le support informatique, qui avait été développé en Europe, gérant les dossiers informatiques des patients de l'hôpital universitaire vaudois, a été racheté par une société américaine. Lorsque l'annonce de ce rachat a été connue, des craintes ont été émises, notamment celle que les données gérées par ce support soient soumises au «Patriot Act» qui, comme je le disais, donne aux services américains de sécurité un accès aux données informatiques détenues par des entreprises ou des particuliers, de manière quasi discrétionnaire et sans autorisation préalable. Mais, au final, ces craintes se sont avérées infondées. Pourquoi donc? Précisément parce que les contrats prévoyaient que les données seraient stockées en Suisse, selon notre droit.
C'est exactement le but visé par les propositions de minorité Schwaab, que je vous remercie donc de soutenir.

Rickli Natalie Simone (V, ZH): Vorab möchte ich Ihnen sagen, dass ich die Änderung des Büpf unterstütze und dass es mir ein grosses Anliegen ist, dass man der Polizei und den Strafverfolgungsbehörden die Möglichkeit gibt, Straftaten ermitteln zu können, und dass das dann schlussendlich auch zu einer Verurteilung führt. Ich bin überzeugt, dass wir den Strafverfolgungsbehörden die Möglichkeit geben müssen, im Internetbereich ermitteln zu können. Die Kriminellen sind der Polizei nämlich immer einen Schritt voraus.
Auch die Asut, der Verband der schweizerischen Telekommunikationsunternehmen, und ICT Switzerland unterstützen die Änderung des Büpf. Sie sagen allerdings «ja, aber». Warum? Mit dem geplanten Ausbau der Überwachungsmassnahmen und der Ausweitung des Kreises der betroffenen Unternehmen befürchten viele IT-Unternehmen weitreichende Konsequenzen für die Telekommunikationsanbieter, und zwar vor allem auch für die vielen kleinen schweizerischen Internetanbieter und Start-ups. Die Telekombranche fordert darum – was ich voll unterstützen kann –, dass die Rechte und Pflichten der betroffenen Unternehmen dem Grundsatz nach im Büpf abschliessend und verhältnismässig geregelt werden: Der Kreis der betroffenen Unternehmen soll begrenzt werden, Internetunternehmen sollen nicht auf Vorrat in Überwachungssysteme investieren müssen, und die Anbieter sollen für ihre Aufwendungen entschädigt werden. Meine Minderheitsanträge zum Büpf gehen alle in diese Richtung, Sie können ihnen also gut zustimmen.
Damit zum Antrag meiner Minderheit zu Artikel 27 Absatz 3: Die Absätze 1 und 2 sind unbestritten, diese unterstütze ich und nehme meine Unterstützung der Minderheit Reimann Lukas zurück. In diesen Absätzen geht es darum, dass die Anbieter abgeleiteter Kommunikationsdienste die Überwachung dulden müssen. Damit haben diese kein Problem. In Absatz 2 wird weiter gesagt, dass sie auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern sollen. Sie beteiligen sich also an den Ermittlungen. Wichtig ist dabei, wie eingangs gesagt, dass die Rechte und Pflichten abschliessend geklärt werden.
In Absatz 3 schlägt der Bundesrat nun aber eine vage, sehr unkonkrete Formulierung vor, die keine Rechtssicherheit schafft. Es heisst dort: «Soweit für die Überwachung des Fernmeldeverkehrs notwendig, unterstellt der Bundesrat alle oder einen Teil der Anbieterinnen abgeleiteter Kommunikationsdienste ... allen oder einem Teil der in Artikel 26 genannten Pflichten.» Ich möchte Ihnen beliebt machen, dies nicht zu unterstützen. Was sind abgeleitete Kommunikationsdienste? In der Schweiz sind das z. B. Chats, wie Threema, Online-Speicher, wie Mount 10 oder Wuala, oder Webhosting, z. B. Hostpoint. Ein Anbieter, den Sie sicher alle kennen, ist Doodle. Das sind alles solche Anbieter, solche Start-ups, abgeleitete Kommunikationsdienste, die vom Büpf betroffen sind. Diese sind selbstverständlich bereit, die Daten zu liefern, die sie haben. Es soll aber nicht nötig sein, dass diese Firmen ein teures System einkaufen müssen, dafür bezahlen müssen, eine 24-Stunden-Bereitschaft garantieren müssen oder eben, wie hier in Artikel 27 Absatz 3, damit rechnen müssen, dass ihnen irgendwann Auflagen gemäss Artikel 26 gemacht werden.
Aus diesen Gründen beantrage ich Ihnen, meinem Minderheitsantrag zuzustimmen.

Chevalley Isabelle (GL, VD): Je parlerai principalement de l'article 26 alinéa 5, qui concerne en partie aussi l'article 19 alinéa 4.
L'article 26 alinéa 5 concerne le délai durant lequel les fournisseurs de services de télécommunication doivent conserver les données secondaires. Si la majorité du groupe vert'libéral estime que six mois sont suffisants, une minorité estime que douze mois sont nécessaires. En effet, la majorité de notre groupe est sceptique sur le bénéfice réel que pourrait apporter une conservation de douze mois en regard des atteintes à la liberté individuelle.
Les autorités de poursuite pénale que nous avons entendues nous ont demandé un délai de douze mois. Selon les cas, ils n'arrivent pas à obtenir toutes les autorisations en six mois. Pour le cas, par exemple, d'un pédophile pour lequel nos autorités devraient requérir l'entraide d'un autre pays, on a pu observer que le délai de six mois n'était pas suffisant. C'est très frustrant pour les enquêteurs de se retrouver, pour une question de délai, dans l'incapacité d'analyser des données qui auraient pu faire condamner un criminel.
Par ailleurs, il faut mentionner le risque de stockage de toutes ces données pour la protection de la sphère privée, car si certes seules les données d'une toute petite minorité de personnes soupçonnées seront finalement écoutées et analysées, il n'en demeure pas moins que toutes les données, y compris les miennes et celles de tous mes collègues et citoyens résidant en Suisse seront également stockées.
D'un côté, on double la durée de conservation des données et, de l'autre, on pourra attraper quelques criminels en plus. Il s'agit donc de faire une pesée d'intérêts entre protection

de la sphère privée et sécurité. Cela relève d'une appréciation très personnelle, c'est pourquoi notre groupe n'est pas unanime sur la question.
Concernant l'article 19 alinéa 4bis, le groupe vert'libéral soutiendra la proposition de la minorité Schwaab. Nous estimons qu'il est important que les données secondaires soient stockées en Suisse, car d'autres pays ont une notion de la protection de la sphère privée toute relative; on peut bien sûr penser aux Etats-Unis, mais pas seulement.
En ce qui concerne les autres articles du bloc 1, la majorité du groupe vert'libéral soutiendra les propositions de la majorité de la commission.

Maier Thomas (GL, ZH): Ich spreche noch kurz für die Mehrheit der grünliberalen Fraktion, die bei Artikel 26 Absatz 5 die Minderheit I (Schwaab) unterstützt, das heisst, sich dafür einsetzt, dass die Frist von sechs Monaten für die Aufbewahrung der Randdaten als absolut ausreichend gilt. Der Mehrwert einer Ausweitung der Speicherdauer ist sehr gering. Vielmehr würde eine Verlängerung bei den Strafverfolgungsbehörden eher zu einer Verlangsamung der Verfahren führen, was ja kaum anzustreben ist. Der direkte Nutzen der Randdaten für die Aufklärung von Verbrechen nimmt nach einigen Monaten stark ab; der grösste Teil der Ermittlungserfolge ist in den ersten drei bis vier Monaten festzustellen. Der Nutzen einer solchen Ausdehnung der Frist ist also so gesehen und auch statistisch beweisbar praktisch gleich null. Die sechs Monate haben sich zudem in der Praxis absolut bewährt.
Dem sehr geringen Nutzen einer Ausweitung stehen, so meinen wir, hohe Kosten gegenüber. Wie Sie wissen, arbeite ich selber in der Informatikbranche. Bei einer Frist von zwölf Monaten müsste man wohl doppelt so viele Daten aufbewahren. Professionelle, redundante, sichere Datenspeicherung inklusive Backup kostet pro Terabyte rasch ein paar Tausend Franken – und hier werden eher Petabyte an Daten generiert werden, nicht Terabyte. Es ist leider nicht vergleichbar, wenn Sie zu Hause für den persönlichen Gebrauch bei Digitec eine Harddisk mit ein paar Terabyte Speicherkapazität bestellen. Zudem bleiben den Behörden ja auch die anderen sowieso noch verfügbaren Daten der Telekomanbieter, die sie als buchhalterische Abrechnungsdaten aufbewahren. Auch diese haben unter Umständen Beweischarakter oder können wichtige Indizienbeweise liefern.
Daher sind in unseren Augen sechs Monate für die Aufbewahrung der Randdaten absolut ausreichend. Ich bitte Sie im Namen der Mehrheit der grünliberalen Fraktion, hier der Minderheit I (Schwaab) zu folgen.

Huber Gabi (RL, UR): Die Vorlage sieht sowohl im Bereich des Postverkehrs wie auch im Bereich des Fernmeldeverkehrs eine Verlängerung der Aufbewahrungsfrist der Randdaten von sechs auf zwölf Monate vor, denn das Problem des Verlusts von für die Strafverfolgung wichtigen Daten stellt sich nicht nur im Fernmeldeverkehr, sondern auch im Postverkehr. Somit muss die Verlängerung der Aufbewahrungsfrist logischerweise für beide Bereiche gelten. Aus der Praxis der Staatsanwaltschaften hat sich nämlich ergeben, dass eine Aufbewahrungsfrist von sechs Monaten zu kurz bemessen bzw. so kurz ist, dass Daten bei der Bekämpfung gewisser Formen von Kriminalität verlorengehen. Im Vordergrund stehen hier Fälle von Kinderpornografie, von organisiertem Verbrechen und Terrorismus, bei denen die Meldungen oft aus dem Ausland eintreffen und die Eröffnung der Verfahren erst mit Verzögerung stattfindet. Die Frist ist dann in solchen Fällen abgelaufen, ehe die Behörde überhaupt in der Lage ist zu sagen, gegen welche beschuldigte Person das Verfahren laufen soll oder welches Opfer genau identifiziert werden muss.
Die in Artikel 26 Absatz 5 festgelegte Pflicht bedeutet, dass die Anbieter von Fernmeldediensten wie nach der geltenden Regelung die Randdaten des gesamten Fernmeldeverkehrs quasi auf Vorrat für allfällige künftige Strafuntersuchungen aufbewahren müssen. Gestützt auf die in Artikel 31 enthaltene Kompetenz bezeichnet der Bundesrat die Randdaten, die aufzubewahren sind. Die Möglichkeit der Vorratsdatenspeicherung gleich ganz aus der Vorlage zu streichen, wie dies die Minderheit IV (Vischer Daniel) bei Artikel 19 Absatz 4 und die Minderheit V (Vischer Daniel) bei Artikel 26 Absatz 5 vorschlagen, würde also einer enormen Schwächung der Strafverfolgungsbehörden gleichkommen.
Die Minderheiten III (Reimann Lukas) und IV (Reimann Lukas) wollen bei den beiden erwähnten Artikeln das sogenannte Quick-Freeze-Modell ins Gesetz einführen. Das würde dann bedeuten, dass die Daten im Moment der Anordnung quasi vorübergehend aufbewahrt würden. Wie lange «vorübergehend» sein soll, geht aus dem Minderheitskonzept nicht hervor, und die Vorzüge dieses Modells gegenüber demjenigen des Bundesrates erschliessen sich uns nicht.
Die Minderheitsanträge Schneider-Schüttel, welche bei beiden Artikeln die Löschung der Daten nach der Aufbewahrungsfrist anordnen wollen, wurden offenbar zurückgezogen. Schliesslich gibt es noch eine Minderheit Schwaab, welche in Artikel 26 Absatz 5bis geografische Vorgaben zum Aufbewahrungsort der Randdaten macht. Damit mischt sich diese Minderheit in die interne Organisation der Post ein, und das hätte einen Wettbewerbsnachteil gegenüber anderen Unternehmen zur Folge. Es kommt dazu, dass die Post gleichwohl schweizerischem Recht unterstellt ist, auch wenn sie Daten im Ausland aufbewahren würde.
Die FDP-Liberale Fraktion wird grossmehrheitlich sämtliche Minderheitsanträge in diesem Block ablehnen, und ich lade Sie ein, Gleiches zu tun.

Guhl Bernhard (BD, AG): Organisierte Kriminalität kann durchaus auch über firmeninterne Netze koordiniert werden. Den Kriminellen ist es völlig egal, ob sie nun über ein Firmennetz oder zum Beispiel über das Netz der ETH mailen. Ich will damit nicht die ETH anprangern; ich will nur aufzeigen, dass niemand verhindern kann, dass auch ein solches Netz für kriminelle Zwecke verwendet wird. Daher sind bei Artikel 2 Buchstabe c und Artikel 2 Absatz 2 die Minderheitsanträge abzulehnen, denn damit würden wir Lücken schaffen. Ich bin überzeugt, dass die kriminellen Organisationen genau solche Lücken suchen und finden werden.
Bei Artikel 8 Buchstabe b, bei den Verbindungsversuchen, sieht die BDP-Fraktion durchaus, dass deren Erfassung das Tüpfchen auf dem i bei den Ermittlungen sein könnte. Aber Aufwand und Ertrag stimmen für die BDP-Fraktion hier nicht überein. Die BDP-Fraktion will die Telekomanbieter nicht noch mit dieser zusätzlichen Erfassung des Verbindungsaufbaus, der heute noch nicht erfasst wird, belasten. Sie wird daher bei diesem Artikel der Minderheit Reimann Lukas zustimmen.
Die zentrale Frage ist die Aufbewahrungsfrist für die Randdaten des Fernmeldeverkehrs. Vorweg: Die BDP-Fraktion wird hier die Mehrheit unterstützen. Die BDP-Fraktion setzt alles daran, dass möglichst viele Fälle gelöst werden können. Wenn ein Fall erst später zur Anzeige kommt oder ein Rechtshilfegesuch aus dem Ausland spät eintrifft, so sind halt die sechs Monate sehr schnell vorbei. Die Speicherkosten sind heute auch nicht mehr horrend, sodass sie hier nicht mehr als Argument verwendet werden können. Ob die Daten nun sechs oder zwölf Monate gespeichert werden, das macht den Braten auch nicht mehr feiss. Über 99 Prozent der Daten werden eh ungelesen oder ungesehen gelöscht. Wer nichts Schweres verbrochen hat, muss die Speicherung der Randdaten wirklich nicht fürchten. Wie schon mehrfach hier drin erwähnt, werden letztendlich nur die Daten verwendet, denen ein schweres Verbrechen vorangeht.
So viel von uns zu Block 1.

Vogler Karl (CE, OW): Namens der CVP/EVP-Fraktion ersuche ich Sie, in Block 1 – mit Ausnahme der Minderheitsanträge zu Artikel 19 Absatz 4bis und zu Artikel 26 Absatz 5bis – immer der Mehrheit zu folgen und die Minderheitsanträge abzulehnen.
Folgende Begründung hierzu: Bei Artikel 2 Litera c und beim neuen Absatz 2 geht es um den persönlichen Geltungsbe-

reich, der ganz bewusst erweitert werden soll. Mit der Streichung von Litera c schafft man eine Lücke und damit quasi eine Einladung an Kriminelle, auf diese Art zu kommunizieren. Unsere Fraktion lehnt solches ab. Was die Ergänzung in Absatz 2 gemäss Antrag der Minderheit Reimann Lukas betrifft, so lehnen wir dies ebenfalls ab. Man würde damit sogar einen Rückschritt machen und hinter die heutige Regelung gemäss Strafprozessordnung fallen sowie einen entsprechenden Widerspruch stipulieren.
Was den Antrag der Minderheit Reimann Lukas bei Artikel 8 Litera b betrifft, so ist dieser ebenfalls abzulehnen. Es geht hier letztlich wiederum um die Frage, ob man Täter unnötig schützen will oder nicht. Unsere Fraktion will das nicht und unterstützt eine wirkungsvolle Strafverfolgung.
Kurz zu den verschiedenen Minderheiten bei Artikel 19 Absatz 4: Hier geht es um die Dauer der Aufbewahrungspflicht von Randdaten der Postdienste und deren allfällige anschliessende Löschung beziehungsweise um den Antrag der Minderheit IV (Vischer Daniel), die Vorratsdatenspeicherung generell zu streichen. Vorab, es geht hier um Postranddaten und damit um sehr wenige Fälle, und trotzdem ist es halt wichtig, dass diese gemäss Bundesrat für die Dauer von zwölf Monaten aufbewahrt werden. Es muss verhindert werden, dass bei schweren Delikten – wir sprechen hier, es wurde gesagt, von Kinderpornografie, von organisiertem Verbrechen, von Terrorismus usw. – Täter der Strafverfolgung entgehen, nur weil solche Daten nicht mehr zur Verfügung stehen. Der entsprechende Mehraufwand für die Postdienste wie auch die Dauer von zwölf Monaten sind angesichts des öffentlichen Interesses absolut vertretbar und auch verhältnismässig.
Die Anträge der Minderheiten I, III und IV sind somit abzulehnen, ebenfalls der Antrag der Minderheit II, der zwischenzeitlich allerdings zurückgezogen worden ist. Zustimmen wird unsere Fraktion dem Minderheitsantrag Schwaab betreffend Artikel 19 Absatz 4bis. Es geht hier um den Ort der Aufbewahrung der Randdaten aus dem Postverkehr. Wir haben uns hier für die Schweiz als Aufbewahrungsort entschieden.
Was die Aufbewahrungsfrist der Randdaten im Fernmeldeverkehr betrifft, und damit komme ich zu den Minderheiten bei Artikel 26 Absatz 5, so kann ich im Wesentlichen auf meine Hinweise zu den Minderheiten bei Artikel 19 Absatz 4 verweisen. Ergänzend feststellen möchte ich, dass der Entscheid des Europäischen Gerichtshofes in Luxemburg zur Vorratsdatenspeicherung letztlich für die Schweiz ohne Belang ist; die entsprechenden Ausführungen wurden heute hinreichend gemacht.
Was die Pflicht zur Aufbewahrung der Randdaten durch die Fernmeldedienste in der Schweiz gemäss Minderheitsantrag zu Artikel 26 Absatz 5bis betrifft, so gelten analog die gemachten Hinweise zu den Randdaten im Postverkehr. Unsere Fraktion wird dem Minderheitsantrag Schwaab zustimmen. Schliesslich lehnen wir die Minderheitsanträge bei Artikel 27 ab. Auch diese Minderheitsanträge untergraben letztlich eine effiziente Strafverfolgung, was wir, ich habe es gesagt, nicht wollen.
Zusammengefasst ersuche ich Sie, in Block 1 immer der Mehrheit zu folgen, mit Ausnahme der Artikel 19 Absatz 4bis und 26 Absatz 5bis, wo ich Sie bitte, den Minderheiten zuzustimmen.

Ruiz Rebecca Ana (S, VD): Les données secondaires permettent de savoir qui a été en communication avec qui, quand, pendant combien de temps et d'où ont eu lieu ces échanges. Comme il s'agit de données de facturation, elles sont à l'heure actuelle d'ores et déjà conservées par les opérateurs. Elles sont aussi déjà parfois utilisées à des fins d'enquête, lorsqu'il s'agit de poursuivre des infractions graves. Mais une telle utilisation ne peut se faire que dans le cadre d'une procédure pénale, enclenchée après la commission d'un crime, avec l'autorisation du Tribunal des mesures de contrainte ou alors pour rechercher une personne disparue en grand danger, par exemple un enfant.
Les données secondaires ne peuvent aucunement être obtenues à titre préventif ou pour surveiller Madame ou Monsieur Tout-le-Monde en l'absence de tout soupçon. Non, la surveillance d'individus au travers de ces données secondaires ne peut concerner que des personnes fortement soupçonnées d'avoir commis un crime grave – la liste des infractions en question étant énumérée à l'article 269 alinéa 2 du Code de procédure pénale –, comme les homicides, les assassinats, différents délits économiques, la traite d'êtres humains, l'enlèvement ou encore les délits sexuels.
Une des nouveautés du projet en lien avec les données secondaires concerne leur durée de conservation. Actuellement, la loi prévoit six mois, dans le projet douze mois sont jugés nécessaires, six mois étant considérés comme insuffisants. Autre nouveauté, il est prévu de pouvoir désormais obliger sur demande les fournisseurs de services de communication dérivés à conserver les données secondaires, ce qui est actuellement impossible. Il s'agit par exemple des purs fournisseurs de services e-mail, des fournisseurs tels que Facebook, Dropbox, des plates-formes de «chat», ainsi que des fournisseurs de téléphonie Internet tels que Skype.
En lien avec ces deux points, plusieurs propositions de minorité ont été déposées. Concernant la conservation, notre groupe vous invite à soutenir les propositions de minorité Schwaab qui exigent le stockage des données en Suisse pour s'assurer que la conservation se fasse dans le respect de nos règles en matière de protection des données.
La durée de conservation divise passablement le groupe socialiste. Une partie s'oppose à la prolongation de six à douze mois en mettant en évidence que le faible gain en matière de poursuite pénale qu'une telle prolongation amènera n'est pas suffisant pour justifier une pareille atteinte aux droits fondamentaux.
Ainsi une partie du groupe socialiste soutiendra les propositions de la minorité I (Leutenegger Oberholzer), III (Reimann Lukas) et IV (Vischer Daniel) à l'article 19 alinéa 4, ainsi que les propositions de la minorité I (Schwaab), II (Vischer Daniel), IV (Reimann Lukas) et V (Vischer Daniel) à l'article 26 alinéa 5. Une autre partie du groupe soutiendra les propositions de la minorité II (Schneider Schüttel) à l'article 19 alinéa 4 et III (Schneider Schüttel) à l'article 26 alinéa 5, qui visent à maintenir la durée de conservation à douze mois, tout en exigeant l'effacement des données après l'échéance du délai. Pour cette partie du groupe, le délai de douze mois se justifie, car il permettra de mieux pouvoir poursuivre la criminalité en ligne, notamment la pédocriminalité, ou les activités criminelles à ramifications internationales, puisqu'il apparaît que les six mois actuels sont trop courts et que ce délai est souvent totalement, ou en grande partie échu, lorsque l'autorité est en mesure d'ordonner une surveillance.
Le groupe socialiste vous invite par ailleurs à rejeter la proposition de la minorité Reimann Lukas à l'article 8 lettre b qui vise à supprimer des données secondaires les informations relatives aux tentatives de communication.
Notre groupe vous invite également à rejeter les propositions de la minorité Reimann Lukas à l'article 2 lettre c, à l'article 2 alinéa 2 et à l'article 27, ainsi que la proposition de la minorité Rickli Natalie à l'article 27. Ces propositions concernent les nouvelles obligations de collaborer imposées aux fournisseurs de services de communication dérivés. Ces derniers étant susceptibles de détenir des données pouvant intéresser les autorités de poursuite pénale, par exemple un échange de messages sur Facebook, il paraît légitime que ces acteurs soient aussi soumis à des obligations dans le domaine de la surveillance.

Schwander Pirmin (V, SZ): Ich bitte Sie namens der SVP-Fraktion, den Minderheiten Reimann Lukas zu folgen und bei Artikel 27 Absatz 3, wenn die Minderheit Reimann Lukas nicht durchkommt, der Minderheit Rickli Natalie zuzustimmen.
Warum? Ich gehe nicht auf die Anträge der Minderheiten und der Mehrheit zu den einzelnen Artikeln ein. Es geht in diesem Block insbesondere darum, den Aufwand für die Fernmeldedienstanbieter abzuschätzen. Die Minderheiten

Reimann Lukas versuchen, den Aufwand zu reduzieren. Wir haben in verschiedenen Artikeln Auflagen – wir wissen das zwar zugegebenermassen eigentlich noch nicht, aber wir müssen darauf hinweisen –, da wir dem Bundesrat in x Artikeln die Kompetenz geben, die Details zu regeln. Aufgrund dieser Details kommen dann Kosten auf die Fernmeldedienstanbieter zu. Der Bundesrat muss aufgrund dieser gesetzlichen Grundlage Details regeln bezüglich Akteneinsicht, bezüglich Aufbewahrung, bezüglich Sicherheit, bezüglich Überwachungstyp – ich erwähne jetzt die einzelnen Artikel nicht. Das ist sehr gefährlich für die Fernmeldedienstanbieter. Der Bundesrat muss das alles noch regeln; er muss Vorschriften erlassen über rückwirkende Überwachung, die Kundenbeziehungen näher definieren, Modalitäten der Datenerfassung verifizieren, präzisieren; er muss Vorschriften erlassen über die Befreiung von Pflichten. Übrigens haben die Fernmeldedienstanbieter nur Pflichten und Kosten, und sie müssen dann die Kosten auch noch selbst tragen – das ist das Konkrete, das noch kommt. Dann muss der Bundesrat Vorschriften über Daten pro Überwachungstyp und letztlich auch Vorschriften bezüglich Entschädigung und Gebühren erlassen.
Ich habe Ihnen zehn Punkte aufgezeigt, bei denen nicht klar ist, was noch alles kommt. Wir haben den Verdacht – dieser Verdacht ist nicht unbegründet, wenn wir andere gesetzliche Vorlagen anschauen, ich erinnere an die Swissness-Vorlage –, dass dann die Kosten kommen, wenn auf Verordnungsstufe die Präzisierungen für die Fernmeldedienstanbieter geregelt werden. Jetzt können wir sie wahrscheinlich noch nicht so genau abschätzen, deshalb konnten die Fernmeldedienstanbieter ihre Kosten auch nicht genau bekanntgeben. Aber wenn der Bundesrat mit seinen Vorschriften kommt, kommen auch die entsprechenden Kosten, und diese Kosten möchten wir mit den Minderheitsanträgen Reimann Lukas reduzieren. Wir möchten Klarheit schaffen für die Fernmeldedienstanbieter und erreichen, dass die ganze Angelegenheit für sie auch tragbar wird.
Ich bitte Sie namens der Mehrheit der SVP-Fraktion, den Minderheitsanträgen Reimann Lukas zu folgen.

Glättli Balthasar (G, ZH): Im Namen der Grünen möchte ich jetzt einen kleinen Appell an all jene richten, die vorher gesagt haben, dass unser Rückweisungsantrag eine Selbstkapitulation des Parlamentes darstelle, und die uns quasi formaljuristisch angegriffen haben, indem sie sagten, wir hätten ja für die Detailberatung Minderheitsanträge für eine Verkürzung oder Abschaffung der Vorratsdatenspeicherung stellen können: Sie haben jetzt solche Minderheitsanträge vorliegen. Das ist jetzt der Moment der Wahrheit. Hier zeigt sich, ob das vorher nur rhetorische Ausflüchte gewesen sind oder ob Sie – ich denke jetzt zum Beispiel an Herrn Lüscher, der mir die Frage gestellt hat – es wirklich ernst meinen mit dem Schutz der Privatsphäre.
In diesem Block sehen wir aber auch noch etwas anderes: Wir sehen, wie absurd es ist, über die gesteigerte Sicherheit und die Möglichkeit zu debattieren, Verbrechen einfacher aufzuklären, indem man die Randdaten speichern würde. Wir haben es hier nämlich nicht nur mit den Randdaten im Fernmeldeverkehr zu tun, sondern auch mit jenen im Postverkehr. Entweder meinen Sie es so – das steht nicht im Text –, dass wir alle künftig nur noch eingeschriebene Briefe verschicken und auf dem Postweg nur noch eingeschrieben miteinander kommunizieren dürften, weil man dort auch den Absender angeben muss, denn ansonsten sind das völlig lächerliche Bestimmungen! Die Randdaten des Briefpostverkehrs aufzubewahren ist lächerlich, weil doch auf einem Brief in den meisten Fällen – vor allem bei jenen Briefen, mit denen irgendetwas Problematisches oder rechtlich nicht Korrektes kommunizieren werden soll – nicht der Absender dick draufsteht. Im Prinzip zeigen Sie hier eigentlich auch eine gewisse Hilflosigkeit. Und Sie zeigen auch, dass das Versprechen der totalen Sicherheit – oder zumindest das Versprechen einer grösstmöglichen Sicherheit – schon an sehr viel einfacheren Orten als im Internetbereich, der jetzt immer genannt wird, nicht gehalten werden kann.
Wenn ich ein Krimineller wäre, der sich mit anderen austauschen müsste, dann würde ich eine CD mit verschlüsselten Daten oder einen USB-Stick mit verschlüsselten Daten per normale Briefpost verschicken, ohne den Absender darauf, und dann wäre diese ganze Randdaten-Geschichte im Postverkehr ausser Kraft gesetzt. Also, nehmen Sie zumindest den Antrag der Minderheit IV (Vischer Daniel) an, wenn es um die Randdaten im Postverkehr geht. Sonst ist das dann wirklich nichts anderes als Bürokratie pur und Mehraufwand pur.
Nochmals zurück zur Telekommunikation, über die wir vorher gesprochen haben. Ich muss Ihnen sagen, ich hätte eigentlich von den Verteidigern einer besseren Möglichkeit, die Strafverfolgung vornehmen zu können, erwartet, dass sie nicht einfach nur wild mit den Reizwörtern «Pädophilie», «Terrorismus», «Kinderschänder» um sich geschlagen hätten. Ich hätte vielmehr erwartet, dass sie vielleicht auch zur Kenntnis genommen hätten, dass es in anderen europäischen Staaten durchaus ernsthafte Bemühungen von Verantwortlichen für die Justiz gibt – in der Diskussion fiel das eine oder andere Mal der Name Leutheusser-Schnarrenberger, der Name der FDP-Politikerin –, eine bessere Strafverfolgung sicherzustellen, ohne dass man dabei generell auf das Grundrecht auf geschützte Kommunikation und das Grundrecht auf Privatsphäre aller, die sich der elektronischen Kommunikation bedienen, verzichtet. Ich hätte mir hier eigentlich auch vom Bundesrat, von der Bundespräsidentin, einen etwas differenzierteren Approach gewünscht.

Die Beratung dieses Geschäftes wird unterbrochen
Le débat sur cet objet est interrompu

Schluss der Sitzung um 12.55 Uhr
La séance est levée à 12 h 55

Dreizehnte Sitzung – Treizième séance

Mittwoch, 17. Juni 2015
Mercredi, 17 juin 2015

15.00 h

13.025

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Änderung

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

Fortsetzung – Suite

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)
Nationalrat/Conseil national 17.06.15 (Zweitrat – Deuxième Conseil)
Nationalrat/Conseil national 17.06.15 (Fortsetzung – Suite)

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

Block 1 (Fortsetzung) – Bloc 1 (suite)

Sommaruga Simonetta, Bundespräsidentin: In diesem Block 1 behandeln Sie schwergewichtig den Geltungsbereich des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) und die Frage der Randdatenspeicherung. Ich werde nicht auf alle Minderheitsanträge im Einzelnen eingehen, sondern ich werde die beiden Bereiche etwas zusammenfassen und dazu Stellung nehmen.
Zuerst zum Geltungsbereich: Wenn Sie den Minderheitsanträgen zu den Artikeln 2, 8, 22 und 27 zustimmen würden, dann hätte das erhebliche Lücken in der Fernmeldeüberwachung zur Folge. Die heutige Fernmeldeüberwachung konzentriert sich ja ausschliesslich auf die klassischen Fernmeldedienstanbieterinnen, sie nimmt also nur diese in die Pflicht. Damit aber jetzt keine überwachungsfreien Kommunikationskanäle entstehen, sollen auch neue Akteure in das System der Fernmeldeüberwachung integriert werden. Reine Cloud-Dienst-Anbieter zum Beispiel oder reine E-Mail-Provider werden neu als sogenannte Anbieterinnen abgeleiteter Kommunikationsdienste in die Pflicht genommen. Sie sollen diejenigen Daten liefern, über die sie sowieso verfügen. In der Sache geht es also um eine reine Herausgabepflicht dieser Anbieterinnen.
Ich sage hier gern gleich etwas zum Minderheitsantrag Rickli Natalie zu Artikel 27 Absatz 3. In Artikel 27 geht es um die Pflichten der Anbieterinnen von abgeleiteten Kommunikationsdienstleistungen. Wenn Sie Artikel 26 Absatz 6 anschauen, sehen Sie, dass dort steht, dass der Bundesrat die Kompetenz hat, bei den Fernmeldedienstanbieterinnen die kleinen Anbieterinnen, die von kleiner wirtschaftlicher Bedeutung sind, auszunehmen. Das wird in der Verordnung geregelt. Diese Verordnung gibt es heute schon. In der Tat hat dort der Bundesrat die kleinen Anbieterinnen ausgenommen.
Nun kann ich Ihnen hier eigentlich zusichern, dass wir das Gleiche, was wir heute betreffend Artikel 26 in der Verordnung haben, auch bei Artikel 27 selbstverständlich analog machen werden und dass wir auch bei Anbieterinnen und Anbietern von abgeleiteten Kommunikationsdienstleistungen analog vorgehen werden. Es gibt keinen Grund, dort anders vorzugehen. Sie möchten das im Gesetz festlegen. Wenn Sie aber Absatz 3 streichen, wie Sie von der Minderheit das beantragen, haben Sie das Kind mit dem Bad ausgeschüttet. Ich sage Ihnen einfach heute: Wir werden auch betreffend Artikel 27 in der Verordnung analog zu Artikel 26 entsprechend vorgehen.
Zur Forderung, dass die nichtkommerziellen Anbieterinnen ausgenommen sind: Wir sind der Meinung, dass auch diese nicht grundsätzlich ausgenommen werden dürfen, wenn man keine Lücken in Kauf nehmen will. Um den Eingriff aber möglichst klein zu halten, besteht bei solchen Anbieterinnen lediglich eine Duldungspflicht. Es ist aber schon nicht einsehbar, weshalb z. B. ein privater WLAN-Anbieter nicht zulassen soll, dass die Kommunikation von seinem Netz aus überwacht wird, wenn klar ist, dass dieses für die Vorbereitung oder Begehung von Verbrechen benutzt worden ist. Allerdings entstehen diesem Anbieter dadurch keinerlei Kosten oder Aufwände, weil es hier ja ausschliesslich um eine Duldungspflicht geht.
Gemäss Antrag der Minderheit bei Artikel 8 Buchstabe b sollen die Verbindungsversuche vom Verarbeitungssystem ausgenommen werden. Verbindungsversuche generieren ebenfalls Randdaten, die vor allem für die Verfolgung von Straftaten mit mehreren Beteiligten wichtig sind. Das ist insbesondere auch wichtig, um den Zeitablauf eines Verbrechens zu rekonstruieren oder Beteiligungen nachzuweisen. Der Rückgriff auf solche Randdaten bedeutet aber für die Fernmeldedienstanbieterinnen ebenfalls keinen zusätzlichen Aufwand.
Das sind also die Überlegungen. Es ist eben schon nicht so, dass sich dort keine Kriminellen im Netz bewegen, nur weil ein Anbieter nicht kommerziell anbietet. Die Aussage «Klein ist immer gut, dort gibt es keine Kriminellen» kann nicht per se so angenommen werden. Deshalb möchten wir hier keine Lücken schaffen. Aber mit der Unterscheidung bezüglich der Duldungspflicht stellen wir sicher, dass für Anbieter mit einem kleinen Benutzerkreis oder für nichtkommerzielle Anbieter keine zusätzlichen Aufwände und Kosten entstehen.
Der zweite Bereich in diesem ersten Block betrifft noch einmal die Randdatenspeicherung. Ich habe beim Eintreten schon gesagt, dass es doch ziemlich inkonsequent ist, wenn man das Nachrichtendienstgesetz unterstützt, beim Büpf aber dann die Aufbewahrung von Randdaten ausschliesst. Dann müssten Sie das Nachrichtendienstgesetz übrigens wieder entsprechend anpassen. Ich denke, ansonsten werde ich die Argumente nicht noch einmal aufführen, weshalb diese Vorratsdatenspeicherung sinnvoll ist respektive der Zugriff der Strafverfolgungsbehörden darauf, wenn ein Strafverfahren eröffnet und von einem Zwangsmassnahmengericht bewilligt worden ist.
Ich gebe noch folgende Überlegung zu bedenken: Die Aufbewahrung der Randdaten bei den Fernmeldedienstanbieterinnen ist ja nichts Neues, wir kennen das seit 13 Jahren – seit 13 Jahren kann die Strafverfolgungsbehörde auf diese Randdaten während sechs Monaten zurückgreifen. Das ist ein Bestandteil der Verbrechensbekämpfung. Ich habe jetzt auch heute Morgen nicht gehört, dass diese Möglichkeit in den letzten 13 Jahren missbraucht worden wäre. Ich habe heute Morgen von keinem einzigen Missbrauchsfall gehört. Es wäre schon interessant gewesen zu erfahren – vor allem seitens derjenigen Kreise, welche die Vorratsdatenspeicherung jetzt überhaupt nicht mehr wollen, also ganz streichen wollen –, ob man mit dieser Möglichkeit, während sechs Monaten darauf zurückzugreifen, schlechte Erfahrungen gemacht hat. Das einzig Neue, das wir tun, ist, dass man nicht nur während sechs Monaten darauf zurückgreifen kann, sondern während zwölf Monaten.

Ich habe es beim Eintreten gesagt: Wenn man auf die Aufbewahrung der Randdaten ganz verzichten oder diese Fristen massiv verkürzen würde, wäre das ein Rückschritt gegenüber dem heute geltenden Recht. Gerade diejenigen, die hiergegen ein gewisses Misstrauen verspüren, müssten eigentlich ein Interesse daran haben, dass das klar geregelt ist, dass gesagt wird, wer unter welchen Voraussetzungen Zugriff haben kann, und dass die Hürden, ich sage es noch einmal, möglichst hoch gesetzt werden. Sollten Sie trotzdem beschliessen, dass die Aufbewahrungsfrist für Randdaten verkürzt wird oder dass diese gar nicht mehr benutzt werden dürfen, müssen Sie sich bewusst sein, dass Sie für die Strafverfolgung in verschiedenen Bereichen Erschwerungen einführen oder diese insgesamt sogar verunmöglichen. Gerade bei komplexen Kriminalfällen, und das ist in den Bereichen des organisierten Verbrechens oder des Terrorismus der Fall, sind diese Fristen von sechs Monaten heute häufig einfach zu kurz. Die Frist ist dann häufig schon abgelaufen, bevor die Behörden von der Beweislage her überhaupt in der Lage sind, eine Überwachung anzuordnen. Auch Rechtshilfeverfahren aus dem Ausland nehmen oft mehr als sechs Monate in Anspruch. Das betrifft dann vor allem die Bekämpfung der Internetkriminalität und dort insbesondere das Herunterladen von Kinderpornografie. Zudem bietet die Verlängerung der Aufbewahrungsdauer technisch kaum Schwierigkeiten und verursacht auch keine übertriebenen Kosten.
Ich möchte mich abschliessend noch zum Quick-Freeze-Verfahren äussern. Das wird von der Minderheit IV in Artikel 26 Absatz 5 verlangt. Der Begriff «Quick-Freeze-Verfahren» hört sich modern und unproblematisch an. Danach dürfen die Randdaten nicht mehr im Voraus, sondern erst ab Anordnung der Überwachung gespeichert werden. Damit wäre die ganze rückwirkende Überwachung, wie sie schon heute erlaubt ist, nicht mehr möglich; sie wäre verunmöglicht. Auch dieses Vorgehen schwächt die Strafverfolgung gegenüber heute empfindlich.
Ich bitte Sie, bei allen Bestimmungen von Block 1 den Anträgen der Kommissionsmehrheit zu folgen.
Ich sage gerne noch etwas zur Abwägung im Zusammenhang mit den Grundrechten, das wurde nämlich heute Morgen auch angesprochen. Es wäre gut, wenn diejenigen, die sich vor allem für die Grundrechte interessieren, dann auch zuhören würden. Es muss aber nicht sein ...
Wenn Sie die Grundrechtsdiskussion führen wollen, dann bitte ich Sie, nicht einfach nur die Grundrechte der Täter anzuschauen, sondern auch die Grundrechte der Opfer. Da muss, glaube ich, eine Abwägung geschehen. Wir versuchen mit diesem Gesetz, mit dem Büpf, diese Abwägung vorzunehmen. Wir haben abgewogen und gesagt, dass es im Sinne der Grundrechte der Opfer auch möglich sein muss, der Strafverfolgung bei der Bekämpfung von schwerer Kriminalität die Instrumente in die Hand zu geben, damit diese ihre Arbeit tun kann, wobei diese Möglichkeiten gleichzeitig so stark eingeschränkt werden sollen, dass selbstverständlich die Grundrechte der, sage ich jetzt mal, Täter ebenfalls gewahrt werden. Bei dieser Abwägung befinden Sie sich nun in der Büpf-Revision.
Ich bitte Sie, der Mehrheit Ihrer Kommission zu folgen. Ich denke, wenn Sie das tun, dann haben Sie genau im Sinne des Versuchs, hier ein Gleichgewicht zu finden, gehandelt.

Leutenegger Oberholzer Susanne (S, BL): Frau Bundespräsidentin, ich möchte einfach noch einmal auf Folgendes hinweisen: Sie haben uns gefragt, wie viele Missbrauchsfälle wir kennen. Wissen Sie, wie wir argumentiert haben? Wir sagen, dass die Randdatenspeicherung per se ein Eingriff in die Grundrechte ist. Dieser muss verhältnismässig sein. Erinnern Sie sich? Das ist meine Frage: Ich habe die Verhältniszahlen aufgeführt. Wir haben, wenn wir alle Handys und Computer usw. erfassen, vielleicht 10 bis 20 Millionen Teilnehmer, und die Strafverfolgung greift heute – einfach theoretisch – auf 5000 bis 6000 Fälle zu. Das macht eine Ausbeute im Null-Komma-Promille-Bereich. Das ist nicht mehr verhältnismässig. Das ist eben der Unterschied der Wertung zwischen der Missbrauchsbekämpfung und der Wahrung der Verhältnismässigkeit in Bezug auf die Grundrechte.

Sommaruga Simonetta, Bundespräsidentin: Gut, dann sage ich gerne noch einmal, was ich heute Morgen schon gesagt habe, Frau Leutenegger Oberholzer. Die Randdaten werden nicht vom Staat gespeichert, einfach damit das noch einmal klar ist. Die Randdaten, wer mit wem wann wie lange telefoniert oder kommuniziert hat, werden von den Fernmeldedienstanbieterinnen gespeichert, um Ihnen allen Rechnung zu stellen und auch um ihre Infrastruktur planen zu können, zum Beispiel, um zu schauen, welche Antennen häufiger gebraucht werden. Wenn Sie den Fernmeldedienstanbieterinnen verbieten wollen, Ihre Daten zu speichern, dann regeln Sie das im Fernmeldedienstgesetz, aber nicht im Büpf. Das Büpf sagt nicht, dass die Fernmeldedienstanbieterinnen Ihre Daten noch viel länger speichern müssen, sondern es sagt nur – bei den Daten, die ohnehin von den Privaten gespeichert werden –, unter welchen Voraussetzungen die Strafverfolgungsbehörde das Anrecht hat, auf diese Daten zugreifen zu können. Das ist das Büpf. Der Staat speichert keine Fernmeldedienstdaten, jetzt nicht und auch in Zukunft nicht.

Schwaab Jean Christophe (S, VD), pour la commission: Nul ne le nie, la conservation des données secondaires est une atteinte importante au droit fondamental à la sphère privée. Les données secondaires permettent de savoir qui a été en contact avec qui, depuis quel endroit et pour combien de temps. Mais, en les recoupant, il est possible de reconstituer intégralement l'emploi du temps d'une personne et, partant, ses activités, ses loisirs, probablement ses opinions politiques, ses lieux de prédilection, avec qui elle se trouvait et pourquoi. Autant dire que l'on peut savoir beaucoup de choses à notre sujet. Conserver ce genre de données et, le cas échéant, les transmettre à l'Etat, est donc indéniablement une atteinte grave aux droits fondamentaux.
Cette atteinte nécessite que l'on respecte les règles de l'article 36 de la Constitution fédérale en matière de restriction des droits fondamentaux, qui sont les suivantes: fondement sur une base légale; justification par un intérêt public; respect du principe de la proportionnalité. La base légale, c'est la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. L'intérêt public, c'est la poursuite pénale; c'est le droit fondamental de chacun à vivre en sécurité; c'est l'obligation de l'Etat de pourchasser et de punir les criminels, même s'ils agissent derrière un paravent technologique ou numérique; c'est donner, dans le cadre d'une pesée des intérêts, lorsque cela est nécessaire, la priorité au droit fondamental des victimes par rapport au droit fondamental de l'auteur présumé de l'infraction.
Reconstituer la journée et les contacts d'une personne soupçonnée d'un crime est un élément qui peut être important pour l'enquête. Certes, ce n'est pas un moyen miracle, la majorité de la commission ne le prétend d'ailleurs pas. Il est vrai que l'utilité des données secondaires est contestée, mais les autorités de poursuite pénale, dont nous avons entendu les représentants, sont quasi unanimes: c'est un instrument qui est important en pratique. Or, aujourd'hui, la conservation des données secondaires est limitée à six mois. C'est trop peu pour certains cas de criminalité en ligne, notamment en cas de ramifications internationales, par exemple en cas de pédophilie ou de diffamation en ligne. Il peut arriver que, lorsque la demande d'entraide a enfin reçu une réponse positive, le délai de six mois soit déjà échu et que l'on ne puisse plus reconstituer le passé récent de l'auteur présumé. Le Conseil fédéral et la majorité de la commission sont donc d'avis qu'il faut prolonger le délai de conservation à douze mois, comme le prévoient d'ailleurs plusieurs motions acceptées par le Parlement.
La constitutionnalité de la conservation des données secondaires est une question brûlante que la commission s'est posée avec sérieux, ne serait-ce qu'à cause de la décision de la Cour européenne de justice qui a été déjà maintes fois évoquée au cours de ce débat et de celles d'autres cours

constitutionnelles, qui statuent dans d'autres Etats et qui se sont penchées sur l'application de la directive européenne déjà mentionnée dans le débat.
J'aimerais revenir sur certaines critiques que la Cour européenne de justice a émises à propos de cette directive européenne, critiques qui démontrent à quel point cet arrêt n'est pas transposable en droit suisse. La Cour européenne de justice a critiqué la directive parce qu'elle ne prévoit pas de conditions limitatives concernant la conservation des données secondaires, leur accès et leur utilisation. Elle ne prévoyait pas la limitation à des infractions graves, elle ne prévoyait pas non plus les conditions procédurales, notamment le fait qu'un contrôle soit effectué par une autorité judiciaire. Or, ces conditions, le projet de loi qui nous est soumis aujourd'hui les remplit. Il est prévu d'avoir une intervention d'un juge et de ne pas utiliser les données n'importe comment.
Pour la majorité de la commission, la constitutionnalité de la conservation des données secondaires ne fait donc aucun doute. Tant la loi actuelle que le projet qui nous est soumis aujourd'hui accorde une très grande attention au respect du principe de proportionnalité. Il y a d'ailleurs une décision judiciaire – certes il ne s'agit que d'une décision du Service «Surveillance de la correspondance par poste et télécommunication» en date du 30 juin de l'année passée – qui conclut que la constitutionnalité est bel et bien présente. Cette décision, cela a été dit, est pendante devant le Tribunal administratif fédéral et elle sera probablement portée devant le Tribunal fédéral, mais la seule décision suisse qui existe va dans le sens des réflexions de la majorité de la commission.
Je vous propose de passer en revue les arguments qui plaident pour la constitutionnalité:
1. Ce n'est pas l'Etat qui conserve les données secondaires.
2. L'Etat ne peut obtenir ces données qu'en cas de soupçons avérés d'un crime important, contenu dans la liste de l'article 269 du Code de procédure pénale; autrement, il n'obtient pas ces données.
3. L'utilisation de ces données est subsidiaire par rapport aux autres moyens de surveillance, qui doivent avoir tous échoué avant de pouvoir recourir aux données secondaires.
4. L'utilisation concrète doit être proportionnée au but visé. Il n'est pas question par exemple de se servir de ces données pour pourchasser un voleur de pommes ou les gens qui menacent de tuer des chatons.
5. Enfin, c'est un juge qui autorise ou non la police à faire usage de ces données.
Il est donc erroné de prétendre avoir affaire à une surveillance de masse, incontrôlée, faite par un Etat fouineur. Le préposé fédéral à la protection des données et à la transparence a admis devant la commission que les garanties en matière de droits fondamentaux étaient extrêmement solides. De l'avis de la majorité de la commission, elles sont d'ailleurs bien meilleures que dans la directive européenne. Par ailleurs, la Cour européenne des droits de l'homme admet les mesures de surveillance invasives à condition que les citoyens soient précisément informés de leur existence. On ne va pas prévenir les gens qu'ils vont être surveillés bien sûr, mais nul n'est censé ignorer la loi; on doit pouvoir s'attendre aux mesures de surveillance que les autorités de poursuite pénale peuvent mettre en oeuvre en cas de soupçons de crime grave.
La commission s'est aussi penchée sur la méthode dite du «Quick Freeze», que certains présentent comme une alternative à la conservation des données secondaires. Madame la présidente de la Confédération Sommaruga a parfaitement expliqué pourquoi cette méthode n'était pas adéquate: il serait impossible de savoir ce qui s'est passé dans les six ou douze mois ayant précédé le soupçon avéré. La commission a donc rejeté les propositions défendues par les minorités III et IV (Reimann Lukas) aux articles 19 et 26.
Les propositions de minorité I, défendues par Madame Leutenegger Oberholzer à l'article 19 et par moi-même à l'article 26, prévoient d'en rester au droit actuel, soit à un délai de six mois – ce délai ayant été repris dans les propositions des minorités II et III (Schneider Schüttel). Par 15 voix contre 8 et 0 abstention, la commission a rejeté le délai de six mois pour les données secondaires postales à l'article 19 et, par 13 voix contre 10 et 0 abstention, pour les données secondaires de télécommunications à l'article 26.
La proposition de la minorité II (Vischer Daniel) à l'article 26 vise à réduire à trois mois le délai actuel de conservation des données secondaires de télécommunication. La commission l'a rejetée, par 22 voix contre 1 et 0 abstention.
Enfin, les propositions des minorités IV et V (Vischer Daniel), aux articles 19 et 26, prévoient de supprimer totalement la possibilité de conserver les données secondaires. Pour les raisons précédemment évoquées, la commission les a rejetées, par 20 voix contre 3 et 0 abstention, à l'article 19 relatif aux données secondaires postales et, par 19 voix contre 4 et 0 abstention, à l'article 26 relatif aux données secondaires de télécommunication.
J'ai d'autres dispositions à commenter. Je vous prie de m'excuser pour la longueur de mes propos. Le contenu du bloc est néanmoins important. Je m'exprime encore sur les articles 2 et 8 de la loi. Monsieur Flach s'exprimera sur les autres dispositions du bloc.
A l'article 2 lettre c, la proposition de la minorité Reimann Lukas vise à ce que la loi ne s'applique pas aux opérateurs qui fournissent des services de télécommunication dits dérivés, c'est-à-dire qui permettent une communication unilatérale, par exemple le téléchargement de documents, ou multilatérale. A l'article 2 alinéa 2, une autre minorité emmenée par Monsieur Reimann Lukas propose à tout le moins d'exempter les fournisseurs non commerciaux.
La majorité de la commission vous invite à rejeter ces deux propositions.
La première aurait pour effet d'exclure du champ d'application des services importants dont ceux, par exemple, de Google ou de Facebook – excusez du peu! Or, ces fournisseurs proposent de plus en plus des services qui s'apparentent bel et bien à des télécommunications bi ou multilatérales, comme c'est le cas de leurs réseaux sociaux, de leurs messageries instantanées ou de la diffusion à grande échelle de documents. Bref, il s'agit de tous les services que fournissaient dans le monde réel les anciens PTT et que fournissent aujourd'hui, en partie, ses successeurs dont la Poste, mais aussi les opérateurs téléphoniques. Soutenir la première proposition de la minorité Reimann Lukas reviendrait à offrir un vaste champ libre aux criminels, qui pourraient recourir aux services des plus grands fournisseurs de services d'Internet – que dis-je, du monde! –, sans avoir à craindre une réelle surveillance.
Quant à la proposition qui prévoit d'exclure du champ d'application les fournisseurs non commerciaux, elle laisse aussi un vaste champ libre aux criminels, qui n'auraient qu'à s'installer confortablement au poste Internet public d'une bibliothèque, par exemple, pour ne pas avoir à craindre de surveillance. Il convient par ailleurs de rappeler que les fournisseurs de services qui seraient exemptés de mettre eux-mêmes sur pied les infrastructures de surveillance parce qu'ils sont de peu d'importance n'auraient qu'à tolérer une surveillance qui serait menée par les services de la Confédération, sans avoir eux-mêmes à la mettre sur pied. Dans tous les cas, les opérateurs privés, quels qu'ils soient, qui doivent tolérer ou mettre en place une surveillance, seront indemnisés équitablement, comme le commande l'article 38.
La commission a rejeté, par 15 voix contre 7 et 2 abstentions, les deux propositions défendues par la minorité Reimann Lukas.
Enfin, à l'article 8 lettre b, une minorité Reimann Lukas vise à ce que les tentatives de communication n'appartiennent pas aux données secondaires de télécommunication, qu'il s'agit de conserver. Il est vrai que ce n'est aujourd'hui pas le cas. Toutefois, de l'avis du Conseil fédéral et de la majorité de la commission, ces tentatives sont aussi très importantes pour identifier les auteurs potentiels, leurs actes et les lieux où ils se trouvent, pour reconstituer leur emploi du temps; ce sont autant de moyens de preuve dont l'utilité est incontestée sur le terrain. D'ailleurs, ce sont les acteurs actifs sur le terrain qui nous demandent de prévoir la conservation des

données secondaires qui se rapportent aux tentatives de télécommunication.
Je vous remercie, là aussi, de suivre la majorité de la commission, c'est-à-dire de rejeter la proposition de la minorité Reimann Lukas.

Flach Beat (GL, AG), für die Kommission: In Block 1 behandeln wir jetzt einige der tatsächlichen Änderungen, die wir im Bundesgesetz vornehmen wollen. Zum einen geht es um die Randdatenspeicherung, die bis jetzt sechs Monate gedauert hat, zum andern um eine Ausweitung auch auf sogenannte Verbindungsversuche.
In Artikel 2 Buchstabe c, Artikel 22 Absatz 3 sowie in Artikel 27 geht es um sogenannte abgeleitete Kommunikationsdienste. Das ist eines der Konzepte dieses Gesetzes, das eben vorsieht, dass eigentliche Telekommunikationsanbieter die Randdaten aufbewahren sollen und sogenannte abgeleitete Kommunikationsdienste – jetzt schauen wir in die Gegenwart und ein bisschen in die Zukunft – eben nur eine sogenannte Duldungspflicht haben. Das heisst, es ist eben nicht so, dass jedes kleine WLAN zu Hause, in der WG oder am Arbeitsplatz dann irgendwelche Randdaten aufbewahren muss. Wenn die Strafverfolgungsbehörde mit einer Verfügung eines Zwangsmassnahmengerichtes kommt – aufgrund eines konkreten Strafantrages und bei Vorliegen eines schweren Verbrechens –, kann sie beim Dienstleister eben Einsitz nehmen, kann sich in die Anlagen einstöpseln und auslesen, was da ist. Die Dienstleister müssen also allenfalls herausgeben, was sie sowieso herausgeben müssten. Der Antrag Reimann Lukas zu den drei genannten Bestimmungen wurde in der Kommission mit 14 zu 6 Stimmen abgelehnt.
Ich möchte hierzu auch darauf hinweisen, dass die Herausgabepflicht, die wir hier im Gesetz regeln, eigentlich eine Spezialbestimmung zu Artikel 265 der Strafprozessordnung ist, wonach jede Person, die im Besitze von Unterlagen, Gegenständen, Aufzeichnungen, Belegen usw. im Zusammenhang mit einer Straftat ist, diese herausgeben muss. Sinn und Zweck der Spezialbestimmung ist es natürlich, dass man bei Kommunikationsdienstleistern nicht jedes Mal über die allgemeine Herausgabepflicht (Art. 265 StPO) gehen muss, sondern über eine entsprechende Regelung für Kommunikationsdaten im Spezialgesetz verfügt. Darum macht es auch keinen Sinn, hier einzelne kleine Anbieter aus der Pflicht zu nehmen beziehungsweise sie von der Herausgabepflicht gemäss Büpf auszunehmen, weil sie keine kommerziellen Dienste anbieten. Das hat nichts damit zu tun, ob jemand kommerziell erfolgreich ist, sondern vielmehr damit, für welche Zwecke das Netz eben auch verwendet wird.
Ich komme noch zur Randdatenaufbewahrung im Bereich des Postdienstes: Herr Glättli hat ausgeführt, das sei eine hilflose Sache hier. Denn wenn jemand den Willen habe, sich da zu verstecken, dann könne er das auf eine CD brennen oder auf einem Stick verschlüsselt versenden; dann sei das sicher. Darum geht es aber gar nicht. Es geht einfach darum, dass man vielleicht nachschauen möchte, wie z. B. der Weg von gefälschten Medikamenten ist. Dann, glaube ich, ist es doch wieder interessant, dass die Strafverfolgungsbehörden in solchen Fällen ermitteln und auch tatsächlich auf Daten zugreifen können, ob das jetzt für Pakete oder für andere Briefpost ist.
Bei Artikel 19 Absatz 4bis haben wir noch eine Minderheit, die darauf abzielt, dass die gesammelten Randdaten an einem physisch sicheren Ort aufbewahrt werden sollen, und zwar eben in der Schweiz. Die Kommission hat diese Frage – wie auch die Randdatenproblematik überhaupt – lange beraten. Sie hat diesen Antrag mit 13 zu 8 Stimmen abgelehnt. Wahrscheinlich war schlicht die Tatsache ausschlaggebend, dass heute in dieser digitalen Welt der rein physische Ort, wo sich Daten auf einem Datenträger befinden, vermutlich nicht mehr so wahnsinnig wichtig ist; es geht eher um die Zugriffsfähigkeiten von Personen.
Zu den Randdaten in Artikel 26 haben wir mehrere Minderheiten. Die Kommission hat hier sehr lange darüber diskutiert, ob die Ausweitung auf zwölf Monate, ein Verbleiben bei sechs Monaten oder allenfalls sogar nur drei Monate sinnvoll seien. Ebenso ist die Möglichkeit des sogenannten Quick Freeze eingehend beraten worden. Zum Quick-Freeze-Verfahren muss man einfach noch sagen: Da weiss man nicht genau, was man bekommt. In der Kommission waren die Anhörungsteilnehmer unschlüssig darüber, was denn da alles ausgehändigt wird. Es kann also sehr gut sein, dass es anbieterabhängig ist, was man bei einem Quick-Freeze-Verfahren tatsächlich bekommt. Denn es ist ja nicht so, dass das sekundengenau einfach für die letzten paar Anrufe oder so gespeichert ist, sondern technisch sieht das je nach Anbieter und je nach System dann anders aus. Es kann sein, dass Sie dann sogar mehr haben, länger zurück gespeicherte Daten erhalten, als eigentlich im Büpf verlangt ist. Die Kommission ist hier, Sie haben es gehört, auf zwölf Monate gegangen.
Ich bitte Sie, überall der Mehrheit zu folgen.

Art. 2
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Brand, Egloff, Müri, Nidegger, Rickli Natalie)
Abs. 1
...
c. Streichen
...

Antrag der Minderheit
(Reimann Lukas, Brand, Egloff, Nidegger, Rickli Natalie, Schwander, Stamm)
Abs. 2
Personen nach Absatz 1 Buchstaben c, d und e sind nicht zur Mitwirkung verpflichtet, wenn sie die entsprechende Dienstleistung auf der fraglichen Anlage nicht kommerziell anbieten.

Art. 2
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Brand, Egloff, Müri, Nidegger, Rickli Natalie)
Al. 1
...
c. Biffer
...

Proposition de la minorité
(Reimann Lukas, Brand, Egloff, Nidegger, Rickli Natalie, Schwander, Stamm)
Al. 2
Les personnes visées par l'alinéa 1 lettres c, d et e ne sont pas tenues de collaborer pour autant qu'elles ne fournissent pas les prestations en question à des fins commerciales via les installations visées.

Abs. 1 – Al. 1

Le président (Rossini Stéphane, président): Le vote vaut également pour l'article 22 alinéa 3.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 093)
Für den Antrag der Mehrheit ... 128 Stimmen
Für den Antrag der Minderheit ... 41 Stimmen
(15 Enthaltungen)

Abs. 2 – Al. 2

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 094)
Für den Antrag der Minderheit ... 39 Stimmen
Dagegen ... 126 Stimmen
(20 Enthaltungen)

Art. 8
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Brand, Egloff, Nidegger, Schwander, Stamm)
...
b. ... die technischen Merkmale der zustande gekommenen Verbindung (Randdaten des Fernmeldeverkehrs); Verbindungsversuche gehören nicht zu den Randdaten;
...

Art. 8
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Brand, Egloff, Nidegger, Schwander, Stamm)
...
b. ... ainsi que les caractéristiques techniques de la communication établie (données secondaires de télécommunication); les tentatives de communication n'appartiennent pas aux données secondaires de télécommunication;
...

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 095)
Für den Antrag der Mehrheit ... 103 Stimmen
Für den Antrag der Minderheit ... 56 Stimmen
(26 Enthaltungen)

Art. 19
Antrag der Mehrheit
Abs. 1–3
Zustimmung zum Beschluss des Ständerates
Abs. 4
Zustimmung zum Entwurf des Bundesrates
Abs. 5
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 4
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit II
(Schneider Schüttel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Ruiz Rebecca, Schwaab, Vischer Daniel)
Abs. 4
... aufbewahren. Nach Ablauf dieser Frist sind sie zu löschen.

Antrag der Minderheit III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Abs. 4
... des Postverkehrs nach Anordnung vorübergehend aufbewahren.
Abs. 4ter
Die Randdaten nach Absatz 4 werden zur Löschung durch den Anbieter freigegeben, wenn eine Anordnung gemäss Absatz 3 nach drei Monaten nicht erfolgt ist oder nicht mehr zu erwarten ist.

Antrag der Minderheit IV
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer)
Abs. 4
Streichen

Antrag der Minderheit
(Schwaab, Chevalley, Flach, Kiener Nellen, Leutenegger Oberholzer, Schneider Schüttel, Vischer Daniel)
Abs. 4bis
Die Anbieterinnen bewahren die Randdaten des Postverkehrs in der Schweiz auf.

Art. 19
Proposition de la majorité
Al. 1–3
Adhérer à la décision du Conseil des Etats
Al. 4
Adhérer au projet du Conseil fédéral
Al. 5
Adhérer à la décision du Conseil des Etats

Proposition de la minorité I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 4
Adhérer à la décision du Conseil des Etats

Proposition de la minorité II
(Schneider Schüttel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Ruiz Rebecca, Schwaab, Vischer Daniel)
Al. 4
... mois. A l'expiration de ce délai, les données doivent être détruites.

Proposition de la minorité III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Al. 4
Les fournisseurs conservent provisoirement, sur ordre, les données secondaires postales définies par le Conseil fédéral en vertu de l'alinéa 3.
Al. 4ter
Ils sont habilités à supprimer les données secondaires visées à l'alinéa 4 s'il n'y a pas eu d'ordre au sens de l'alinéa 3 après trois mois ou s'il ne faut plus s'attendre à ce qu'il y en ait un.

Proposition de la minorité IV
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer)
Al. 4
Biffer

Proposition de la minorité
(Schwaab, Chevalley, Flach, Kiener Nellen, Leutenegger Oberholzer, Schneider Schüttel, Vischer Daniel)
Al. 4bis
Les fournisseurs conservent les données secondaires postales en Suisse.

Abs. 4, 4ter – Al. 4, 4ter

Le président (Rossini Stéphane, président): La proposition de la minorité II (Schneider Schüttel) a été retirée. Le vote sur la proposition de la minorité I (Leutenegger Oberholzer) vaut également pour les propositions de la même minorité à l'article 45 alinéa 3, au chiffre II chiffre 1 article 273 alinéa 3 et au chiffre II chiffre 2 article 70d alinéa 3.

Erste Abstimmung – Premier vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 096)
Für den Antrag der Mehrheit ... 104 Stimmen
Für den Antrag der Minderheit I ... 80 Stimmen
(1 Enthaltung)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 097)
Für den Antrag der Mehrheit ... 106 Stimmen
Für den Antrag der Minderheit III ... 68 Stimmen
(11 Enthaltungen)

Dritte Abstimmung – Troisième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 098)
Für den Antrag der Mehrheit ... 122 Stimmen
Für den Antrag der Minderheit IV ... 62 Stimmen
(1 Enthaltung)

Abs. 4bis – Al. 4bis

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 099)
Für den Antrag der Minderheit ... 83 Stimmen
Dagegen ... 102 Stimmen
(0 Enthaltungen)

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 22 Abs. 3
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Brand, Egloff, Müri, Nidegger, Rickli Natalie)
Betreiberinnen interner Fernmeldenetze müssen dem Dienst die ihnen vorliegenden Angaben liefern.

Art. 22 al. 3
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Brand, Egloff, Müri, Nidegger, Rickli Natalie)
Les exploitants de réseaux de télécommunication internes fournissent au service les indications dont ils disposent.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Art. 26 Abs. 1–5, 5bis, 5ter
Antrag der Mehrheit
Abs. 1–5
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Abs. 1 Bst. b
Streichen

Antrag der Minderheit I
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Abs. 5
... während sechs Monaten aufbewahren.

Antrag der Minderheit II
(Vischer Daniel)
Abs. 5
... während drei Monaten aufbewahren.

Antrag der Minderheit III
(Schneider Schüttel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Ruiz Rebecca, Schwaab, Vischer Daniel)
Abs. 5
... aufbewahren. Nach Ablauf dieser Frist sind sie zu löschen.

Antrag der Minderheit IV
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Abs. 5
Die Anbieterinnen müssen die Randdaten des Fernmeldeverkehrs nach Anordnung vorübergehend aufbewahren.
Abs. 5ter
Die Randdaten nach Absatz 5 werden zur Löschung durch den Anbieter freigegeben, wenn eine Anordnung gemäss Absatz 4 nach drei Monaten nicht erfolgt ist oder nicht mehr zu erwarten ist.

Antrag der Minderheit V
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Abs. 5
Streichen

Antrag der Minderheit
(Schwaab, Amherd, Chevalley, Flach, Kiener Nellen, Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Vischer Daniel)
Abs. 5bis
Die Anbieterinnen von Fernmeldediensten bewahren die Randdaten des Fernmeldeverkehrs in der Schweiz auf.

Art. 26 al. 1–5, 5bis, 5ter
Proposition de la majorité
Al. 1–5
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Al. 1 let. b
Biffer

Proposition de la minorité I
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Al. 5
... durant six mois.

Proposition de la minorité II
(Vischer Daniel)
Al. 5
... durant trois mois.

Proposition de la minorité III
(Schneider Schüttel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Ruiz Rebecca, Schwaab, Vischer Daniel)
Al. 5
... mois. A l'expiration de ce délai, les données doivent être détruites.

Proposition de la minorité IV
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Al. 5
Les fournisseurs conservent provisoirement, sur ordre, les données secondaires de télécommunication.
Al. 5ter
Ils sont habilités à supprimer les données secondaires visées à l'alinéa 5 s'il n'y a pas eu d'ordre au sens de l'alinéa 4

après trois mois ou s'il ne faut plus s'attendre à ce qu'il y en ait un.

Proposition de la minorité V
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Al. 5
Biffer

Proposition de la minorité
(Schwaab, Amherd, Chevalley, Flach, Kiener Nellen, Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Vischer Daniel)
Al. 5bis
Les fournisseurs de services de télécommunication conservent les données secondaires de télécommunication en Suisse.

Abs. 1, 5 – Al. 1, 5

Le président (Rossini Stéphane, président): La proposition de la minorité III (Schneider Schüttel) a été retirée. Le vote sur la proposition de la minorité I (Schwaab) vaut également pour les propositions de la même minorité à l'article 45 alinéa 3, au chiffre II chiffre 1 article 273 alinéa 3 et au chiffre II chiffre 2 article 70d alinéa 3.

Erste Abstimmung – Premier vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 100)
Für den Antrag der Minderheit I ... 128 Stimmen
Für den Antrag der Minderheit II ... 49 Stimmen
(8 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 101)
Für den Antrag der Mehrheit ... 95 Stimmen
Für den Antrag der Minderheit I ... 87 Stimmen
(3 Enthaltungen)

Le président (Rossini Stéphane, président): Le vote sur la proposition de la minorité IV (Reimann Lukas) vaut également pour les propositions de la même minorité à l'article 26 alinéa 5ter, au chiffre II chiffre 1 article 273 alinéas 1 et 3 et au chiffre II chiffre 2 article 70d alinéas 1 et 3.

Dritte Abstimmung – Troisième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 102)
Für den Antrag der Mehrheit ... 112 Stimmen
Für den Antrag der Minderheit IV ... 65 Stimmen
(8 Enthaltungen)

Le président (Rossini Stéphane, président): Le vote sur la proposition de la minorité Vischer Daniel vaut également pour les propositions de la même minorité aux articles 27 alinéa 2, 28 alinéa 2, 29 alinéa 2, 39 alinéa 1 lettre b, 45 alinéa 3, au chiffre II chiffre 1 article 273 alinéa 3 et au chiffre II chiffre 2 article 70d alinéa 3.

Vierte Abstimmung – Quatrième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 103)
Für den Antrag der Mehrheit ... 121 Stimmen
Für den Antrag der Minderheit V ... 58 Stimmen
(6 Enthaltungen)

Abs. 5bis – Al. 5bis

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 104)
Für den Antrag der Minderheit ... 102 Stimmen
Dagegen ... 83 Stimmen
(0 Enthaltungen)

Abs. 5ter – Al. 5ter

Le président (Rossini Stéphane, président): Cet alinéa est caduc à la suite du rejet de la proposition de la minorité IV.

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 27
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer)
Abs. 2
Streichen

Antrag der Minderheit
(Rickli Natalie, Brand, Egloff, Kiener Nellen, Müri, Nidegger, Reimann Lukas, Vischer Daniel)
Abs. 3
Streichen

Antrag der Minderheit
(Reimann Lukas, Brand, Egloff, Müri, Nidegger, Rickli Natalie)
Abs. 1–3
Streichen

Art. 27
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer)
Al. 2
Biffer

Proposition de la minorité
(Rickli Natalie, Brand, Egloff, Kiener Nellen, Müri, Nidegger, Reimann Lukas, Vischer Daniel)
Al. 3
Biffer

Proposition de la minorité
(Reimann Lukas, Brand, Egloff, Müri, Nidegger, Rickli Natalie)
Al. 1–3
Biffer

Abs. 2 – Al. 2

Le président (Rossini Stéphane, président): La proposition de la minorité Vischer Daniel a déjà été rejetée à l'article 26 alinéa 5.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Abs. 3 – Al. 3

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 105)
Für den Antrag der Mehrheit ... 106 Stimmen
Für den Antrag der Minderheit ... 72 Stimmen
(6 Enthaltungen)

Abs. 1–3 – Al. 1–3

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 106)
Für den Antrag der Mehrheit ... 127 Stimmen
Für den Antrag der Minderheit ... 43 Stimmen
(15 Enthaltungen)

Art. 28
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Abs. 2
Streichen

Art. 28
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Al. 2
Biffer

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Art. 29
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Abs. 2
Streichen

Art. 29
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Al. 2
Biffer

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Art. 39 Abs. 1 Bst. b
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit I
(Schneider Schüttel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Ruiz Rebecca, Schwaab, Vischer Daniel)
b. der Pflicht zur Aufbewahrung oder zur Löschung der Daten ...

Antrag der Minderheit II
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Streichen

Art. 39 al. 1 let. b
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité I
(Schneider Schüttel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Ruiz Rebecca, Schwaab, Vischer Daniel)
b. ... obligation de conserver ou de détruire des données ...

Proposition de la minorité II
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Biffer

Le président (Rossini Stéphane, président): La proposition de la minorité I (Schneider Schüttel) a été retirée. La proposition de la minorité II (Vischer Daniel) a déjà été rejetée à l'article 26 alinéa 5.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Art. 45
Antrag der Mehrheit
Abs. 1, 2, 4, 5
Zustimmung zum Beschluss des Ständerates
Abs. 3
Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 3
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit II
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Abs. 3
Streichen

Antrag der Minderheit III
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Abs. 3
Streichen

Art. 45
Proposition de la majorité
Al. 1, 2, 4, 5
Adhérer à la décision du Conseil des Etats
Al. 3
Adhérer au projet du Conseil fédéral

Proposition de la minorité I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 3
Adhérer à la décision du Conseil des Etats

Proposition de la minorité II
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Al. 3
Biffer

Proposition de la minorité III
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Al. 3
Biffer

Le président (Rossini Stéphane, président): La proposition de la minorité I (Leutenegger Oberholzer) a déjà été rejetée à l'article 19 alinéa 4. La proposition de la minorité II (Schwaab) et la proposition de la minorité III (Vischer Daniel) ont déjà été rejetées à l'article 26 alinéa 5.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

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

Ziff. I; II Einleitung
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. I; II introduction
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Ziff. II Ziff. 1 Art. 273
Antrag der Mehrheit
Abs. 1, 2
Zustimmung zum Beschluss des Ständerates
Abs. 3
Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Abs. 1
Besteht der Verdacht, ein Verbrechen oder Vergehen oder eine Übertretung nach Artikel 179septies StGB sei begangen worden oder stehe bevor, so kann die Polizei oder Staatsanwaltschaft die Aufbewahrung der Randdaten des Fernmeldeverkehrs sowie des Postverkehrs der überwachten Person gemäss Artikel 26 Absatz 5 des Bundesgesetzes vom ... betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) und gemäss Artikel 19 Absatz 4 Büpf verlangen.

Antrag der Minderheit I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 3
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit II
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Abs. 3
Unverändert

Antrag der Minderheit III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Abs. 3
Aufheben

Antrag der Minderheit IV
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Abs. 3
Aufheben

Ch. II ch. 1 art. 273
Proposition de la majorité
Al. 1, 2
Adhérer à la décision du Conseil des Etats
Al. 3
Adhérer au projet du Conseil fédéral

Proposition de la minorité
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Al. 1
Lorsque des soupçons laissent présumer qu'un crime, un délit ou une contravention au sens de l'article 179septies CP a été commis ou est sur le point de l'être, la police ou le ministère public peut exiger la conservation des données secondaires postales au sens de l'article 19 alinéa 4 de la loi fédérale du ... sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et des données secondaires de télécommunication au sens de l'article 26 alinéa 5 LSCPT de la personne surveillée.

Proposition de la minorité I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 3
Adhérer à la décision du Conseil des Etats

Proposition de la minorité II
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Al. 3
Inchangé

Proposition de la minorité III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Al. 3
Abroger

Proposition de la minorité IV
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Al. 3
Abroger

Le président (Rossini Stéphane, président): Les propositions des cinq minorités ont déjà été rejetées.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. II Ziff. 2 Art. 70d
Antrag der Mehrheit
Abs. 1, 2
Zustimmung zum Beschluss des Ständerates
Abs. 3
Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Abs. 1
Besteht der Verdacht, ein Verbrechen oder Vergehen oder eine Übertretung nach Artikel 179septies StGB sei begangen worden oder stehe bevor, so kann der Untersuchungsrichter die Aufbewahrung der Randdaten des Fernmeldeverkehrs sowie des Postverkehrs der überwachten Person gemäss Artikel 26 Absatz 5 des Bundesgesetzes vom ... betreffend die Überwachung des Post- und Fernmeldeverkehrs (Büpf) und gemäss Artikel 19 Absatz 4 Büpf verlangen.

Antrag der Minderheit I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 3
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit II
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Abs. 3
Unverändert

Antrag der Minderheit III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Abs. 3
Aufheben

Antrag der Minderheit IV
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Abs. 3
Aufheben

Ch. II ch. 2 art. 70d
Proposition de la majorité
Al. 1, 2
Adhérer à la décision du Conseil des Etats
Al. 3
Adhérer au projet du Conseil fédéral

Proposition de la minorité
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Al. 1
Lorsque des soupçons laissent présumer qu'un crime, un délit ou une contravention au sens de l'article 179septies CP a été commis ou est sur le point de l'être, le juge d'instruction peut exiger la conservation des données secondaires postales au sens de l'article 19 alinéa 4 de la loi fédérale du ... sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et des données secondaires de télécommunication au sens de l'article 26 alinéa 5 LSCPT de la personne surveillée.

Proposition de la minorité I
(Leutenegger Oberholzer, Kiener Nellen, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 3
Adhérer à la décision du Conseil des Etats

Proposition de la minorité II
(Schwaab, Flach, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas, Schneider Schüttel, Vischer Daniel)
Al. 3
Inchangé

Proposition de la minorité III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Al. 3
Abroger

Proposition de la minorité IV
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Reimann Lukas)
Al. 3
Abroger

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Block 2 – Bloc 2
Govware und Imsi-Catcher
Chevaux de Troie utilisés par l'Etat (Govware) et IMSI-Catcher

Leutenegger Oberholzer Susanne (S, BL): Ich spreche zu zwei Minderheitsanträgen von mir, zuerst zu jenem zu den Artikeln 269bis Absatz 2 und 269ter Absatz 4. Es geht hier darum, dass wir mit einer Statistik kontrollieren können, ob sich die Überwachung, ob sich der Einsatz lohnt oder nicht. Es wurde bis jetzt immer geltend gemacht, die Überwachung sei sehr effizient, das würde auch das öffentliche Interesse rechtfertigen. Ich beantrage Ihnen, dass man nicht nur eine Statistik über diese Überwachungen führt, sondern dass man diese Statistik – wie es sich sowieso gehört, finde ich – öffentlich zugänglich macht, dass man den Einsatz und die gerichtliche Verwertung ebenfalls erfasst. Nur so wissen wir, ob sich die Überwachung lohnt und wie der Kosten-Nutzen-Vergleich aussieht. Ich bitte Sie, der Minderheit zu folgen.

Der zweite Minderheitsantrag, auch das ist eine zentrale Frage, betrifft Artikel 269ter Absätze 1, 5 und 6. Mit meiner Minderheit will ich sicherstellen, dass Govware, die eingeschleust wird, nicht in Datenverarbeitungssysteme eingeschleust werden darf. Das heisst, die Systemintegrität muss gesichert sein. Nach allen Rückfragen in der Kommission und bei allen Papieren, die verteilt worden sind, muss ich sagen – die Kommissionssprecher werden mich vielleicht korrigieren –: Wir haben weder gesetzliche Garantien dafür noch eine Kontrolle, noch die Gewähr. Ich glaube, das müssen auch die Kommissionssprecher bestätigen.
Ob die Entwicklung in der Schweiz möglich ist oder nicht, ist unklar. Wie die Kontrolle effektiv erfolgen soll, ist auch unklar. Damit stellen sich zahlreiche Fragen in Bezug auf die Sicherheit und die rechtliche Absicherung. Letztlich wissen wir nicht einmal, wer schlussendlich auf die Instrumente Zugriff hat. Nachdem ich jetzt zur Kenntnis nehmen muss, wie grossen Zugriff die NSA sogar auf unsere Infrastrukturen hat, ohne dass das in der Schweiz wirklich zur Kenntnis genommen wird, muss ich sagen: Man kann nicht ausschliessen, dass sie schlussendlich auch auf diese programmierte Software Zugriff haben kann.
Ich bitte Sie, hier grössere Sicherheitskontrollen einzubauen und den Auftrag dazu auch im Gesetz zu verankern.

Reimann Lukas (V, SG): Ich habe den Antrag der Minderheit II bei Artikel 269bis gestellt, wo es um den Einsatz von besonderen technischen Geräten zur Überwachung des Fernmeldeverkehrs geht.
Es geht hier insbesondere um den sogenannten Imsi-Catcher. Ein Imsi-Catcher schiebt sich im Handynetz zwischen die Mobiltelefone in der Umgebung und das eigentliche Mobilfunknetz. Er ermöglicht die sofortige Identifizierung der Netzteilnehmer, die Erstellung eines Bewegungsprofils und das Mithören von Handyanrufen. Der Einsatz solcher Geräte ist höchst problematisch. Klar wird dies, wenn man sich eine gesetzliche Norm vorstellt, die es der Polizei erlauben würde, auf einen Schlag die Identität aller Personen, die sich in einem bestimmten Gebiet aufhalten, zu kontrollieren und alle Namen zu protokollieren. Nachdem heute fast jede Person ein Handy auf sich trägt, läuft der Einsatz eines solchen Imsi-Catchers auf eine flächendeckende Personenkontrolle hinaus, ohne dass es die Betroffenen merken.
Ein weiterer Aspekt sind unbeteiligte Dritte, die einen Notruf tätigen wollen und sich mit dem Imsi-Catcher verbinden. Diese Notrufe können nicht garantiert mit der Notrufzentrale verbunden werden. Dies widerspricht Artikel 16 des Fernmeldegesetzes und beschneidet den Umfang der Grundversorgung, wonach der Zugang zu Notrufdiensten gewährleistet werden soll. Auch eingehende SMS und eingehende Anrufe können dementsprechend nicht empfangen werden. Man hat im Ausland gesehen, dass plötzlich Tausende Personen, die sich zur falschen Zeit am falschen Ort befunden haben, vorgeladen und von der Polizei befragt wurden. Wenn jetzt hier vor dem Bundeshaus etwas passiert, dann sind wir hier drin – alle, die ein aktives Handy auf sich tragen – plötzlich Verdächtige.
Bei Artikel 269ter habe ich den Antrag der Minderheit III zum Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs gestellt. Wir sprechen hier vom Bundestrojaner. In der Eintretensdebatte haben wir ja bereits darüber gesprochen. Beim Bundestrojaner werden gezielt Sicherheitslücken gefunden und dann auch geheim gehalten. Wenn man also eine Sicherheitslücke in einem Android- oder Windowsphone findet, dann nützt man diese aus und versucht, auf das Gerät zuzugreifen, statt dass man der Bevölkerung sagt: «Hey, eure mobilen Geräte sind nicht sicher, die haben eine Sicherheitslücke, und das können sich Kriminelle zunutze machen und haben es in der Vergangenheit auch getan.»
Weiter stellt sich die Frage, ob die Beweise überhaupt verwertbar sind. Wenn auch Dritte Zugriff haben und auch Dritte Sicherheitslücken ausnutzen und auf ein Gerät zugreifen können, dann können natürlich auch Dritte auf dem Computer etwas manipulieren. Man fördert hier also die Ar-

beit von Kriminellen und gibt vor, die Arbeit von Kriminellen bekämpfen zu wollen. Für was alles solche Programme verwendet werden können, das wurde gerade vor Kurzem sichtbar, als die Atomverhandlungen in Genf von irgendjemandem ausspioniert wurden.
Es ist natürlich auch so, dass diese Trojaner so programmiert werden können, dass alle Spuren verwischt werden und man nachher gar nicht auswerten kann, was gemacht worden ist, was verändert worden ist, wo zugegriffen worden ist. Das sind technische Probleme; da stimmen die technische und die juristische Linie nicht überein.
Wir bitten hier um Zurückhaltung, und ich bitte deshalb um Zustimmung zu meinem Minderheitsantrag.

Vischer Daniel (G, ZH): Wir sind jetzt beim zweiten wichtigen Thema neben der Vorratsdatenspeicherung. Die entsprechende Frist haben Sie ja jetzt auf zwölf Monate erhöht. Ich weiss nicht, ob das ein kluger Entscheid war. Damit haben Sie natürlich die Gegnerschaft gegen dieses Gesetz endgültig besiegelt. Sie wollen ja jetzt die Vorratsdatenspeicherung sogar ausbauen.
Wir sind also beim Staatstrojaner. Das war ja das Kernanliegen des Bundesrates bei dieser Gesetzesänderung. Das Hauptargument ist: gleich lange Spiesse wie die Verbrecher. Man redet von schwerer Kriminalität.
Wir sind nicht a priori gegen einen Staatstrojaner. Das heisst, dass auch auf Computer zugegriffen werden kann – unter eingeengtesten Bedingungen. Aber Sie sind gar nicht bereit, überhaupt den Diskurs zu eröffnen. Wir haben in der Kommission gemerkt, dass es zwischen den Polizeien dieses Landes einen Streit gibt, wie man sich überhaupt diesen Staatstrojaner vorstellen soll. Ist es nur über eine Wanze möglich – das behaupten die einen –, Zugriff auf die Computer zu haben, oder ist es möglich über Software? Das haben wir mit Erstaunen zur Kenntnis genommen, dass einige sagen, über Software sei das gar nicht möglich. Wir legiferieren also etwas, von dem wir technisch nicht einmal wissen, ob es praktikabel ist.
Und nun kommt der Haupteinwand: Es sind keine einschränkenden Bestimmungen legiferiert worden, welche die Zweckentfremdung der Bestimmung des Einsatzes verunmöglichen. Die Mehrheit hat alles abgelehnt; ich verweise auf die Anträge der Minderheit Leutenegger Oberholzer. Vor diesem Hintergrund muss man sagen: Sie wollen einen Staatstrojaner, wie wir ihn beim Nachrichtendienstgesetz haben, Sie wollen einen unkontrollierten Staatstrojaner, ohne dass Sie Gewähr haben, tatsächlich die Daten gemäss ihrer strafprozessualen Bestimmung kontrollieren zu können.
Frau Bundespräsidentin, wenn Sie sagen, niemand habe Missbräuche aufzählen können: Ja, 1986 hätte Ihnen auch niemand Missbräuche bezüglich Fichen aufzählen können. Es liegt in der Natur der Sache, dass es eben schwierig ist, solche Missbräuche festzustellen, weil es oft nur Zufallsfunde sind oder Aktionen wie diejenige von Snowden – ohne dass ich das jetzt vergleichen möchte –, die überhaupt solche Missbräuche auf den Tisch bringen.
Es gibt nun einen Antrag meiner Minderheit, der einen strengeren Deliktskatalog will, das ist der Antrag der Minderheit II zu Artikel 269ter Absatz 1 Buchstabe b der Strafprozessordnung. Sie sagen, es betreffe nur Schwerkriminalität. Das stimmt ja gar nicht. Sie haben einen Deliktskatalog, der relativ gesehen sehr offen ist, der sich nicht auf Gewaltdelikte konzentriert. Deswegen ist eine Bedingung von uns: wenn Staatstrojaner, dann nur unter eingeschränktem Deliktskatalog. Wenn Sie sagen, meiner gehe zu weit, dann machen Sie einen entsprechend besseren Vorschlag auf der Basis Gewaltkriminalität/Schwerkriminalität. Damit schaffen Sie eine Differenz zum Ständerat. Denn es ist Beliebigkeitstheater, wenn Herr Staatsanwalt Hansjakob landauf, landab sagt: «Ja, das stimmt. An sich könnte man einen strengeren Katalog machen, aber das bringt dann doch nichts, und man weiss nicht, wo abgrenzen.» Da muss man sich entscheiden.
In diesem Sinne empfehle ich Ihnen dringend, den Antrag der Minderheit II anzunehmen, damit diese Diskussion in der Differenzbereinigung noch einmal geführt werden kann.
Ein weiterer Punkt: Ich verlange ein Verwertungsverbot. Das ist eigentlich eine Selbstverständlichkeit, die aber nicht gilt, wenn das nicht explizit verankert ist. Dieses Verwertungsverbot verlangt, dass Daten nicht verwertet werden dürfen, die über eine Nichteinhaltung des Gesetzes gemäss den Einschränkungen, wie wir sie wollen, beschafft worden sind. Die Mehrheit lehnt dies ab. Warum? Das heisst, man nimmt das Beweisverwertungsverbot gar nicht ernst, man ist gar nicht bereit, überhaupt auf die Probleme einzugehen, nämlich dass wir im Strafprozess mit einem sehr sensiblen Artefakt konfrontiert sind. Dabei kann es eben nicht einfach so hergehen, dass am Schluss alles verwertet wird, was halt dann auf dem Tisch liegt.
Deswegen haben wir diesen Minderheitsantrag eingereicht, dessen Annahme für uns eine Conditio sine qua non ist, um Staatstrojaner überhaupt ernsthaft in Erwägung ziehen zu können.
Hier sind wir tatsächlich an einem Triangulationspunkt dieser Vorlage angelangt. Wir sind hier nicht einfach am Punkt, an dem wir sagen können: «Selbstverständlich brauchen wir eine bessere Handhabe für die Verbrechensbekämpfung – es spielt ja keine Rolle, wie!» Das aber machen Sie, wenn Sie den Minderheitsanträgen Leutenegger Oberholzer und Vischer Daniel nicht zustimmen: Dann führen Sie einen Staatstrojaner ein, bei dem Sie keine Gewähr haben zu wissen, wer welche Daten wie beschafft. Dann sind wir so weit wie beim unsäglichen Nachrichtendienstgesetz.
Genau das können wir nicht wollen. Deswegen müssen wir am Schluss zum Staatstrojaner Nein sagen, wenn die anderen Minderheitsanträge nicht angenommen werden.

Kiener Nellen Margret (S, BE): Ich vertrete meine Minderheit bei Artikel 269ter Absatz 1bis sowie die Minderheit Leutenegger Oberholzer bei Absatz 6 desselben Artikels. Es geht um sehr heikle Fragen. Es geht um die Sicherheit und die Reputation der Schweiz, sollte sie denn auch Staatstrojaner oder Govware einsetzen.
Die Minderheit bei Absatz 1bis bittet Sie, die Beschaffungsvielfalt einzuschränken. Wir beantragen Ihnen, dass solche «besonderen Informatikprogramme ... weder bei einer Behörde eines Landes beschafft werden, dessen Nachrichtendienste eine grossangelegte Fernmeldeüberwachung betreiben, noch bei einem Unternehmen mit Sitz in einem solchen Land». Diese Einschränkung gilt auch für Artikel 70ter Absatz 1bis des Militärstrafprozesses, auf der Fahne in Deutsch auf Seite 51.
Das Resultat der Abstimmung über den Antrag, den diese Minderheit aufgenommen hat, zeigt das grosse Unbehagen bei diesem Thema in Ihrer vorberatenden Kommission: 10 zu 6 Stimmen bei 7 Enthaltungen. Das bringt, meine ich, ein grosses Unbehagen zum Ausdruck.
Wir liessen uns bei der Formulierung des Antrages auch von den als sehr sorgfältig beurteilten Kriterien der Vertreter der Kantonspolizei Zürich leiten, die für Auswahl und Beschaffung zuständig sind und in den Anhörungen bei uns aussagten.
Es wurde uns in der Kommission entgegengehalten, dass die Formulierung «eine grossangelegte Fernmeldeüberwachung» ein unbestimmter Rechtsbegriff sei. Es wurde aber kein Alternativvorschlag, kein Verbesserungsvorschlag zu diesem unbestimmten Rechtsbegriff vorgebracht. Ich möchte Sie daher bitten: Unterstützen Sie die Minderheit, schon nur, um eine Differenz zu bilden, damit dann in der weiterführenden Differenzbereinigung gegebenenfalls dieser unbestimmte Rechtsbegriff noch präzisiert und geschärft werden kann. Denn sicher ist – und das möchte ich zu den Materialien geben –, dass die Minderheit der Auffassung ist, dass die Schweiz keinen Staatstrojaner und keine Govware von den USA oder von Israel kaufen darf. Bezüglich der anderen Länder möchten wir sicher Kriterien bewertet und zugrunde gelegt haben, damit die Schweiz diese nicht von ei-

nem Land kauft, das sich in aktiver Kriegführung befindet oder in interne bewaffnete Konflikte verwickelt ist.
Ich komme zur Minderheit bei Absatz 6. Es dürfen nur in der Schweiz entwickelte Programme zum Einsatz gelangen. Das ist jetzt eine noch viel engere Einschränkung, die Ihnen diese Minderheit beliebt macht, und dies mit guten Gründen. Das ist nichts anderes als Swissness, das ist Swissness pur. Wir finanzieren über das Bundesbudget ja unsere beiden hervorragenden Eidgenössischen Technischen Hochschulen in Zürich und in Lausanne. Wir wollen Weltspitze sein, und wir sind Weltspitze in einigen technologischen Gebieten. In der Schweiz wird investiert in die Forschung, in die Technologieentwicklung, und zwar von der öffentlichen Hand wie von Privaten. Die Minderheit ist deshalb dezidiert der Auffassung, dass sich die Schweiz als neutraler und unabhängiger Staat mit ihren Eidgenössischen Technischen Hochschulen sehr gut positionieren kann in der Produktion von solcher Govware, die dann auch von anderen Staaten als unverdächtig übernommen werden kann.
Ich bitte Sie, die beiden Minderheitsanträge anzunehmen.

Lüscher Christian (RL, GE): Le 16 avril 2015, lors des travaux de la Commission des affaires juridiques, nous avons discuté de la répartition des compétences entre les cantons et la Confédération, et de l'autonomie des premiers pour la responsabilité de l'achat et de la mise à disposition des logiciels espions.
La majorité de la commission a décidé de donner cette compétence à la Confédération. Ma minorité quant à elle prévoit d'attribuer cette compétence aux cantons.
La question des différentes règles d'adjudication des marchés publics a été rapidement, peut-être trop rapidement, abordée en commission. Or, cette problématique est d'une grande complexité. Il existe de grandes différences entre les cantons ainsi que des enjeux importants selon que la compétence est attribuée à la Confédération ou aux cantons. A la réflexion, je considère que ces points ont été insuffisamment discutés en commission. Par conséquent, je retire ma proposition de minorité pour permettre le maintien de la divergence. J'invite donc la commission soeur du Conseil des Etats à approfondir cette question.

Rickli Natalie Simone (V, ZH): Herr Lüscher, ich habe verstanden, dass Sie Ihren Minderheitsantrag zurückziehen wollen, was ich sehr schade finde, weil er inhaltlich völlig richtig ist. Sie wollten, dass der Ständerat noch einmal darüber debattiert; das finde ich auch richtig. Wenn Sie jetzt der Mehrheit zustimmen, haben Sie dann keine Bedenken, dass der Bund tatsächlich Informatikprogramme beschafft und auch betreibt? Haben Sie die Informationen der Kantonspolizei Zürich gesehen, nach deren Ansicht es nicht möglich ist, dass die Bundesverwaltung den erforderlichen Pikettdienst gewährleistet? Bisher war es ja so, dass für die Beschaffung dieser Software die Kantone verantwortlich waren. Unterstützen Sie inhaltlich eigentlich immer noch den Antrag der Minderheit, zu der auch ich gehöre?

Lüscher Christian (RL, GE): Tout d'abord, je suis très flatté, Madame Rickli, que vous estimiez regrettable que je retire une proposition de minorité; j'en prends note.
En outre, j'ai effectivement bien entendu durant les travaux de la commission quelle était la position de la police cantonale zurichoise, et c'est précisément pour que cette position puisse aussi être analysée par le Conseil des Etats que je retire ma proposition de minorité. Si je ne le faisais pas, le Conseil des Etats serait privé de la possibilité d'analyser cette question. Or, comme vous le relevez vous-même, c'est une question extrêmement importante, qui sera donc débattue aussi au Conseil des Etats.

Le président (Rossini Stéphane, président): La proposition de la minorité Lüscher au chiffre II chiffre 1 article 269quater alinéas 4 et 5 et au chiffre II chiffre 2 article 70quater alinéas 4 et 5 a été reprise par Madame Natalie Rickli.

Schneider Schüttel Ursula (S, FR): Ich habe die etwas schwierige Aufgabe, die Meinung der SP-Fraktion bekanntzugeben. Die SP-Fraktion ist in der Frage des Einsatzes von Govware oder Imsi-Catchern, um die es hier in Block 2 geht, geteilter Meinung. Ich versuche, die beiden Meinungen darzustellen.
Ein Teil der SP-Fraktion wird aus grundsätzlichen Überlegungen den Einsatz von Govware und namentlich Artikel 269ter der Strafprozessordnung ablehnen bzw. in Absatz 1 die Minderheit I (Leutenegger Oberholzer) unterstützen. Dabei geht es diesem Teil der Fraktion um den hoch zu wertenden Schutz der Grundrechte, namentlich der Persönlichkeitsrechte der potenziell von einer Überwachung betroffenen Personen. Dies können je nach Standpunkt sehr viele sein. Es geht diesem Teil der Fraktion auch um einen weitreichenden Datenschutz. Der Eingriff in die Grundrechte durch die möglichen Überwachungsmassnahmen durch Govware erscheint vielen in unserer Fraktion als zu gross.
Der andere Teil der SP-Fraktion – zu dem mit der Mehrheit unserer Delegation in der Kommission für Rechtsfragen des Nationalrates auch ich gehöre – achtet die Grundrechte, die Persönlichkeitsrechte und den Datenschutz ebenso. Wir sind aber der Meinung, dass die Strafverfolgungsbehörden zur Bekämpfung der schweren Kriminalität und zur Aufklärung von schweren Straftaten über effiziente Mittel verfügen müssen, um namentlich zu verschlüsselter Kommunikation, zum Beispiel über Skype oder Whatsapp, Zugang haben zu können. Wichtig ist, dass namentlich mit dem in der Kommission erarbeiteten neuen Artikel 269quater – Sie finden ihn auf Seite 40 der deutschen Fahne – effiziente Massnahmen gegen einen möglichen Missbrauch von Govware eingeführt werden. So sollen die Informatikprogramme die Überwachung lückenlos und unveränderbar protokollieren, die Ausleitung der Daten muss gesichert erfolgen, und die Strafverfolgungsbehörden müssen sicherstellen, dass der Quellcode überprüft werden kann. Damit kann sichergestellt werden, dass das Programm nur das gesetzlich Zulässige tun kann. Nebst den verfahrensrechtlichen Voraussetzungen in Artikel 269ter der Strafprozessordnung werden somit auch die technischen Bedingungen für den Einsatz von Govware festgelegt, was grundsätzlich von der SP-Fraktion begrüsst wird.
Hinzuweisen ist an dieser Stelle zudem auf das Beweisverwertungsverbot, das aus Artikel 141 der Strafprozessordnung hervorgeht – es besteht übrigens schon heute –, sofern die verfahrensrechtlichen Voraussetzungen beim Einsatz von Govware missachtet werden. Das Beweisverwertungsverbot bedeutet, dass widerrechtlich erlangte Daten im Strafprozess nicht verwendet werden dürfen. Letztlich ist es auch eine Frage des Vertrauens in die Institutionen, dass Sie das Notwendige vorkehren, um Missbräuche zu verhindern beziehungsweise diese in den Griff zu bekommen.
An dieser Stelle möchte ich noch einmal wiederholen, was in der Eintretensdebatte auch schon gesagt wurde: Das Büpf ist nicht das Nachrichtendienstgesetz. Es geht um rückwirkende und nicht um präventive Überwachung. Es geht um eine Überwachung, die gemäss Artikel 269ter nur bei ganz bestimmten Voraussetzungen angeordnet werden kann, also bei dringendem Verdacht, dass eine Straftat gemäss einem bestimmten Katalog begangen wurde, dass diese Straftat so schwer war, dass eine Überwachung gerechtfertigt ist, und wenn alle bisherigen Untersuchungshandlungen erfolglos geblieben sind, die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden.
Die SP-Fraktion unterstützt in diesem Block mehrheitlich noch einige gegenüber dem Entwurf des Bundesrates oder der Version des Ständerates weiter gehende Anforderungen, so gemäss dem Minderheitsantrag Kiener Nellen bei Artikel 269ter bezüglich Beschaffung von Govware wie auch die weiter gehenden Anforderungen an die Statistiken gemäss den entsprechenden Minderheitsanträgen Leutenegger Oberholzer.

Huber Gabi (RL, UR): In diesem Block bewegen wir uns in der eidgenössischen Strafprozessordnung, und ich äussere mich zu den Artikeln 269ter und 269quater.
Artikel 269ter soll der Staatsanwaltschaft die Möglichkeit einräumen, im Rahmen von Strafverfahren unter ganz bestimmten Bedingungen die Verwendung von besonderen Informatikprogrammen, sogenannter Government Software oder Govware, anzuordnen. Dabei geht es darum, diese Programme in ein Datenverarbeitungssystem einzuführen, um den Inhalt der Kommunikation und der Randdaten abzufangen und zu lesen. Diese Aufgabe übernimmt die Polizei im Auftrag der Staatsanwaltschaft. Eine Mitwirkung der Fernmeldedienstanbieter ist nicht erforderlich. Der Einsatz von Govware erfolgt ausschliesslich im Rahmen eines Strafverfahrens und niemals präventiv. Ohne Govware sind bestimmte Arten von Telefonie nicht lesbar oder nicht abhörbar. Vor dem Inkrafttreten der eidgenössischen Strafprozessordnung haben Strafverfolgungsbehörden von Bund und Kantonen bereits vereinzelt Govware eingesetzt. Ob die nun geltende Strafprozessordnung den Einsatz zulässt, ist umstritten. Mit der Vorlage würde diese Frage geklärt. Wichtig zu wissen: Der Einsatz von Govware wäre nur wegen den in Artikel 286 Absatz 2 der Strafprozessordnung katalogisierten Straftatbeständen erlaubt, und das sind Straftaten, zu deren Verfolgung verdeckte Ermittlung erfolgen kann. Der Einsatz von Govware darf zudem nur subsidiär zu den klassischen Überwachungsmassnahmen erfolgen.
Bei Artikel 269quater ist der Kommission eine echte Verbesserung gelungen, so meine ich. Es wurden nämlich Anforderungen an die besonderen Informatikprogramme zur Überwachung des Fernmeldeverkehrs definiert und in einen neuen Artikel eingefügt. Ursprung dieser Innovation ist die Tatsache, dass Govware nur von absoluten Spezialisten, um nicht zu sagen Hackern, entwickelt werden kann, deren Wissen kaum kontrollierbar ist, und eine wirksame Aufsicht deshalb im grössten Ausmass erschwert oder gar aussichtslos wäre. Um sich dieser Ausgangslage nicht widerstandslos auszusetzen, hat die Kommission zunächst eine vorgängige Zertifizierung von Govware ins Auge gefasst, diese Variante aber wieder fallenlassen müssen, weil die Software laufend, zum Teil in Wochenabständen, an die neueste Entwicklung angepasst wird, sodass bei jedem Update eine neue Zertifizierung nötig wäre. Das würde natürlich eine Unmöglichkeit in der praktischen Anwendung bedeuten.
Die neue Lösung besteht nun darin, dass den Strafverfolgern im Gesetz verbindliche Auflagen gemacht werden. So dürfen sie nur besondere Informatikprogramme einsetzen, welche die Überwachung lückenlos und unveränderbar protokollieren. Die Ausleitung aus dem überwachten System bis zur zuständigen Strafverfolgungsbehörde muss gesichert erfolgen. Und schliesslich ist sicherzustellen, dass der Quellcode überprüft werden kann zwecks Prüfung, dass das Programm nur über die zulässigen Funktionen verfügt. Die am Strafverfahren beteiligten Personen können im Rahmen ihrer Verfahrensrechte jederzeit auf die Einhaltung dieser Auflagen pochen. Der neue Artikel 269quater ist in diesem Sinne auch eine wichtige vertrauensbildende Massnahme.
Die FDP-Liberale Fraktion begrüsst diesen neuen Artikel und wird bei den Absätzen 4 und 5 grossmehrheitlich die Mehrheit unterstützen, nachdem nun Frau Rickli den zurückgezogenen Minderheitsantrag Lüscher übernommen hat, denn die Idee, dass solche hochspezialisierten Informatikprogramme zentral und nicht im föderalistischen Wildwuchs beschafft werden, ist nicht zu schnell von der Hand zu weisen. Dem war auch der von der Kommission konsultierte Vorstand der KKJPD nicht ganz abgeneigt. Es lohnt sich, hier eine Differenz zum Ständerat zu schaffen, der somit aufgefordert ist, die sich hier stellenden Fragen noch zu vertiefen. Dazu gehören insbesondere Abklärungen zur Beschaffungsbehörde an sich und zum Beschaffungsrecht des Bundes, welches im Vergleich zu demjenigen in den Kantonen unterschiedlich ausgestaltet ist.

Guhl Bernhard (BD, AG): Bei der Govware und den sogenannten Imsi-Catchern nimmt die BDP-Fraktion wiederum die Haltung ein, dass wir den Strafverfolgungsbehörden die gleichen technischen Mittel geben müssen, wie sie die Kriminellen auch haben. Würden wir da der Minderheit zustimmen, würden wir den Strafverfolgungsbehörden Steine in den Weg legen. Dazu wird die BDP-Fraktion aber nicht Hand bieten, denn auch hier gilt es wiederum zu sagen, dass es um den Einsatz von Geräten und Software geht, die richterlich bewilligt werden mussten. Wir sprechen auch von relativ wenigen Fällen im Kontext der gesamten Kommunikation innerhalb des Landes. Es muss auch so sein, dass zuvor andere Möglichkeiten ausgeschöpft wurden und diese nicht dazu geführt haben, die Kriminellen dingfest zu machen. Zudem muss es sich eben um Fälle von sehr schwerer Kriminalität handeln.
Die BDP-Fraktion steht auf der Seite der Strafverfolgungsbehörden und wird darum bei Artikel 269bis und bei Artikel 269ter Absatz 1 mit der Mehrheit stimmen.
Noch kurz zu Artikel 269ter Absatz 6, wonach nur in der Schweiz entwickelte Programme zum Einsatz kommen sollen: Das ist nicht Swissness, Frau Kiener Nellen, das ist Protektionismus, und zwar fataler Protektionismus! Bei diesen Programmen müssen wir Anbieter mit Erfahrung in diesem Bereich und gute Software haben. Da dürfen wir uns nicht einschränken, indem wir nur Schweizer Software einsetzen.
Bei Artikel 269quater Absätze 4 und 5 bitten wir Sie, den Antrag der Minderheit Lüscher abzulehnen. In der Kommission wurde dieses Thema sehr lange diskutiert, wir haben da auch die Meinung von Dritten eingeholt; Frau Huber, meine Vorrednerin, hat es erwähnt. Die KKJPD steht auch hinter dieser Lösung. Ich bitte Sie, hier mit der Mehrheit zu stimmen.
So viel von unserer Seite zu Block 2.

Chevalley Isabelle (GL, VD): Ce bloc concerne les outils que nous allons permettre à nos autorités d'utiliser ou pas. Certes, certains d'entre eux peuvent être dangereux s'ils sont utilisés à mauvais escient. Ceci dit, seul un tribunal pourra ordonner l'utilisation d'un Govware – nécessaire pour suivre des conversations sur Skype ou Whatsapp – ou d'un IMSI-Catcher. Il faut donc déjà des soupçons graves et étayés pour pouvoir mettre une personne sous surveillance.
Le principe de proportionnalité sera appliqué, car un Govware ne pourra être utilisé que si les autres moyens de surveillance moins invasifs ont échoué. D'autre part, seuls les crimes qui figurent dans la liste à l'article 269 du Code de procédure pénale pourront faire l'objet d'une telle surveillance. On ne pourra pas intervenir dans la sphère privée d'un citoyen pour un simple vol à l'étalage ou pour un vol de chatons. Rappelons encore que c'est un tribunal qui autorisera l'utilisation d'un tel outil et que seules les données utiles à l'enquête pourront être conservées. En plus de ces limitations, la commission a prévu l'établissement d'un procès-verbal mis en place lors de l'utilisation d'un Govware. Ceci permettra de s'assurer qu'il n'y a pas d'abus. Les droits fondamentaux ne sont donc pas violés.
Ne pas permettre l'utilisation d'outils adaptés à l'évolution de la technique reviendrait à protéger les délinquants et à leur permettre de continuer leur trafic en toute sécurité.
Le monde technologique évolue; nous devons aussi faire évoluer la législation pour pouvoir continuer à appréhender les criminels en tous genres.
La majorité du groupe vert'libéral soutiendra la proposition de la minorité Vogler à l'article 269 alinéa 2 lettre k et la majorité s'agissant des autres articles.

Glättli Balthasar (G, ZH): In diesem Bereich, muss man sagen, hat die Kommission im Vergleich zu anderen Bereichen aus meiner Sicht wirklich auch substanzielle Verbesserungen hingekriegt, soweit es um den Staatstrojaner geht. Das müssen auch wir von den Grünen anerkennen: Man hat wirklich versucht, einige der Problembereiche in der Version des Bundesrates und auch in der Version, wie sie vom Ständerat kam, zu adressieren.
Nichtsdestotrotz ist es natürlich so, dass es aus unserer Sicht weiterhin auch grundlegende Kritikpunkte gibt, die

nicht adressiert werden wollten oder konnten. Das ist einerseits der ganze Deliktskatalog, der, wie wir Grünen weiterhin meinen, hier nochmals deutlich eingeschränkt werden müsste. Das andere ist, dass Staatstrojaner – ich sage es jetzt mal so und nicht in Neusprech «Govware», weil das ja ein Wort ist, das vor allem dazu dient, dass niemand weiss, worum es geht – natürlich in der Informatiklandschaft, die wir heute kennen, Risiken haben, die aus meiner Sicht auch mit diesen Verbesserungen nicht unbedingt adressiert, gelöst werden konnten.
Was meine ich konkret? Sehr viele Angestellte haben heutzutage einen Computer. Diesen brauchen sie sowohl als persönliches Arbeitsinstrument als auch in der Firma, wo sie arbeiten, sei es, dass der Computer oder der Laptop von der Firma zur Verfügung gestellt wird, sei es, dass man nach der Devise «bring your own device» versucht, verschiedene Computer in eine Informatiklandschaft zu integrieren. Die Zeit ist lange her, als ich unter anderem auch als Systemadministrator tätig war. Aber ich kann mir vorstellen, was das dann für zusätzliche Risiken sind, wenn man weiss, man wird nicht nur von Viren aller Sorten angegriffen, sondern eben auch noch möglicherweise von einem Staatstrojaner, der – und das wäre ja dann die Erwartung, die man hat, damit die Strafverfolgung auch funktionieren kann – mindestens so gut sein muss wie der State of the Art in der Technik und bei einem normalen Viren- oder Trojaner-Abwehrprogramm oder bei einem Virenscanner sicher nicht auffliegen sollte.
Es werden dann eben auch Lücken, Hintertüren geschaffen, denn man muss ja eine Hintertür auftun, um überhaupt einen solchen Trojaner zu platzieren, wenn man jetzt mal die Idee verfolgt, die vielleicht noch nicht realisierbar ist, dass das auch von aussen, ohne persönlichen Kontakt, infiziert werden kann. Da macht man natürlich nicht nur bei der betroffenen Einzelperson und bei ihrem Computer eine Hintertür auf, sondern man öffnet eine Hintertür in das Netzwerk, in das dieser Computer eingebunden ist. Damit kann man dann natürlich auch die Informatiksicherheit des ganzen Unternehmens gefährden, wenn dieses das Pech hat – dafür kann es ja nichts –, in seinen Reihen einen vielleicht zu Recht Verdächtigten zu haben.
Das sind Fragen, die aus grüner Sicht offenbleiben. Auch die Haftung ist nicht klar. Wir sind grundsätzlich schon der Meinung, dass man über dieses Mittel diskutieren kann, aber es muss, wenn schon, in sehr, sehr eingeschränktem Masse eingesetzt werden.
Ich äussere mich noch ganz kurz zu den Imsi-Catchern. Ich glaube, die wesentlichen Argumente sind bereits von Herrn Reimann vorgebracht worden. Es müsste wirklich sichergestellt sein, dass nicht plötzlich in Notrufsituationen ein Problem entsteht. Aus meiner Sicht muss natürlich auch in Betracht gezogen werden, dass da im Sinne eines Beifangs sehr viele Personen einfach mit betroffen sind. Betroffen sind dann eben nicht nur die Personen, die man meint, sondern auch alle anderen, die sich per Zufall im Empfangsbereich des gleichen Imsi-Catchers aufhalten.

Vogler Karl (CE, OW): Namens der CVP/EVP-Fraktion ersuche ich Sie, in Block 2 immer der Mehrheit zu folgen und die Minderheitsanträge abzulehnen – das mit Ausnahme der Minderheitsanträge zu Artikel 269quater Absätze 4 und 5, der bisherigen Anträge Lüscher, die nun von Frau Kollegin Rickli übernommen wurden.
Bei der ersten Differenz, Artikel 269bis, bitte ich Sie, den Antrag der Minderheit I abzulehnen, weil bereits der Ständerat beschlossen hat, dass die Staatsanwaltschaft betreffend Überwachung eine Statistik zu führen hat. Die Regelung der Details soll dem Bundesrat vorbehalten bleiben. Ebenfalls abzulehnen sind hier die Anträge der Minderheiten II und III. Die Verwendung von Imsi-Catchern ist nur zulässig, wenn die entsprechenden, strengen Voraussetzungen erfüllt sind. Insbesondere muss auch das Zwangsmassnahmengericht dem entsprechenden Einsatz zustimmen, und das Bakom muss diese Geräte geprüft haben. Auch hier gilt im Sinne der Wahrung des Grundsatzes der Verhältnismässigkeit, dass solche Geräte nur subsidiär zur Anwendung kommen, also nur dann, wenn die bisherigen Massnahmen nicht zum Erfolg geführt haben. In diesem Fall sind solche Geräte eben gerade notwendig.
Analoges gilt, was die Anträge der Minderheiten I, II und III zu Artikel 269ter der Strafprozessordnung betrifft. Es geht hier primär darum, dass diese Minderheiten den Einsatz von sogenannter Govware verbieten wollen. Nach Meinung unserer Fraktion ist das falsch. Der Einsatz von Govware ist für eine effiziente Strafverfolgung, selbstverständlich unter Wahrung der entsprechend vorgesehenen Voraussetzungen, richtig und auch notwendig. Das gilt auch für die von der Minderheit Vischer Daniel in Artikel 269ter Absatz 1 Buchstabe b beantragte Ergänzung, welche ebenfalls zu einer übermässigen Einschränkung in der Strafverfolgung führen würde.
Kurz zum Antrag der Minderheit Kiener Nellen zu Artikel 269ter Absatz 1bis: Auch wenn man auf den ersten Blick Sympathien für diesen Antrag haben mag, so gilt es festzustellen, dass solche Programme nur von ganz wenigen Herstellern angeboten werden. Man würde also damit die Beschaffung weiter erschweren, und letztlich wäre wahrscheinlich gar nicht feststellbar, welche Länder unter diese Bestimmung fallen würden. Wer gibt denn schon zu, grossangelegte Fernüberwachungen zu betreiben? Hinzu kommt, dass in Artikel 269quater die Anforderungen an diese besonderen Informatikprogramme geregelt sind. Der Minderheitsantrag ist entsprechend abzulehnen.
Betreffend den Minderheitsantrag zu Artikel 269ter Absatz 4 gilt analog das bei Artikel 269bis Gesagte. Ich bitte Sie, den Minderheitsantrag abzulehnen, weil bereits der Ständerat beschlossen hat, dass die Staatsanwaltschaft betreffend die Überwachungen eine Statistik zu führen hat.
Was den Minderheitsantrag zu Absatz 5 betrifft, so bitte ich Sie, auch diesen abzulehnen, weil das entsprechende Anliegen technisch nicht umsetzbar ist.
Schliesslich abzulehnen ist auch der Minderheitsantrag zu Absatz 6, weil es gemäss Auskunft der Verwaltung in der Schweiz kein Unternehmen gibt, das solche Programme entwickelt. Die Entwicklung solcher ist enorm aufwendig. Die Annahme dieses Minderheitsantrages würde in der Konsequenz dazu führen, dass in der Schweiz keine Govware eingesetzt werden könnte.
Unsere Fraktion wird auch den Minderheitsantrag Vischer Daniel betreffend Artikel 269quater Absatz 6 ablehnen.
Zusammengefasst: Ich ersuche Sie, bei Block 2 immer dem Antrag der Kommissionsmehrheit zu folgen, ausser bei Artikel 269quater Absätze 4 und 5.

Schwander Pirmin (V, SZ): Ich bitte Sie namens der SVP-Fraktion, bei Artikel 269bis und bei Artikel 269ter der Minderheit Reimann Lukas zu folgen.
Weshalb? Wir haben ja bereits heute im geltenden Recht in Artikel 296 eine Generalklausel – ich möchte das so ausdrücken. Es ist schon erwähnt worden heute Morgen, es sind drei Voraussetzungen fixiert: dringender Verdacht, Schwere der Straftat und die Überwachung des Post- und des Fernmeldeverkehrs durch die Staatsanwaltschaft, wenn keine anderen Mittel zum Erfolg führen. Was wollen wir noch mehr? Das ist eine technologieneutrale Generalklausel. Ich habe schon einmal gesagt, auch beim Nachrichtendienstgesetz: Sie können ein technisches Problem nicht juristisch lösen, und Sie können ein juristisches Problem nicht technisch lösen. Aber genau das tun wir mit diesem Gesetz, wir machen eine Vermischung. Am Ende weiss niemand mehr, wie das läuft.
Dieser Eindruck ist mir auch aus der Kommissionsberatung geblieben. Heute Morgen hat das bis jetzt niemand aufgezeigt, zumindest habe ich es nicht gehört. Es geht um Risikopolitik, es geht darum, das Risiko abzuschätzen. Ich habe bis jetzt von niemandem gehört, womit und wie die Risiken vermieden werden, womit und wie die Risiken vermindert werden, womit und wie die Risiken begrenzt werden. Das wäre Risikopolitik. Und wir leben ja in einer Risikogesell-

schaft. Das konnte bis jetzt aber, zumindest habe ich das nicht gehört, nicht konkret aufgezeigt werden.
Ich habe heute Morgen und teilweise heute Nachmittag auch gehört, man müsse den Zugriff auf verschlüsselte Daten haben. Ja, aber das ist gerade ein Hinweis, wie man über das Gesetz oder über diese Technik denkt. Ich muss nicht den Zugriff auf die verschlüsselten Daten haben. Die Staatsanwaltschaft braucht Daten in unverschlüsselter Form. Solche muss sie haben. Das ist die Frage: Wo setze ich an? Wenn ich verschlüsselte Daten habe, habe ich noch nichts. Bis Sie verschlüsselte Daten entschlüsselt haben, sind die Täter schon längst auf der anderen Seite der Erde. Also müssen wir genau überlegen, wo man diese Software einsetzen soll.
Eine Mehrheit der SVP-Fraktion ist der Meinung, wir würden hier falsch ansetzen.
Es ist bezüglich dieser Staatstrojaner jetzt mehrmals erwähnt worden, was sie machen sollen und was sie nicht machen sollen. Aber ich muss Ihnen sagen: Sie können eine Software nicht so zielgerichtet entwickeln, wie es der Gesetzgeber hier will. Ich wüsste nicht wie. Ich bin aber lernfähig, Sie können mir gerne einmal einen solchen Entwickler schicken, dann werde ich es mit ihm anschauen, und vielleicht lerne ich es noch, zwanzig Jahre, nachdem ich selber programmiert habe. Es ist mir jedoch unvorstellbar, wie das geschehen sollte. Nicht einmal ein Expertensystem kann das, was Sie hier im Gesetz möchten. Ein Staatstrojaner kann nicht so zielgerichtet sein, dass keine Daten verändert werden, dass sich am Zielsystem nichts ändert. Wie wollen Sie das denn machen? Bei einem Staatstrojaner geht es – das wurde auch in der Kommission gesagt – um mindestens 2 Millionen Zeilen Code, ich würde sogar sagen, ein Staatstrojaner habe mindestens 3 Millionen Zeilen Code. Das ist ein Staatstrojaner, der vielleicht noch Sicherheitsschlaufen drin hätte – aber das ist dann wieder eine andere Frage. Ein Staatstrojaner muss auch sehr dynamisch sein, und weil er dynamisch sein und laufend an die veränderten Verhältnisse angepasst werden muss, ist er sehr gefährlich. Wenn ein Trojaner in ein Zielsystem eingeführt wird, ist davon auszugehen, dass er auch Sicherheitslücken hinterlässt. Diese Sicherheitslücken können entsprechend vom Zielsystem oder von Verbrechern ausgenützt werden.
Wenn Sie glauben, wir könnten uns mit solchen Überwachungsmassnahmen dann sicher fühlen – wir beruhigen einfach die Bevölkerung, indem wir sagen, wir hätten etwas gemacht. Aber am Schluss kommt heraus, wie wir es auch schon festgestellt haben, dass die Ziele nicht erreicht werden und dass wir die Risiken, die in unserer Gesellschaft bestehen, mit solchen Massnahmen nicht mindern können.
Ich bitte Sie deshalb, die Minderheiten Reimann Lukas zu unterstützen.

Sommaruga Simonetta, Bundespräsidentin: Es geht in diesem zweiten Block um den Einsatz von sogenannten Imsi-Catchern und den Einsatz von Govware bzw. Staatstrojanern.
Zuerst zu den Imsi-Catchern: Es ist Ihnen bekannt, dass Imsi-Catcher schon heute im Einsatz stehen. Was wir hier wollen, was wir hier mit diesem Gesetz tun, ist, dass wir die gesetzliche Grundlage dafür verbessern wollen. Über Missbräuche und Probleme beim Einsatz dieser Imsi-Catcher habe ich auch in dieser Debatte nichts gehört.
Herr Schwander hat jetzt über die Risiken gesprochen. Ich denke, das ist eine sehr wichtige und sehr interessante Diskussion. Was Sie jetzt aber nicht erwähnt haben, ist das Risiko, dass man Straftäter nicht finden kann. Über dieses Risiko haben Sie nichts gesagt: dass man Ermittlungen nicht machen kann, dass man bei Kriminellen, die sich auch mit verschlüsselter Kommunikation unterhalten, keinen Zugang hat, wenn man nicht mit Govware, mit Staatstrojanern operieren kann. Sie können gerne über diese Risiken sprechen. Ich denke, Sie haben das auch in Ihrer Kommission sehr ausführlich getan. Ich bin froh, dass Sie es getan haben.
Frau Huber und andere haben es erwähnt: Sie haben hier auch noch Klärungen, Verbesserungen eingebracht, die der Bundesrat unterstützt. Wir sind froh darüber und sind dankbar für diese Arbeit, die Sie gemacht haben. Aber wenn Sie über Risiken sprechen, müssen Sie verschiedene Risiken erwähnen, wie ich es vorher in Bezug auf die Grundrechte und die Eingriffe bei den Grundrechten erwähnt habe. Da müssen Sie immer beides erwähnen. Am Schluss ist es ein Abwägen, auch bei diesem Gesetz. Es gibt auch bei diesem Gesetz, wie so oft im Leben und wie so oft bei Entscheidungen, die Sie fällen müssen, nicht einfach Schwarz oder Weiss, sondern man muss abwägen. Ich denke, gerade Ihre Kommission hat beim Einsatz von Govware diese Abwägung noch einmal gemacht; sie hat sie sehr sorgfältig gemacht und zusätzliche Einschränkungen beschlossen.
Noch einmal zurück zu den Imsi-Catchern: Die Minderheit I bei Artikel 269bis der Strafprozessordnung verlangt eine Statistik. Sie möchte auch Vorgaben zur Führung dieser Statistik machen; die Staatsanwaltschaften sollen diese Statistik führen. Das hat der Ständerat bereits eingebracht, und der Bundesrat hat sich damit einverstanden erklärt. Die Frage ist nur, wollen Sie im Gesetz jetzt noch zusätzlich im Detail festhalten, was mit diesen Statistiken erfasst wird, oder überlassen Sie das dem Bundesrat? Nach unserer Meinung und der Meinung der Kommissionsmehrheit soll der Bundesrat die Einzelheiten in Bezug auf diese Statistik regeln. Es geht ja darum, dass wir dem Umstand Rechnung tragen müssen, dass die Zuständigkeit für den Einsatz von Imsi-Catchern dezentral geregelt ist. Das heisst, jede kantonale Staatsanwaltschaft – in gewissen Kantonen gibt es sogar mehr als eine Staatsanwaltschaft – wird eine solche Statistik führen müssen. Je nach Grösse der Kantone ist dies auch unterschiedlich organisiert. Ich denke, wir haben die beste Lösung, wenn der Bundesrat hier die Vorgaben macht, wie diese Statistiken geführt und veröffentlicht werden, damit Sie auch die Informationen, die Sie daraus ziehen möchten, erhalten können.
Ich bitte Sie hier, der Kommissionsmehrheit zu folgen.
Die Minderheit II bei Artikel 269bis möchte Störungen des Fernmeldeverkehrs beim Einsatz von Imsi-Catchern verhindern. Dazu möchte ich Folgendes sagen: Es ist klar, dass es durch den Einsatz von Imsi-Catchern zu keinen Unterbrüchen bei den Gesprächen kommt, und es gibt auch keine Netzunterbrüche dadurch. Das heisst, dass Telefonate und vor allem auch Notrufe dann möglich sind. Aber es stimmt, dass es hier ein gewisses Störungspotenzial gibt. Diesem Anliegen haben wir Rechnung getragen, indem wir für den Einsatz eines Imsi-Catchers eben auch die Genehmigung des Bundesamtes für Kommunikation verlangen, gerade um hier abzuklären, inwiefern der Einsatz eines solchen Imsi-Catchers zu Störungen führen könnte.
Noch zur Minderheit III: Sie möchte die Imsi-Catcher ganz verbieten und damit hinter das geltende Recht zurückgehen. Das wäre für die Abwägung, was die Strafverfolgungsbehörde tun soll und tun muss, um eben auch unseren Rechtsstaat sicherzustellen, ein beträchtlicher Rückschritt.
Wir lehnen alle diese Minderheitsanträge ab.
Ich komme jetzt noch zum Einsatz von Govware. Ich habe es heute Morgen schon gesagt und wiederhole es jetzt, einfach damit es klar ist: Govware wurde auch schon in der Vergangenheit eingesetzt. Sie haben sich darüber unterhalten, ich erinnere mich, es war eine ziemliche Aufregung im Land, und man hat sich darüber gestritten, ob es für den Einsatz von Govware heute überhaupt eine gesetzliche Grundlage gibt. Die Frage ist bis heute umstritten geblieben. Gerade diejenigen, die dem Einsatz von Govware kritisch gegenüberstehen, müssten doch ein Interesse haben, jetzt hier im Gesetz festzulegen, wann und unter welchen Voraussetzungen – ganz streng, ganz klar geregelt – Staatstrojaner eingesetzt werden dürfen und wie es mit der Verwertung der gesammelten Daten aussieht; ich komme nachher noch darauf zurück. Tatsache ist, dass Govware für die Strafverfolgungsbehörden eine unentbehrliche Überwachungsmethode ist. Die verschlüsselte Kommunikation hat in unseren Alltag Einzug gehalten. Wenn Sie heute sagen, dass die Kommunikation mit einem i-Phone über Facetime oder über Skype nicht überwacht werden darf und dass diese Art von

Kommunikation den Strafverfolgungsbehörden nicht zugänglich gemacht werden soll, selbst dann nicht, wenn ein Strafverfahren eröffnet worden ist und ein Zwangsmassnahmengericht diese Massnahme bewilligt hat, dann ist dies eigentlich unvorstellbar.
Ich habe es gesagt, die Strafverfolgung wird für den Einsatz von Govware noch einmal eingeschränkt. Wir können es uns aber nicht leisten, dass die Schweiz eine überwachungsfreie Insel für Verbrecher wird, welche ihre Straftaten über Skype, über Whatsapp oder über verschlüsselte E-Mails vorbereiten oder begehen. Der Entwurf des Bundesrates enthält nicht nur eine explizite Grundlage, welche die Verwendung von Govware erlaubt, sondern auch Bestimmungen, welche besondere Schranken für die Verwendung vorsehen.
Hier würde ich gerne noch etwas zum Verwertungsverbot sagen. Es wurde nämlich erwähnt, dass es in diesem Gesetz gar kein Verwertungsverbot gebe. Lesen Sie Artikel 269ter Absatz 3 der Strafprozessordnung. Dort steht: «Durch Absatz 1 nicht gedeckte Daten» – Absatz 1 sagt eben, wann Govware eingesetzt werden kann –, «die beim Einsatz solcher Informatikprogramme gesammelt werden, sind sofort zu vernichten. Durch solche Daten erlangte Erkenntnisse dürfen nicht verwertet werden.» Das ist das Verwertungsverbot, das steht bereits so im Gesetzentwurf.
Nochmals zu den Voraussetzungen: Sie haben den Deliktskatalog für den Einsatz von Govware beschränkt, stärker als denjenigen für die sogenannt normale Überwachung. Sie haben den Govware-Einsatz auf jene Delikte beschränkt, bei welchen eben auch die verdeckte Ermittlung möglich ist. Verdeckte Ermittlung und Govware-Einsatz sind massive Eingriffe, und deshalb ist es auch richtig, dass man diese Beschränkung vornimmt. Ansonsten gelten die gleichen Vorschriften. Der Einsatz von Govware muss von einer Staatsanwaltschaft angeordnet werden. Das heisst, das Strafverfahren ist eröffnet, das Zwangsmassnahmengericht muss den Einsatz genehmigen, und gegenüber anderen Überwachungen darf diese Massnahme nur als Ultima Ratio angewendet werden. Schliesslich ist auch der Anwendungsbereich eng begrenzt, nämlich auf die Überwachung der Kommunikation. Das heisst, Govware darf für Online-Durchsuchungen von Computern nicht verwendet werden. Eine Annahme der Minderheitsanträge zu Artikel 269ter hätte eine erhebliche Überwachungslücke zur Folge.
Einer der Minderheitsanträge zu Artikel 269ter, der Antrag der Minderheit Vischer Daniel zu Absatz 1 Buchstabe b, bezieht sich auf Artikel 260bis StGB. Wenn man Govware nur für die Verfolgung von Straftaten gemäss Artikel 260bis StGB zulassen würde, also nur für die Verfolgung von Gewaltverbrechen, dann könnte sie für die Verfolgung der organisierten Kriminalität oder der Finanzierung von Terrorismus nicht mehr eingesetzt werden. Es gibt schon gute Gründe, weshalb wir nicht nur Gewaltverbrechen aufklären und dafür die entsprechenden Mittel zur Verfügung stellen wollen. Gerade die Strafverfolgung der Finanzierung von Terrorismus ist eine eminent wichtige Aufgabe eines jeden Staates. Deshalb kann ich schlecht nachvollziehen, weshalb man Govware für die Aufklärung der Finanzierung von Terrorismus oder von organisierter Kriminalität nicht soll einsetzen können.
Die Minderheit Kiener Nellen möchte, dass Govware nur in Ländern beschafft werden kann, welche keine grossangelegte Fernmeldeüberwachung betreiben. Das schränkt die Auswahl beim Kauf solcher Programme natürlich ein. Es ist aus unserer Sicht nicht nötig, weil die Frage der Sicherheit – es gibt bei der Beschaffung solcher Informatiksoftware Sicherheitsbedenken, das ist klar – in Artikel 269quater der Strafprozessordnung geregelt wird; das ist absolut sinnvoll. Wenn Sie die Einschränkung aber so vornehmen, wie das die Minderheit beantragt, haben Sie letztlich nichts gewonnen. Sie müssen vielmehr die Sicherheitsvorschriften beachten, wie sie in Artikel 269quater festgeschrieben sind.
Ich komme noch zu Artikel 269quater Absätze 4 und 5: Das Konzept der KKJPD und der Konferenz der kantonalen Polizeikommandanten sieht vor, dass nicht nur der Bund diese Programme beschaffen soll, sondern die Beschaffung auch in den Kantonen möglich sein soll. Die Kommissionsmehrheit hat nun vorgesehen, dass nur ein Bundesdienst diese Informatiksoftware beschaffen kann. Herr Nationalrat Lüscher hat seinen Minderheitsantrag zurückgezogen, Frau Rickli hat ihn aber aufgenommen. Grundsätzlich unterstützt der Bundesrat diese Minderheit, er wird es auch weiterhin tun. Wir sind aber einverstanden damit, dass diese Frage im Ständerat – das Geschäft geht ja ohnehin dorthin zurück – noch einmal angeschaut wird. Er kann die Frage, was die Vorteile und was die Nachteile sind, vor allem auch mit den Kantonen nochmals diskutieren. Wie wir heute ja gehört haben, haben die Kantone da unterschiedliche Einschätzungen. Von daher ist es richtig, dass Sie bei dieser Frage eine Differenz schaffen. Das ist eigentlich das, was wir bezwecken, damit im Erstrat diese Frage gerade auch mit den Kantonen noch einmal angeschaut werden kann.
Ich bitte Sie, in Block 2 jeweils die Kommissionsmehrheit zu unterstützen.

Schwander Pirmin (V, SZ): Frau Bundespräsidentin, Sie haben heute mehrmals das Beispiel der Finanzierung des Terrorismus genannt. Ist nicht gerade die Finanzierung des Terrorismus, zumindest in der Anfangsphase, ein Paradebeispiel für den Nachrichtendienst?

Sommaruga Simonetta, Bundespräsidentin: Herr Nationalrat Schwander, das kann für den Nachrichtendienst durchaus ein wichtiges Objekt sein. Das haben Sie beim Nachrichtendienst auch so vorgesehen. Ich würde Ihnen gerne eine Frage stellen. Aber ich darf ja keine Fragen stellen. Wenn der Nachrichtendienst aufgrund seiner Ermittlungen auf eine Person stösst, bei der sich der Verdacht bestätigt, dass Terrorismus finanziert wurde, kommt die Strafverfolgung zum Zug. Diese Person muss dann vor Gericht gebracht werden. Sie wissen, dass der Nachrichtendienst nicht Personen vor Gericht bringen kann. Wie argumentieren Sie dann, wenn Sie den Strafverfolgungsbehörden nicht die gleichen Mittel in die Hand geben wie dem Nachrichtendienst? Ich habe Ihnen das Beispiel genannt. Unter Umständen wird der Verdacht bestätigt, dass eine Person Terrorismus finanziert. Nachher können Sie diese Person aber nicht vor Gericht belangen, weil die Strafverfolgungsbehörden nicht die gleichen Mittel haben wie der Nachrichtendienst. Sie brauchen ja Beweismittel. Sie müssen am Schluss die Person wieder laufenlassen, obwohl sich der Verdacht bestätigt hat. Das kann doch nicht in Ihrem Sinne sein. Das war jetzt eine Frage, allerdings eine rhetorische.

Flach Beat (GL, AG), für die Kommission: Die Kommission hat sich bei den Fragen in Block 2 sehr lange aufgehalten, denn hier geht es um die sogenannte Govware oder eben den Staatstrojaner und um den Imsi-Catcher. Der Imsi-Catcher ist ein Gerät, das sich, salopp gesagt, als Natelantenne ausgibt und in einem Bereich, wo es andere Natelantennen hat, quasi die vorhandenen Handys absaugt. Ein Handy wird dann veranlasst, sich bei diesem sogenannten Imsi-Catcher anzumelden. Der Imsi-Catcher gibt ein Signal, worauf das Handy dann seine Imsi-Nummer wieder zurückgibt. Auf diese Art und Weise kann man Handys in einem Radius von rund hundert Metern lokalisieren. Diese Geräte sind bereits heute im Einsatz. Diese Geräte sind auch nicht dazu vorgesehen, Abhörungen oder etwas Ähnliches zu machen. Diese Geräte sind vielmehr vornehmlich dazu da, den Standort von Handys zu ermitteln, die entweder stationär irgendwo sind oder auf Personen sind, die sich bewegen. Wie gesagt, sind diese Geräte bereits heute Bestandteil der Ausrüstung, teilweise auch bei den Kantonspolizeien. Das Bundesamt für Justiz hat diese Geräte ebenfalls. Beim Büpf gibt es so etwas.
Die Minderheiten II und III (Reimann Lukas) wollen den Einsatz von Imsi-Catchern sehr einschränken oder verbieten. Die Minderheit II legt die Voraussetzungen für den Einsatz eines Imsi-Catchers so fest, dass es wahrscheinlich überhaupt nicht mehr möglich ist, ihn tatsächlich im Feld einzusetzen. Die Minderheit III ist immerhin insofern klar, als sie

den Einsatz einfach verbieten will. Ich möchte Sie daran erinnern, dass es diese Geräte bereits gibt, dass man sie halt eben auch zur Personensuche und zur Notsuche einsetzt.
Zur Frage der Störungen des Mobilfunknetzes, wenn ein solcher Imsi-Catcher eingesetzt wird: Wie schon ausgeführt wurde, kann es tatsächlich sein, dass es zu Störungen kommt. Man muss allerdings auch sagen, dass es sich um einen Polizeieinsatz handelt. Wenn die Polizei in Ihrer Strasse eine Verhaftung vornimmt, dann müssen Sie vielleicht auch mit Störungen geringeren oder grösseren Ausmasses rechnen. Sie müssen vielleicht eine andere Strasse entlanggehen, wenn da ein Polizeieinsatz ist. Ich glaube, uns ist allen klar, dass die Polizeibehörden da einen gewissen Freiraum haben müssen. Aber es ist auch klar, und das kommt im Gesetz auch deutlich zum Ausdruck, dass diese Geräte vom Bakom geprüft werden müssen, bevor sie in Betrieb gehen, und dass man darauf achtet, dass die Störungen, sofern es welche gibt, so gering wie irgendwie möglich sind.
Ich möchte noch auf die Frage der Government Software, der Govware, eingehen. Darüber haben wir in der Kommission ebenfalls sehr ausgiebig gesprochen; ich habe es beim Eintreten schon erwähnt. Wir machen ein Gesetz für die Zukunft und betrachten die Vergangenheit und die Gegenwart. Darum ist es relativ schwierig, in diesem Technikbereich, wie Herr Kollege Schwander auch gesagt hat, jetzt schon genau zu sagen, in welche Richtung es denn geht. Das Gesetz soll technikneutral sein. Wir sind in der Kommission aber überzeugt worden, dass der Einsatz von Govware oder eines Staatstrojaners eben doch sinnvoll und notwendig ist; denn es geht nicht darum, wie Kollege Schwander gesagt hat, dass man die Daten entschlüsselt, sondern darum, dass man die Daten, bevor sie von einem Laptop oder von einem anderen Gerät abgeschickt werden, auslesen kann, bevor sie verschlüsselt werden, sei es über die Tastatur, sei es über ein ähnliches System.
Die Kommission hat, genau wegen den allfälligen Gefahren eines solchen Trojaners, noch einmal Kriterien ins Gesetz eingefügt, die sicherstellen sollen, dass diese Software, wenn sie denn nach bestem Wissen und Gewissen eingesetzt wird, hohe Qualitätsstandards erfüllt und dass es keinesfalls dazu kommt, dass sich diese Software, wie es der Name Trojaner eben sagt, verteilen kann. Das ist auch nicht im Interesse der Ermittlungsbehörden. Im Interesse der Ermittlungsbehörden ist selbstverständlich, dafür zu sorgen, dass niemand merkt, dass eine solche Software bei ihm auf dem Computer ist. Ich habe nach der Diskussion in der Kommission auch nicht so wahnsinnig viel Verständnis dafür, wenn man sich Sorgen macht, dass bei einem Straftäter allenfalls der Computer verlangsamt wird. Selbstverständlich wird das Einfügen einer solchen Software in den Computer einer Person, die einer schweren Straftat verdächtigt wird, eine Auswirkung haben. Die beste Auswirkung ist, wenn die Staatsanwaltschaft in den Besitz der Kommunikation kommt, die sie braucht.
Beim Antrag der Minderheit Vischer Daniel zu Artikel 269ter handelt es sich darum, dass der Einsatz des Imsi-Catchers und von Govware noch einmal einer restriktiveren Liste von Straftaten unterliegen soll. Es soll so sein, dass diese Software oder der Imsi-Catcher nur noch bei schweren Straftaten – vorsätzliche Tötung, Mord, Geiselnahme, Brandstiftung usw. – zum Einsatz kommen. Die Frau Bundespräsidentin hat bereits ausgeführt, dass das wahrscheinlich einfach viel zu weit gehe und dass sehr viele Einsatzbereiche von Govware so einfach ausgeblendet seien. Ich erwähne nur Betrügereien, Erpressung und ähnliche Dinge, vom Drogenhandel muss ich schon gar nicht sprechen, das ist ganz klar. Keines dieser Delikte ist unter Artikel 260bis StGB aufgelistet.
Zur Frage, woher die Software kommt, wer die Software herstellt: Gemäss dem Antrag Kiener Nellen, den die Kommission dann letztlich abgelehnt hat, soll die Beschaffung solcher Software nur aus Ländern, die keine grossangelegte Fernmeldeüberwachung betreiben, erfolgen können. Diesen Antrag haben wir ausführlich diskutiert, jedoch dann mit 10 zu 6 Stimmen bei 7 Enthaltungen abgelehnt. Sie sehen: Die Kommission hat es sich da nicht leicht gemacht.
Ich bitte Sie, überall den Anträgen der Mehrheit zu folgen.

Schwander Pirmin (V, SZ): Herr Kollege, Sie haben gesagt, Sie hätten keine Mühe, wenn die Daten auf dem Computer eines Straftäters verändert würden. Nun, was sagen Sie dann, wenn der Verdächtige nicht der Täter ist?

Flach Beat (GL, AG), für die Kommission: Danke für diese Frage, Herr Kollege Schwander. Selbstverständlich ist es so, dass man niemals ganz ausschliessen kann, dass eine Ermittlung durch die Polizei bzw. durch die Staatsanwaltschaft irgendeinen Schaden verursacht. Es kommt ab und zu einmal vor, dass eine falsche Person verhaftet wird, beispielsweise wegen einer Verwechslung. Es ist auch schon vorgekommen, dass die Polizei bei einer Hausdurchsuchung die falsche Tür eingetreten hat. Dann muss selbstverständlich der Staat dafür aufkommen, wenn er bei einem unbescholtenen Bürger einen Schaden verursacht hat. Aber aufgrund dessen, dass es ein Risiko im Promillebereich gibt, sich in der Tür zu irren, was niemals der Fall sein sollte, wird man wahrscheinlich den Einsatz nicht absagen, sondern dann halt die Tür eintreten und allenfalls nachher den Schaden bezahlen.

Schwaab Jean Christophe (S, VD), pour la commission: Je m'exprimerai exclusivement sur les programmes informatiques dits spéciaux ou Govware ou encore chevaux de Troie. Il s'agit de créer une base légale claire, précise et qui tienne compte des droits fondamentaux pour brider l'emploi de ces logiciels qui sont tout sauf anodins. Il faut bien avouer qu'ils sont déjà utilisés aujourd'hui par certaines polices cantonales et que la base légale fait clairement défaut.
D'ailleurs, si nous en restions à la clause très générale de l'article 269 du Code de procédure pénale, comme cela a été souhaité par Monsieur Schwander, nul doute que nous risquerions de faire face à un emploi incontrôlé de chevaux de Troie. Ce n'est certainement pas ce que souhaite la majorité de la commission, et ce n'est d'ailleurs certainement pas ce que souhaite ce conseil. Je ne vais pas revenir sur les avantages de ces logiciels et sur la nécessité d'en faire usage au cours d'une enquête pénale, car cela a déjà été exposé en long et en large. Je vais plutôt m'étendre sur leurs inconvénients et leurs dangers potentiels ainsi que sur la façon par laquelle la commission propose d'y remédier.
Un cheval de Troie peut être utilisé pour bien autre chose qu'une simple écoute d'une télécommunication sur Internet. C'est un type de programme qui existe en milliers de versions malveillantes. Ce programme peut modifier le contenu du disque dur dans lequel il s'est introduit, par exemple pour créer de fausses preuves, endommager la machine, ou pour mener une véritable perquisition en ligne. Il peut aussi être utilisé pour allumer micros et caméras et surveiller non pas une télécommunication, mais tout ce qui se passe dans la pièce où se trouve l'appareil. Il faut donc être très prudent, car le risque d'abus est énorme.
La commission, sans fausse modestie, a trouvé la parade. Elle s'est appuyée sur le très bon projet du Conseil fédéral, mais elle l'a amélioré et a renforcé les garanties en matière de droits fondamentaux. Tout d'abord, je vous propose un rappel des règles proposées par le Conseil fédéral. L'emploi d'un cheval de Troie, il faut l'admettre, est une atteinte grave aux droits fondamentaux. Il faut donc que cette atteinte se fonde sur les règles strictes en vigueur. En particulier, l'usage doit respecter le principe de proportionnalité. Le programme ne peut être utilisé que si les autres mesures de surveillance moins invasives ont échoué. L'usage concret doit aussi être proportionné au résultat. Le crime que l'on souhaite élucider doit être important et se trouver sur la liste prévue à l'article 269 du Code de procédure pénale. Le tribunal des mesures de contrainte doit donner son accord. Et les données collectées qui ne seraient pas les données visées dans l'ordre de surveillance doivent être détruites. Les règles en vigueur concernant l'exploitation des preuves

restent en vigueur, cela a été rappelé. Il n'est donc en principe pas possible d'utiliser ce qu'on aurait découvert fortuitement en essayant d'écouter une communication. Comme vous pouvez le constater, la bride des chevaux de Troie est déjà serrée!
Mais ces garanties solides n'ont pas suffi à la commission, qui a souhaité non seulement une bride, mais aussi un mors et des oeillères. Elle a élaboré avec le soutien de l'administration un article 269 quater du Code de procédure pénale, qui pose les conditions supplémentaires suivantes:
– Les programmes ne peuvent être utilisés que s'ils prévoient un procès-verbal complet et inaltérable de la surveillance effectuée. Ainsi, l'on peut vérifier que le Govware ne sert qu'à surveiller les communications et pas à autre chose.
– Le transfert des données à l'autorité de poursuite pénale doit être sécurisé.
– L'autorité doit avoir accès au code source pour vérifier que le programme ne contient que les fonctions autorisées par la loi. Les programmes informatiques spéciaux doivent donc respecter le principe de la légalité dès la conception ou «legal by design», comme diront les anglophones.
Ces principes n'ont pas été contestés lors des débats en commission.
Il faut rappeler que les règles sur l'inexploitabilité des preuves obtenues frauduleusement restent en vigueur, en particulier l'article 141 du Code de procédure pénale. De l'avis de la majorité de la commission, ces règles en vigueur rendent caduque la proposition défendue par la minorité Vischer Daniel à l'article 269quater alinéa 6, que la commission a rejetée par 12 voix contre 5 et 4 abstentions.
Afin de garantir une mise en oeuvre parfaite dans tout le pays, la proposition de la majorité prévoit en outre de confier l'achat et le développement des programmes à un service centralisé de la Confédération, ce qui renforce encore le contrôle légal et permet d'harmoniser les pratiques. Une proposition de minorité, déposée par Monsieur Lüscher et reprise par Madame Rickli, s'y oppose toutefois. La commission l'a rejetée par 12 voix contre 12 et 1 abstention avec la voix prépondérante du président. Mais nous pensons à toutes fins utiles qu'il serait nécessaire de créer une divergence afin – cela a été dit – que le premier conseil, lors de l'élimination des divergences, se penche un petit plus dans le détail sur cet élément particulier. Je rejoins sur ce point ce qu'a dit notamment Monsieur Lüscher: il est possible que la commission n'ait peut-être pas considéré tous les aspects pertinents en la matière.
La commission s'est penchée sur la possibilité de certifier les chevaux de Troie, mais elle y a finalement renoncé, car une certification devrait être refaite lors de chaque mise à jour du programme, ce qui entraînerait des coûts démesurés.
La proposition de la minorité Leutenegger Oberholzer à l'article 269ter alinéa 5 vise à ce que l'intégrité de la machine infectée ne soit pas touchée et que l'accès par des tiers puisse être exclu. Certes, il n'est pas possible de garantir l'intégrité d'une machine suite à l'emploi d'un cheval de Troie, mais le but de ce programme n'est pas de désactiver des mécanismes de sécurité ou d'ouvrir des portes dérobées. Ce n'est pas utile pour l'usage que l'on compte faire du Govware. Par ailleurs, l'obligation de tenir un procès-verbal complet de l'usage du logiciel permet de vérifier que cela n'a pas été le cas et qu'aucun dégât collatéral déraisonnable n'a été commis.
La commission a rejeté la proposition défendue par la minorité Leutenegger Oberholzer, par 12 voix contre 9 et 2 abstentions.
La commission a aussi rejeté, par 16 voix contre 6 et 4 abstentions, la proposition défendue par la minorité Leutenegger Oberholzer, à l'article 269ter alinéa 6, dont le but est de faire en sorte que ces programmes informatiques spéciaux ne soient conçus qu'en Suisse. Il s'agit d'une condition tout simplement impossible à remplir étant donné qu'il n'existe en Suisse aucune entreprise capable de fournir ces programmes.
La commission vous invite aussi, par 10 voix contre 6 et 7 abstentions, à rejeter la proposition défendue par la minorité Kiener-Nellen à l'article 269ter alinéa 1bis. En effet, restreindre l'achat des Govware à un certain type de pays difficile à définir serait ardu à mettre en pratique et créerait probablement passablement d'insécurité juridique.
A l'article 269ter alinéa 4, la commission s'est aussi ralliée à la solution du Conseil des Etats en matière de statistique et a rejeté, par 13 voix contre 6 et 4 absentions, la proposition défendue par la minorité Leutenegger Oberholzer qui souhaitait aller plus loin.
A l'article 269ter alinéa 1 lettre b, la commission a rejeté, par 15 voix contre 5 et 5 abstentions, une proposition défendue par la minorité Vischer Daniel, laquelle visait à restreindre le catalogue d'infractions autorisant l'usage d'un cheval de Troie aux infractions prévues à l'article 260bis alinéa 1 du Code pénal. La commission part de l'idée que cette liste serait beaucoup trop étroite et entraverait de manière significative le travail des autorités de poursuite pénale. En particulier, bon nombre des délits liés au trafic de drogue, à la cybercriminalité ou de nature financière ne seraient plus dans la liste autorisant l'usage des chevaux de Troie. Or c'est un domaine où l'emploi de Govware est nécessaire, car les trafiquants se savent écoutés et passent donc par des canaux que l'on ne peut actuellement pas surveiller avec les méthodes habituelles.
Forte de ces constats, la majorité de la commission est convaincue que l'utilisation des chevaux de Troie, si invasive soit-elle, est tout à fait possible en respectant les droits fondamentaux. La plupart des critiques publiques que l'on peut entendre à leur sujet sont, de l'avis de la majorité de la commission, balayées à la lecture de l'article 269quater proposé, à part bien entendu l'objection de principe, sur laquelle je vais encore brièvement revenir. Mais la commission soutient le Conseil fédéral et le Conseil des Etats sur le principe: l'évolution technologique et les habitudes de télécommunication rendent l'usage de ces programmes nécessaire pour combattre efficacement la criminalité.
Comme il est possible de le faire en garantissant un haut niveau de protection des droits fondamentaux, la commission vous propose de rejeter, à l'article 269ter, les propositions défendues par les minorités I (Leutenegger Oberholzer), II (Vischer Daniel) et III (Reimann Lukas), qui visent à biffer la possibilité d'utiliser des programmes informatiques spéciaux. La commission a rejeté ces propositions par 15 voix contre 7 pour la première, et 14 voix contre 7 pour les deux suivantes, chaque fois sans abstention.

Kiener Nellen Margret (S, BE): Monsieur Schwaab, si je vous ai bien entendu, vous avez dit, à propos de ma proposition de minorité, que de restreindre les pays offrants à ceux qui ne sont pas ou peu impliqués dans des conflits armés créerait une insécurité juridique. Pensez-vous vraiment que le fait de vouloir exclure expressément de la production ou de l'offre de matériel des pays comme les Etats-Unis ou Israël créerait pour la Suisse une insécurité juridique?

Schwaab Jean Christophe (S, VD), pour la commission: Madame Kiener Nellen, je connais particulièrement bien cette proposition, étant donné que j'en suis l'auteur originel. Il est clair que si on lit la proposition, on constate qu'elle introduit un terme juridique indéfini. De l'avis de la majorité de la commission, que j'ai l'honneur de représenter à cet instant, cela créerait de l'insécurité juridique étant donné qu'un terme juridique indéfini doit être défini à un moment donné ou à un autre par la jurisprudence.

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

Ziff. II Ziff. 1 Art. 269bis
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit I
(Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 2
Die Staatsanwaltschaft führt eine öffentlich zugängliche Statistik über die Überwachungen, die über den Einsatz und die gerichtliche Verwertung Auskunft gibt.

Antrag der Minderheit II
(Reimann Lukas, Büchel Roland, Fehr Hans, Schwander, Stamm, Vischer Daniel)
Die Durchführung der Überwachung des Fernmeldeverkehrs stellt sicher, dass durch die Überwachungsmassnahmen oder als Folge davon:
a. der Fernmeldeverkehr der zu überwachenden Person sowie anderer Benutzer nicht beeinträchtigt wird;
b. nicht in Fernmelde- und Datenverarbeitungsanlagen in der Verfügung der zu überwachenden Person sowie anderer Benutzer eingegriffen wird, insbesondere keine Daten, Programme, Zustände und Verbindungen verändert werden;
c. in die fernmeldetechnischen Übertragungen nicht durch Hinzufügen, Verändern oder Entfernen von Information oder durch Verzögerung, Neuordnung, Wiederholung oder Umleitung von Teilen der Übertragung eingegriffen wird;
d. die fernmeldetechnischen Übertragungen nicht zwischen anderen als den durch die Benutzer intendierten oder erwarteten Geräten, Benutzern und Diensten zustande kommen.

Antrag der Minderheit III
(Reimann Lukas, Schwander)
Streichen

Ch. II ch. 1 art. 269bis
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité I
(Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 2
Le ministère public tient une statistique de ces surveillances; accessible au public, cette statistique renseigne sur l'utilisation des dispositifs et l'exploitation des résultats faite par les tribunaux.

Proposition de la minorité II
(Reimann Lukas, Büchel Roland, Fehr Hans, Schwander, Stamm, Vischer Daniel)
L'exécution de la surveillance de la correspondance par télécommunication garantit que les mesures de surveillance ou leurs effets:
a. n'entravent pas la correspondance par télécommunication de la personne devant faire l'objet d'une surveillance et d'autres utilisateurs;
b. ne portent pas atteinte aux installations de télécommunication et de traitement des données dont disposent la personne devant faire l'objet d'une surveillance et les autres utilisateurs, et notamment ne modifient aucune donnée, aucun programme, aucun état ni aucune connexion;
c. ne portent pas atteinte à la transmission de données au moyen de techniques de télécommunication par l'ajout, la modification ou la suppression d'informations ou par l'ajournement, la réorganisation, la répétition ou la déviation de parties de la transmission;
d. ne permettent pas à la transmission de données au moyen de techniques de télécommunication, d'avoir lieu entre d'autres appareils, utilisateurs ou services que ceux qui sont visés ou prévus par l'utilisateur.

Proposition de la minorité III
(Reimann Lukas, Schwander)
Biffer

Erste Abstimmung – Premier vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 107)
Für den Antrag der Mehrheit ... 121 Stimmen
Für den Antrag der Minderheit I ... 60 Stimmen
(0 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 108)
Für den Antrag der Mehrheit ... 119 Stimmen
Für den Antrag der Minderheit II ... 53 Stimmen
(9 Enthaltungen)

Dritte Abstimmung – Troisième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 109)
Für den Antrag der Mehrheit ... 115 Stimmen
Für den Antrag der Minderheit III ... 31 Stimmen
(35 Enthaltungen)

Ziff. II Ziff. 1 Art. 269ter
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit I
(Leutenegger Oberholzer, Kiener Nellen, Nidegger, Reimann Lukas, Schwander, Stamm, Vischer Daniel)
Der Einsatz von besonderen Informatikprogrammen zum Zweck der Einschleusung in ein Datenverarbeitungssystem zur Überwachung des Fernmeldeverkehrs ist untersagt.

Antrag der Minderheit II
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Reimann Lukas, Schwander, Stamm)
Streichen

Antrag der Minderheit III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Streichen

Antrag der Minderheit
(Vischer Daniel, Leutenegger Oberholzer, Reimann Lukas, Schwander)
Abs. 1
...
b. es sich um die Verfolgung einer in Artikel 260bis Absatz 1 StGB aufgelisteten Straftat handelt;
...

Antrag der Minderheit
(Kiener Nellen, Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 1bis
Diese besonderen Informatikprogramme dürfen weder bei einer Behörde eines Landes beschafft werden, dessen Nachrichtendienste eine grossangelegte Fernmeldeüberwachung betreiben, noch bei einem Unternehmen mit Sitz in einem solchen Land.

Antrag der Minderheit
(Leutenegger Oberholzer, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 4
Die Staatsanwaltschaft führt eine öffentlich zugängliche Statistik über diese Überwachungen, die über den Einsatz und die gerichtliche Verwertung Auskunft gibt.

Antrag der Minderheit
(Leutenegger Oberholzer, Flach, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel, von Graffenried)
Abs. 5
Es dürfen nur Programme zur Anwendung gelangen, bei denen gewährleistet ist, dass die Systemintegrität des betroffenen Rechners sowie der beteiligten Netzwerke nicht geschwächt oder gefährdet wird. Es muss insbesondere

ausgeschlossen werden können, dass Dritte aufgrund der Massnahmen ebenfalls in den Rechner eindringen können.

Antrag der Minderheit
(Leutenegger Oberholzer, Kiener Nellen, Schwaab, Vischer Daniel)
Abs. 6
Es dürfen nur in der Schweiz entwickelte Programme zum Einsatz gelangen.

Ch. II ch. 1 art. 269ter
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité I
(Leutenegger Oberholzer, Kiener Nellen, Nidegger, Reimann Lukas, Schwander, Stamm, Vischer Daniel)
L'utilisation de programmes informatiques spéciaux dans le but de s'introduire dans un système informatique pour surveiller la correspondance par télécommunication est interdite.

Proposition de la minorité II
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Reimann Lukas, Schwander, Stamm)
Biffer

Proposition de la minorité III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Biffer

Proposition de la minorité
(Vischer Daniel, Leutenegger Oberholzer, Reimann Lukas, Schwander)
Al. 1
...
b. il s'agit de poursuivre l'une des infractions énumérées à l'article 260bis alinéa 1 CP;
...

Proposition de la minorité
(Kiener Nellen, Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 1bis
Ces programmes informatiques spéciaux ne peuvent être obtenus auprès d'une autorité d'un pays dont les services de renseignement pratiquent une surveillance des télécommunications à grande échelle ou d'une entreprise dont le siège se trouve dans un tel pays.

Proposition de la minorité
(Leutenegger Oberholzer, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 4
Le ministère public tient une statistique de ces surveillances; accessible au public, cette statistique renseigne sur l'utilisation des programmes et l'exploitation des résultats faite par les tribunaux.

Proposition de la minorité
(Leutenegger Oberholzer, Flach, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel, von Graffenried)
Al. 5
Seuls peuvent être utilisés des programmes qui ne risquent pas d'affaiblir ou de mettre en péril l'intégrité de la machine et des réseaux concernés. Il faut notamment pouvoir exclure tout accès à la machine par des tiers.

Proposition de la minorité
(Leutenegger Oberholzer, Kiener Nellen, Schwaab, Vischer Daniel)
Al. 6
Seuls peuvent être utilisés les programmes développés en Suisse.

Abs. 1 – Al. 1

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 110)
Für den Antrag der Mehrheit ... 109 Stimmen
Für den Antrag der Minderheit ... 71 Stimmen
(1 Enthaltung)

Abs. 1bis – Al. 1bis

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 111)
Für den Antrag der Minderheit ... 54 Stimmen
Dagegen ... 125 Stimmen
(2 Enthaltungen)

Abs. 4 – Al. 4

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 112)
Für den Antrag der Mehrheit ... 127 Stimmen
Für den Antrag der Minderheit ... 52 Stimmen
(2 Enthaltungen)

Abs. 5 – Al. 5

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 113)
Für den Antrag der Minderheit ... 78 Stimmen
Dagegen ... 103 Stimmen
(0 Enthaltungen)

Abs. 6 – Al. 6

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 114)
Für den Antrag der Minderheit ... 41 Stimmen
Dagegen ... 131 Stimmen
(9 Enthaltungen)

Abs. 1–3 – Al. 1–3

Erste Abstimmung – Premier vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 115)
Für den Antrag der Mehrheit ... 113 Stimmen
Für den Antrag der Minderheit I ... 64 Stimmen
(4 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 116)
Für den Antrag der Mehrheit ... 114 Stimmen
Für den Antrag der Minderheit II ... 66 Stimmen
(1 Enthaltung)

Dritte Abstimmung – Troisième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 117)
Für den Antrag der Mehrheit ... 109 Stimmen
Für den Antrag der Minderheit III ... 62 Stimmen
(10 Enthaltungen)

Ziff. II Ziff. 1 Art. 269quater
Antrag der Mehrheit
Titel
Anforderungen an die besonderen Informatikprogramme zur Überwachung des Fernmeldeverkehrs
Abs. 1
Es dürfen nur besondere Informatikprogramme eingesetzt werden, welche die Überwachung lückenlos und unveränderbar protokollieren. Das Protokoll gehört zu den Verfahrensakten.
Abs. 2
Die Ausleitung aus dem überwachten Datenverarbeitungssystem bis zur zuständigen Strafverfolgungsbehörde erfolgt gesichert.

Abs. 3
Die Strafverfolgungsbehörde stellt sicher, dass der Quellcode überprüft werden kann zwecks Prüfung, dass das Programm nur über gesetzlich zulässige Funktionen verfügt.
Abs. 4
Der Bund führt einen Dienst, welcher die besonderen Informatikprogramme beschafft. Der Dienst hat die Aufgabe, die Informatikprogramme zur Überwachung des Fernmeldeverkehrs zu entwickeln oder sie bei Dritten einzukaufen.
Abs. 5
Die Staatsanwaltschaft setzt ausschliesslich die vom Bund freigegebenen Informatikprogramme ein und entrichtet eine angemessene Gebühr für die Kosten der Beschaffung und Prüfung der besonderen Informatikprogramme.

Antrag der Minderheit
(Lüscher, Amherd, Barazzone, Chevalley, Eichenberger, Flach, Jositsch, Markwalder, Merlini, Rickli Natalie, Vogler)
Abs. 4, 5
Streichen

Antrag der Minderheit
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, von Graffenried)
Abs. 6
Daten, die unter Missachtung der Bestimmungen der Absätze 1 bis 5 beschafft wurden, dürfen nicht verwertet werden.

Ch. II ch. 1 art. 269quater
Proposition de la majorité
Titre
Exigences posées aux programmes informatiques spéciaux de surveillance de la correspondance par télécommunication
Al. 1
Seuls peuvent être utilisés des programmes informatiques spéciaux qui génèrent un procès-verbal complet et inaltérable de la surveillance. Le procès-verbal est joint au dossier de la procédure.
Al. 2
Le transfert des données du système informatique surveillé à l'autorité de poursuite pénale compétente est sécurisé.
Al. 3
L'autorité de poursuite pénale s'assure que le code source peut être contrôlé, dans le but de vérifier que le programme ne contient que des fonctions admises par la loi.
Al. 4
La Confédération gère un service chargé de la mise à disposition des programmes informatiques spéciaux. Ce service a pour tâche de développer les programmes informatiques spéciaux de surveillance de la correspondance par télécommunication ou de les acheter auprès de tiers.
Al. 5
Le ministère public utilise exclusivement des programmes informatiques validés par la Confédération; il s'acquitte d'un émolument approprié pour les frais de mise à disposition et de contrôle des programmes en question.

Proposition de la minorité
(Lüscher, Amherd, Barazzone, Chevalley, Eichenberger, Flach, Jositsch, Markwalder, Merlini, Rickli Natalie, Vogler)
Al. 4, 5
Biffer

Proposition de la minorité
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, von Graffenried)
Al. 6
Les données obtenues en violation des dispositions des alinéas 1 à 5 ne peuvent être exploitées.

Abs. 4, 5 – Al. 4, 5

Le président (Rossini Stéphane, président): La proposition de la minorité Lüscher a été reprise par Madame Natalie Rickli.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 118)
Für den Antrag der Mehrheit ... 132 Stimmen
Für den Antrag der Minderheit ... 44 Stimmen
(5 Enthaltungen)

Abs. 6 – Al. 6

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 119)
Für den Antrag der Minderheit ... 65 Stimmen
Dagegen ... 113 Stimmen
(4 Enthaltungen)

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Ziff. II Ziff. 1 Art. 274 Abs. 4
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Bst. b
Streichen

Ch. II ch. 1 art. 274 al. 4
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Let. b
Biffer

Le président (Rossini Stéphane, président): La proposition de la minorité Reimann Lukas a déjà été rejetée.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. II Ziff. 2 Art. 70bis
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit I
(Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 2
Der Untersuchungsrichter führt eine öffentlich zugängliche Statistik über diese Überwachungen, die über den Einsatz und die gerichtliche Verwertung Auskunft gibt.

Antrag der Minderheit II
(Reimann Lukas, Büchel Roland, Fehr Hans, Schwander, Stamm, Vischer Daniel)
Die Durchführung der Überwachung des Fernmeldeverkehrs stellt sicher, dass durch die Überwachungsmassnahmen oder als Folge davon:
a. der Fernmeldeverkehr der zu überwachenden Person sowie anderer Benutzer nicht beeinträchtigt wird;
b. nicht in Fernmelde- und Datenverarbeitungsanlagen in der Verfügung der zu überwachenden Person sowie anderer Benutzer eingegriffen wird, insbesondere keine Daten, Programme, Zustände und Verbindungen verändert werden;
c. in die fernmeldetechnischen Übertragungen nicht durch Hinzufügen, Verändern oder Entfernen von Information oder

durch Verzögerung, Neuordnung, Wiederholung oder Umleitung von Teilen der Übertragung eingegriffen wird;
d. die fernmeldetechnischen Übertragungen nicht zwischen anderen als den durch die Benutzer intendierten oder erwarteten Geräten, Benutzern und Diensten zustande kommen.

Antrag der Minderheit III
(Reimann Lukas, Schwander)
Streichen

Ch. II ch. 2 art. 70bis
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité I
(Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 2
Le juge d'instruction tient une statistique de ces surveillances; accessible au public, cette statistique renseigne sur l'utilisation des dispositifs et l'exploitation des résultats faite par les tribunaux.

Proposition de la minorité II
(Reimann Lukas, Büchel Roland, Fehr Hans, Schwander, Stamm, Vischer Daniel)
L'exécution de la surveillance de la correspondance par télécommunication garantit que les mesures de surveillance ou leurs effets:
a. n'entravent pas la correspondance par télécommunication de la personne devant faire l'objet d'une surveillance et d'autres utilisateurs;
b. ne portent pas atteinte aux installations de télécommunication et de traitement des données dont disposent la personne devant faire l'objet d'une surveillance et les autres utilisateurs, et notamment ne modifient aucune donnée, aucun programme, aucun état ni aucune connexion;
c. ne portent pas atteinte à la transmission de données au moyen de techniques de télécommunication par l'ajout, la modification ou la suppression d'informations ou par l'ajournement, la réorganisation, la répétition ou la déviation de parties de la transmission;
d. ne permettent pas à la transmission de données au moyen de techniques de télécommunication d'avoir lieu entre d'autres appareils, utilisateurs ou services que ceux qui sont visés ou prévus par l'utilisateur.

Proposition de la minorité III
(Reimann Lukas, Schwander)
Biffer

Le président (Rossini Stéphane, président): Les propositions des minorités I (Leutenegger Oberholzer), II (Reimann Lukas) et III (Reimann Lukas) ont déjà été rejetées au chiffre II chiffre 1 article 269bis.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. II Ziff. 2 Art. 70ter
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates
(die Änderung betrifft nur den französischen Text)

Antrag der Minderheit I
(Leutenegger Oberholzer, Kiener Nellen, Nidegger, Reimann Lukas, Schwander, Stamm, Vischer Daniel)
Der Einsatz von besonderen Informatikprogrammen zum Zweck der Einschleusung in ein Datenverarbeitungssystem zur Überwachung des Fernmeldeverkehrs ist untersagt.

Antrag der Minderheit II
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Reimann Lukas, Schwander, Stamm)
Streichen

Antrag der Minderheit III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Streichen

Antrag der Minderheit
(Vischer Daniel, Leutenegger Oberholzer, Reimann Lukas, Schwander)
Abs. 1
...
b. es sich um die Verfolgung einer in Artikel 260bis Absatz 1 StGB aufgelisteten Straftat handelt;
...

Antrag der Minderheit
(Kiener Nellen, Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 1bis
Diese besonderen Informatikprogramme dürfen weder bei einer Behörde eines Landes beschafft werden, dessen Nachrichtendienste eine grossangelegte Fernmeldeüberwachung betreiben, noch bei einem Unternehmen mit Sitz in einem solchen Land.

Antrag der Minderheit
(Leutenegger Oberholzer, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 4
Der Untersuchungsrichter führt eine öffentlich zugängliche Statistik über diese Überwachungen, die über den Einsatz und die gerichtliche Verwertung Auskunft gibt.

Antrag der Minderheit
(Leutenegger Oberholzer, Flach, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel, von Graffenried)
Abs. 5
Es dürfen nur Programme zur Anwendung gelangen, bei denen gewährleistet ist, dass die Systemintegrität des betroffenen Rechners sowie der beteiligten Netzwerke nicht geschwächt oder gefährdet wird. Es muss insbesondere ausgeschlossen werden können, dass Dritte aufgrund der Massnahmen ebenfalls in den Rechner eindringen können.

Antrag der Minderheit
(Leutenegger Oberholzer, Kiener Nellen, Schwaab, Vischer Daniel)
Abs. 6
Es dürfen nur in der Schweiz entwickelte Programme zum Einsatz gelangen.

Ch. II ch. 2 art. 70ter
Proposition de la majorité
Al. 1
... de télécommunication sous une forme non cryptée aux conditions ...
Al. 2–4
Adhérer à la décision du Conseil des Etats

Proposition de la minorité I
(Leutenegger Oberholzer, Kiener Nellen, Nidegger, Reimann Lukas, Schwander, Stamm, Vischer Daniel)
L'utilisation de programmes informatiques spéciaux dans le but de s'introduire dans un système informatique pour surveiller la correspondance par télécommunication est interdite.

Proposition de la minorité II
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Reimann Lukas, Schwander, Stamm)
Biffer

Proposition de la minorité III
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Biffer

Proposition de la minorité
(Vischer Daniel, Leutenegger Oberholzer, Reimann Lukas, Schwander)
Al. 1
...
b. il s'agit de poursuivre l'une des infractions énumérées à l'article 260bis alinéa 1 CP;
...

Proposition de la minorité
(Kiener Nellen, Leutenegger Oberholzer, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 1bis
Ces programmes informatiques spéciaux ne peuvent être obtenus auprès d'une autorité d'un pays dont les services de renseignement pratiquent une surveillance des télécommunications à grande échelle ou d'une entreprise dont le siège se trouve dans un tel pays.

Proposition de la minorité
(Leutenegger Oberholzer, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 4
Le juge d'instruction tient une statistique de ces surveillances; accessible au public, cette statistique renseigne sur l'utilisation des programmes et l'exploitation des résultats faite par les tribunaux.

Proposition de la minorité
(Leutenegger Oberholzer, Flach, Kiener Nellen, Ruiz Rebecca, Schneider Schüttel, Schwaab, Vischer Daniel, von Graffenried)
Al. 5
Seuls peuvent être utilisés des programmes qui ne risquent pas d'affaiblir ou de mettre en péril l'intégrité de la machine et des réseaux concernés. Il faut notamment pouvoir exclure tout accès à la machine par des tiers.

Proposition de la minorité
(Leutenegger Oberholzer, Kiener Nellen, Schwaab, Vischer Daniel)
Al. 6
Seuls peuvent être utilisés les programmes développés en Suisse.

Le président (Rossini Stéphane, président): Les propositions de toutes les minorités ont déjà été rejetées au chiffre II chiffre 1 article 269ter.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. II Ziff. 2 Art. 70quater
Antrag der Mehrheit
Titel
Anforderungen an die besonderen Informatikprogramme zur Überwachung des Fernmeldeverkehrs
Abs. 1
Es dürfen nur besondere Informatikprogramme eingesetzt werden, welche die Überwachung lückenlos und unveränderbar protokollieren. Das Protokoll gehört zu den Verfahrensakten.
Abs. 2
Die Ausleitung aus dem überwachten Datenverarbeitungssystem bis zur zuständigen Strafverfolgungsbehörde erfolgt gesichert.
Abs. 3
Der Untersuchungsrichter stellt sicher, dass der Quellcode überprüft werden kann zwecks Prüfung, dass das Programm nur über gesetzlich zulässige Funktionen verfügt.
Abs. 4
Der Bund führt einen Dienst, welcher die besonderen Informatikprogramme beschafft. Der Dienst hat die Aufgabe, die Informatikprogramme zur Überwachung des Fernmeldeverkehrs zu entwickeln oder sie bei Dritten einzukaufen.
Abs. 5
Der Untersuchungsrichter setzt ausschliesslich die vom Bund freigegebenen Informatikprogramme ein und entrichtet eine angemessene Gebühr für die Kosten der Beschaffung und Prüfung der besonderen Informatikprogramme.

Antrag der Minderheit
(Lüscher, Amherd, Barazzone, Chevalley, Eichenberger, Flach, Jositsch, Markwalder, Merlini, Rickli Natalie, Vogler)
Abs. 4, 5
Streichen

Antrag der Minderheit
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, von Graffenried)
Abs. 6
Daten, die unter Missachtung der Bestimmungen der Absätze 1 bis 5 beschafft wurden, dürfen nicht verwertet werden.

Ch. II ch. 2 art. 70quater
Proposition de la majorité
Titre
Exigences posées aux programmes informatiques spéciaux de surveillance de la correspondance par télécommunication
Al. 1
Seuls peuvent être utilisés des programmes informatiques spéciaux qui génèrent un procès-verbal complet et inaltérable de la surveillance. Le procès-verbal est joint au dossier de la procédure.
Al. 2
Le transfert des données du système informatique surveillé à l'autorité de poursuite pénale compétente est sécurisé.
Al. 3
Le juge d'instruction s'assure que le code source peut être contrôlé, dans le but de vérifier que le programme ne contient que des fonctions admises par la loi.
Al. 4
La Confédération gère un service chargé de la mise à disposition des programmes informatiques spéciaux. Ce service a pour tâche de développer les programmes informatiques spéciaux de surveillance de la correspondance par télécommunication ou de les acheter auprès de tiers.
Al. 5
Le juge d'instruction utilise exclusivement des programmes informatiques validés par la Confédération; il s'acquitte d'un émolument approprié pour les frais de mise à disposition et de contrôle des programmes en question.

Proposition de la minorité
(Lüscher, Amherd, Barazzone, Chevalley, Eichenberger, Flach, Jositsch, Markwalder, Merlini, Rickli Natalie, Vogler)
Al. 4, 5
Biffer

Proposition de la minorité
(Vischer Daniel, Kiener Nellen, Leutenegger Oberholzer, von Graffenried)
Al. 6
Les données obtenues en violation des dispositions des alinéas 1 à 5 ne peuvent être exploitées.

Le président (Rossini Stéphane, président): Les propositions des deux minorités ont déjà été rejetées au chiffre II chiffre 1 article 269quater.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. II Ziff. 2 Art. 70e Abs. 4
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Bst. b
Streichen

Ch. II ch. 2 art. 70e al. 4
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Nidegger, Schwander, Stamm, Vischer Daniel)
Let. b
Biffer

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Block 3 – Bloc 3
Allgemeine Bestimmungen, Auskünfte und Sonstiges
Dispositions générales, renseignements et divers

Reimann Lukas (V, SG): Wir sind hier bei den allgemeinen Bestimmungen. Bei meinen Anträgen geht es primär darum, dass die Anbieter – also die Wirtschaft – nicht zu sehr belastet werden. Bei Artikel 5 Absatz 1 Büpf geht es darum, dass die Wirtschaft selber bestimmen kann, wen sie als Vertreter im beratenden Organ haben möchte. Der Bund soll nicht einfach bestimmen können, wer im beratenden Organ der Vertreter der Branche ist.
Bei Artikel 11 Absatz 2 Büpf geht es um die Aufbewahrungsfrist für die Daten im Rahmen eines Strafverfahrens. Da sind wir der Meinung, dass zehn Jahre nach Abschluss eines Strafverfahrens absolut genügen und dass das deshalb so festgelegt werden sollte. Das ist übrigens in vielen Bereichen so üblich.
Bei Artikel 16 Buchstabe b Büpf geht es um die Verfügung bei Schwierigkeiten mit angeordneten Überwachungen. Wenn nach Ansicht der Behörde eine Überwachungsmassnahme technisch ungeeignet ist, technisch nicht durchführbar ist oder nicht zu den im Gesetz oder in den Ausführungsbestimmungen vorgesehenen Überwachungstypen gehört, muss dies unserer Meinung nach in einer Verfügung festgestellt werden.
Bei Artikel 32 Absatz 2 Büpf geht es um die Massnahmen der Anbieter und insbesondere auch um die Verhältnismässigkeit. Wir sind da der Meinung, dass die Anbieter die Kernaufgabe haben, als Unternehmen erfolgreich zu sein. Die Aufgaben im Zusammenhang mit diesem Gesetz dürfen die Anbieter nicht übermässig einschränken. Es darf nicht erwartet werden, dass jedes noch so kleine Gewerbeunternehmen, jeder noch so kleine Betrieb 24 Stunden am Tag an 365 Tagen im Jahr sofort Informationen liefern kann. Ebenso darf nicht jedwede technische Massnahme verlangt werden. Die Massnahmen müssen mit verhältnismässigem Aufwand umzusetzen sein. Daher möchten wir hier den Zusatz «alle geeigneten und in technischer und finanzieller Hinsicht verhältnismässigen Massnahmen» in das Gesetz aufnehmen, gerade auch als Schutz für die kleinen Gewerbebetriebe in unserem Land.
Bei Artikel 39 Absatz 1 Buchstabe a Büpf sind wir der Meinung, es brauche eine rechtskräftige Verfügung. Die Verfügungen des Dienstes unterliegen der Beschwerde nach den allgemeinen Bestimmungen über die Bundesverwaltungsrechtspflege. Der Beschwerde ist grundsätzlich aufschiebende Wirkung zuzuerkennen. Die Anbieterinnen haben kein Interesse daran, willkürlich und ohne Not ein Rechtsmittel zu ergreifen. Man unterstellt hier den Gewerbebetrieben, sie seien einfach generell gegen den Staat oder möchten Kriminelle schützen. Das ist nicht der Fall. Die Gewerbebetriebe möchten Internet- oder Kommunikationsdienste anbieten, und zwar in einem vernünftigen Rahmen, wirtschaftlich, nicht mehr und nicht weniger. Mit einer systematischen Erhebung von Beschwerden ist bestimmt nicht zu rechnen.
Bei Artikel 42 Absatz 3 Büpf geht es um die Frage, ob eine Beschwerde aufschiebende Wirkung hat oder nicht. Wir sind da der Meinung, dass eine Beschwerde aufschiebende Wirkung haben muss.
Das in diesen fünf Minuten kurz zusammengefasst zu den verschiedenen Anträgen, die gestellt wurden.

Vischer Daniel (G, ZH): Ich habe einen Minderheitsantrag zu Artikel 11 gestellt. Hier geht es um die Aufbewahrungsfrist für die Daten. Mein Minderheitsantrag will, dass die Daten von Amtes wegen aus dem System gelöscht werden, sobald die Gründe für die entsprechende Überwachung weggefallen sind. Dies ist der Fall bei Abschluss der Fahndung, Einstellung der Untersuchung oder der Notsuche oder durch Erwachsen des Strafurteils in Rechtskraft.
Es ist eigentlich nicht ganz einsichtig, warum eine solche Bestimmung nicht genügen soll, warum es gummihaft formulierte Weiterungen braucht, wie sie die Mehrheit vorschlägt. Mein Antrag ist griffig, er ist klar und verhindert vor allem, dass über den Untersuchungszweck hinaus Daten dann plötzlich sonst wie verwendet werden können. Er nimmt auch Rücksicht auf die spezielle Situation der Notsuche. Vor diesem Hintergrund denke ich, dass wir eine klare Regelung für die Löschung brauchen. Die Löschung der Daten ist ein zentrales Institut. Sie haben ja jetzt übermässig legiferiert; umso wichtiger ist, dass Sie bei der Löschung klar und bündig bleiben, wie ich dies mit meiner Minderheit verlange.
Im Übrigen ersuche ich Sie, folgende Anträge auch zu unterstützen: bei Artikel 11 den Antrag der Minderheit I (Reimann Lukas), bei Artikel 12 den Antrag der Minderheit Schwaab, bei Artikel 21 Absatz 1 den Antrag der Minderheit Rickli Natalie, bei Artikel 26 Absatz 6 den Antrag der Minderheit Rickli Natalie, bei Artikel 32 Absatz 2 den Antrag der Minderheit Reimann Lukas, bei Artikel 42 Absatz 3 den Antrag der Minderheit Reimann Lukas und vor allem auch den Antrag der Minderheit Vogler bei Artikel 269 Absatz 2 Buchstabe k der Strafprozessordnung, der das Waffengesetz betrifft; da wollen wir jetzt mal sehen, wie ernst es all den Strafverfolgern in diesem Saal ist.

Schneider Schüttel Ursula (S, FR): Ich werde zuerst zur Minderheit Schwaab in Artikel 12 Absätze 4 bis 6 sprechen und aus Gründen der Ratseffizienz und aus zeitlichen Gründen das Votum für die Fraktion daran anhängen.
Der Antrag zu Artikel 12 ist auf der Fahne als Minderheitsantrag Schwaab aufgeführt. Aber ich habe den Kommissionsprotokollen entnommen, dass der Antrag von Herrn Lukas Reimann stammt. Ich habe mit Herrn Reimann gesprochen. Ich werde den Antrag trotzdem begründen und unterstütze ihn selbstverständlich auch. Es geht bei diesem Minderheitsantrag um Folgendes: Wenn erhebliche Sicherheitslücken in Systemen entdeckt werden, welche für die Überwachung genutzt werden, soll der Bundesrat den Betrieb des Systems einstellen können, bis die Sicherheitslücken behoben sind. Um Transparenz herzustellen, sollen nebst dem Bundesrat auch der Datenschutzbeauftragte und die Öffentlichkeit informiert werden. Aufgeworfen ist damit die Frage nach der Verpflichtung von Systeminhabern, Sicherheitslücken in ihren Systemen anzumelden. Eine solche Verpflichtung ist ein wichtiger Standard, der eigentlich in allen Zusammenhängen mit dem Datenschutz erwähnt werden sollte.
Wir haben in der Kommission darüber diskutiert, ob sich erstens die Regelung überhaupt am richtigen Ort befindet und ob es zweitens richtig ist, dass auch die Öffentlichkeit informiert werden soll. Bei erheblichen Sicherheitslücken im System muss reagiert werden. Das ist klar, nur: Wo regeln wir das? Wer wird informiert? Wenn der Minderheitsantrag gutgeheissen wird, hat der Ständerat die Gelegenheit, diese Frage ein zweites Mal zu prüfen. Er hätte die Gelegenheit,

die Frage detaillierter zu prüfen, aber eben nur dann, wenn Sie dem Minderheitsantrag zustimmen. Wenn der Ständerat diese Gelegenheit erhalten soll zu prüfen, ob der Ausdruck «Öffentlichkeit» aus der Bestimmung gestrichen werden soll und ob diese Regelung, die wir hier diskutieren, eher im Datenschutzgesetz ihren Platz haben soll als im Büpf oder eventuell im Büpf an anderer Stelle, sollten Sie dem Minderheitsantrag zustimmen. Darum ersuche ich Sie.
Zur Stellungnahme der SP-Fraktion: Wir werden die Minderheitsanträge mehrheitlich ablehnen. Wir werden allerdings den Minderheitsantrag Schwaab, den ich soeben begründet habe, unterstützen. Wir werden auch den Minderheitsantrag Reimann Lukas zu Artikel 32 Absatz 2 unterstützen.

Brand Heinz (V, GR): Ich spreche heute einmal nicht von Persönlichkeitsschutz, ich spreche auch nicht von Datenhoheit und anderen Sachen, sondern ich spreche heute erstmals im Rahmen dieser Vorlage vom Geld. Die Kommissionsminderheit beantragt Ihnen eine Anpassung von Artikel 23. Bei dieser Anpassung geht es im Wesentlichen in jedem der drei Absätze um Anpassungen verschiedener Natur.
Ich komme zu Absatz 1: In Absatz 1 ist geregelt, welche spezifischen Informationen zur Person gesammelt werden sollen. Die Sammlung zusätzlicher Informationen in Form von weiteren Daten, wie es in einer Verordnung festgelegt werden soll, ist nach Auffassung der Minderheit abzulehnen. Artikel 21 ist diesbezüglich eigentlich klar, und eine weitere Regelung dieser Fragen ist entweder unpraktikabel, unrealistisch oder führt zu einer weiteren und unerwünschten Datensammlung. Oder wollen Sie etwa in einer Verordnung regeln, nach welchen Kriterien beispielsweise die Namen portugiesischer Staatsangehöriger, die hier ein Mobile kaufen bzw. ein Abo abschliessen, erfasst werden sollen? Auch wenn die Datensicherheit ein ehrenwertes Ziel ist, führt sie hier zu einem unerwünschten Perfektionismus.
Absatz 2 betrifft ein formelles Problem, auf das ich nicht weiter eingehen möchte.
Somit bringe ich noch einige Bemerkungen zu Absatz 3 an: Absatz 3 sieht eine Neuregelung im Bereich der Kosten vor. In Absatz 3 ist vorgesehen, dass das Abrufverfahren bzw. die Bereitstellung und Mitteilung der Daten kostenlos und rund um die Uhr zu erfolgen hat. Diese Regelung ist nach Auffassung der Kommissionsminderheit unbillig und daher nicht vertretbar. Die Kommissionsminderheit schlägt Ihnen deshalb vor, dass der Bundesrat eine entsprechende Entschädigungsregelung zu erlassen hat, in welcher die Kosten für die Pflege und Weitergabe der Daten ausdrücklich geregelt werden. Die Kommissionsminderheit ist dabei nicht etwa der Auffassung, dass alle Informationsweitergaben in jedem Fall kostenpflichtig sein müssen. Vielmehr ist die Kommissionsminderheit der Auffassung, dass die diesbezüglichen Aufwendungen der privaten Kommunikationsanbieter hinsichtlich der Kostenfolgen einfach klar geregelt werden sollen. Dabei ist aber auch zu beachten, dass die Erfassung und gegebenenfalls Mitteilung der Daten mit einem beträchtlichen Aufwand verbunden ist, zumal diese sachgerecht und, wie bereits erwähnt, rund um die Uhr erfolgen muss.
Diese Dienstleistungsbereitschaft der Anbieter ist mit einem erheblichen personellen und technischen Aufwand verbunden, den man den privaten Anbietern nicht einfach für den Bedarfsfall so ohne Weiteres und unentgeltlich übertragen kann. Was für die Verwaltung gilt, soll auch für Private gelten: Wer eine Dienstleistung erbringt, soll dafür auch entschädigt werden. Wenn die Dienstleistungen demgemäss von Privaten bezogen werden, sind diese auch adäquat abzugelten.
Die Kommissionsminderheit macht Ihnen daher beliebt, diese Frage auch folgerichtig gesetzlich klar zu regeln. Hierzu ist nach Auffassung der Kommissionsminderheit eine entsprechende Ergänzung von Absatz 3 unerlässlich. Bei dieser Ergänzung geht es allerdings nicht nur um eine formelle Ergänzung der Bestimmung. Mit dieser Anpassung geht es vielmehr um eine wichtige materielle Ergänzung, welche die Ausrichtung von Entschädigungen an die Telekomunternehmen für ihre sachbezüglichen Aufwendungen zum Gegenstand hat.
Ich möchte Sie deshalb ersuchen, dieser Ergänzungsregelung zuzustimmen, auch wenn dieser Antrag von der Kommissionsminderheit stammt.

Vogler Karl (CE, OW): Ich begründe kurz den Minderheitsantrag zu Artikel 269 Absatz 2 Buchstabe k der Strafprozessordnung. Worum geht es? In Artikel 269 Absatz 2 sind die Straftaten aufgeführt, für die eine Überwachung des Post- und Fernmeldeverkehrs überhaupt zulässig ist. Dabei handelt es sich um schwere, jedenfalls qualifizierte Delikte. Richtigerweise, das haben wir heute mehrmals festgestellt, soll nicht für jedes Bagatelldelikt eine Überwachung zulässig sein. Das soll selbstverständlich auch für das Waffengesetz gelten. Würde man den ganzen Artikel 33 des Waffengesetzes ohne die Beschränkung auf Absatz 3 aufnehmen, so hätte das zur Folge, dass beispielsweise eine fahrlässige Widerhandlung gegen das Waffengesetz zu einer überwachungsfähigen Straftat würde. Solches widerspricht klar dem Prinzip der Verhältnismässigkeit. Dementsprechend hat denn auch der Ständerat befunden, dass solches eben gegen das Prinzip der Verhältnismässigkeit verstossen würde, und die Möglichkeit einer Überwachung auf den qualifizierten Tatbestand gemäss Absatz 3 beschränkt.
Ich ersuche Sie zusammen mit meiner Fraktion, der ständerätlichen Fassung und damit meinem Minderheitsantrag, welcher nicht nur verhältnismässig ist, sondern sich auch systematisch richtig in den Deliktskatalog einreiht, zuzustimmen. Was die übrigen Minderheiten in Block 3 betrifft, so verzichte ich im Sinne eines effizienten Ratsbetriebes im Rahmen der weiteren Diskussion zu ebendiesem Block darauf, noch einmal das Wort zu ergreifen, und ersuche Sie, alle übrigen Minderheitsanträge abzulehnen.
Zusammengefasst: Namens der CVP/EVP-Fraktion ersuche ich Sie, in Block 3 alle Minderheitsanträge, mit Ausnahme desjenigen zu Artikel 269 Absatz 2 Buchstabe k der Strafprozessordnung, abzulehnen.

Schwander Pirmin (V, SZ): Ich bitte Sie, meiner Minderheit zu folgen.
Worum geht es? Ich möchte mit meiner Minderheit, dass nicht nur die beschuldigte Person und die überwachte Drittperson, sondern auch alle anderen Kommunikationspartner der überwachten Person über die Überwachung informiert werden müssen.
Warum möchte ich das? Es geht um die Kontrolle; es geht um die Kontrolle auch der Überwacher, und es geht um die Informationsrechte der Überwachten. Wir haben jetzt in diesem Saal vor ein paar Minuten beschlossen, dass besondere Geräte und besondere Software eingesetzt werden können. Wie garantieren Sie, dass diese eingesetzten Mittel bei einer überwachten Person nicht Daten geändert haben? Das wissen Sie nicht, und ich als Betroffener weiss es vielleicht auch nicht. Ich als Betroffener wundere mich einfach, dass sich etwas auf meinem PC geändert und Kosten verursacht hat. Gerade deswegen bin ich froh, wenn mir mitgeteilt wird, dass ich überwacht worden bin. Dann kann ich den Fehler entsprechend besser eruieren und ihm nachgehen.
Ich muss Ihnen sagen: Ich habe solche PC schon gesehen, in denen Daten plötzlich nicht mehr vorhanden waren, in denen Daten plötzlich verändert worden sind, und niemand wusste, warum dies der Fall war. Erst als die Strafverfolgungsbehörde den PC angeschaut hat, wusste man, warum die Daten verschwunden oder verändert worden waren.
Darum muss es ein Recht aller überwachten Personen sein, dass sie informiert werden, wie und womit sie überwacht worden sind, damit sie allfällige Probleme, die sie später auf ihren PC vorfinden, nachvollziehen können.
Ich bitte Sie, hier der Minderheit zu folgen.

Rickli Natalie Simone (V, ZH): Ich spreche zu meinen Minderheitsanträgen zu den Artikeln 21, 22 und 26.
Zuerst zum Minderheitsantrag zu Artikel 21: Was will ich bei Absatz 1 Buchstabe a ändern? Sie sehen, der Bundesrat

beantragt, dass das Geburtsdatum von den Fernmeldedienstanbietern in jedem Fall geliefert werden muss. Es ist aber so, dass das Geburtsdatum nicht in jedem Fall vorhanden ist, und zwar dann – das habe ich bei den Betroffenen nochmals abgeklärt –, wenn es ältere Verträge sind. Heute werden ja nur Mobile-Prepaid-Kunden sowie Kinder und Jugendliche erfasst. Bei Verträgen, die schon früher abgeschlossen wurden, ist das Geburtsdatum unter Umständen nicht bekannt. Ebenso, wenn man das Handy zum Beispiel vom Geschäft hat, ist den Telekomunternehmen das Geburtsdatum nicht bekannt, da der Vertragspartner eine Firma ist. Sie würden hier also etwas verlangen, was neu programmiert werden muss, was massive Mehrkosten zur Folge hat.
Bei Buchstabe b wird vom Bundesrat beantragt, dass sämtliche Adressierungselemente zu liefern sind. Auch hier ist es so, dass nicht alle Adressierungselemente gemäss Fernmeldegesetz in Gebrauch sind. Diese Adressierungselemente dienen ja der Identifikation der Dienste und Systeme, die an einer Kommunikation beteiligt sind. Diese technischen Parameter sind sehr umfangreich, und in der Regel benützt ein Fernmeldedienstanbieter nicht alle Adressierungselemente. Darum beantragen wir bei Buchstabe b die Ergänzung «soweit verfügbar». Es geht auch hier wieder darum, die Firmen zu entlasten bzw. ihnen nicht etwas aufzuerlegen, was viel mehr Kosten verursacht.
Ebenso bei Buchstabe d: Der Bundesrat will, dass weitere, von ihm selber bezeichnete administrative, technische und die Identifikation von Personen erlaubende Daten über Fernmeldedienste bestellt werden können. Es ist wichtig, dass wir im Büpf abschliessend definieren, was die Rechte und Pflichten der Anbieter sind, weil es hier auch um Rechtssicherheit geht.
Dann zu Artikel 22: Der Bundesrat spricht in Absatz 4 von Anbietern, die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten. Wir finden, das ist kein Kriterium. Denken Sie an die vielen Start-ups in der Schweiz, denken Sie zum Beispiel eben an Doodle und Threema, Schweizer Internet-Start-ups. Die sprechen eine grosse Benutzerschaft an, haben aber noch keine grosse wirtschaftliche Bedeutung. Ihnen diese neue Pflicht aufzuerlegen, halten wir für unangebracht. Diese Unternehmen müssten in Überwachungsmassnahmen investieren, was ihre Existenz gefährden könnte.
Zuletzt noch zu Artikel 26 Absatz 6: Hier will der Bundesrat Unternehmen, die Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten, von bestimmten Pflichten befreien. Auch diese Formulierung ist zu wenig konkret. Deshalb schlagen wir Ihnen Folgendes vor: Es ist wichtig, dass die Dienstleistungen von Unternehmen, die ausgenommen werden können, von geringer Bedeutung sind für die Aufklärung strafbarer Handlungen. Zudem sollen Anbieterinnen von Fernmeldediensten im Bildungsbereich von bestimmten gesetzlichen Verpflichtungen befreit werden können. Kleinere Fernmeldedienstanbieterinnen oder Internet-Access-Anbieterinnen gehören zu dieser Kategorie mit geringerer Bedeutung.
Ich bitte Sie, diese Minderheitsanträge zu unterstützen, damit wir Schweizer Internet-Start-ups nicht unnötig belasten, was die Arbeit, vor allem aber was die Kosten betrifft.

Lüscher Christian (RL, GE): Les dispositions faisant l'objet du bloc 3 consistent en des dispositions générales relatives à la surveillance, notamment en ce qui concerne les droits et les devoirs relatifs aux fournisseurs. Au nom de la majorité des membres du groupe libéral-radical, je vous enjoins de soutenir toutes les propositions de la majorité de la commission.
Voici quelques précisions puisqu'il est absolument impossible de couvrir toute la matière. A l'article 11, la proposition de la minorité II (Vischer Daniel) a pour objectif de faire en sorte que toutes les données soient supprimées dès qu'il n'y a plus de raisons de poursuivre une surveillance. Cette proposition va à l'encontre des dispositions du Code de procédure pénale actuel. Ces informations font en effet partie intégrante du dossier pénal et sont donc soumises à l'article 103 du Code de procédure pénale. Par conséquent, de telles données doivent être conservées au moins jusqu'à l'expiration des délais de prescription de l'action pénale et de la peine.
La proposition de la minorité I (Reimann Lukas) prévoit de limiter à 10 ans la durée de conservation des données récoltées dans le cadre d'une demande d'entraide judiciaire au lieu des 30 ans proposés par le Conseil fédéral et la majorité de la commission. Il est vrai que 30 ans est un délai relativement long, mais nous avons affaire ici à des procédures pénales, même parfois avec un aspect international. Elles doivent donc être soumises logiquement aux mêmes délais que les procédures pénales internes, ce qui signifie un délai de conservation de 30 ans, le délai de 30 ans étant celui de la prescription de la peine.
Les fournisseurs de services de télécommunication actifs sur le marché suisse sont en principe conscients de leurs obligations. Il reste néanmoins nécessaire de prévoir des sanctions en cas d'inobservation des injonctions de l'autorité. La proposition de la minorité Reimann Lukas, à l'article 39 alinéa 1 lettre a, vise à ce que la sanction soit infligée après une décision entrée en force. Selon nous, cette proposition est incompatible avec l'urgence du besoin de récolte de preuves. Il faut préférer le mécanisme prévu par la majorité de la commission qui permet d'inciter les personnes soumises à la loi d'exécuter les injonctions dans les meilleurs délais.
L'article 42 présente les voies de droit ouvertes aux personnes obligées de collaborer et aux autorités tenues de s'acquitter d'émoluments auprès du service contre les décisions de celui-ci. Les alinéas 1 et 2 reprennent et explicitent les règles générales de procédure admises par le droit actuel et la jurisprudence du Tribunal fédéral. La proposition de la minorité Reimann Lukas à l'alinéa 3 prévoit que le recours ait un effet suspensif. Cette proposition est contre-productive puisque la récolte de preuves lors d'une procédure pénale constitue en effet un cas d'urgence qui ne saurait souffrir aucun retard. J'ajouterai que la proposition de la majorité de la commission est compatible avec les conditions du Code de procédure pénale telles qu'elles sont consacrées à l'article 387 dudit code.
Concernant les dispositions de l'article 279 du Code de procédure pénale relatives aux communications des mesures de surveillance, la proposition de la minorité Schwander prévoit, à l'alinéa 1, que le cercle des personnes informées soit substantiellement élargi. Le cercle des tiers concernés est déjà défini à l'article 270 lettre b du Code de procédure pénale, à savoir les personnes qui partagent le raccordement avec la personne surveillée. En suivant la minorité de la commission, il faudrait également prévenir les restaurants qui auraient été contactés et auraient livré une pizza à la personne sous surveillance ce qui, de toute évidence, n'est pas le but de la loi. In extenso, il est normal que les possibilités de recours prévues à l'alinéa 3 ne concernent que les personnes surveillées et les tiers. La minorité propose un nouvel alinéa 1bis stipulant de remettre aux personnes concernées des copies des données rassemblées. Il existe déjà aujourd'hui la possibilité pour ces personnes d'obtenir une copie des informations récoltées. Cela serait exagéré, à notre sens, de demander au Ministère public de la Confédération de toujours envoyer de telles informations sans même qu'elles soient requises. A l'alinéa 2, la minorité propose de limiter à un an l'ajournement de la communication. Cette limitation est selon nous problématique. Pour des raisons de sécurité intérieure, ou pour assurer la sécurité de tiers, par exemple d'un informateur, il doit pouvoir être possible de reporter cette communication.
En résumé, je réaffirme la position de la grande majorité du groupe libéral-radical et vous invite à soutenir toutes les propositions de la majorité de la commission au bloc 3.

Guhl Bernhard (BD, AG): Zur Zusammensetzung des beratenden Organs: Der Antrag Reimann Lukas ist auf den ersten Blick nachvollziehbar. Aber ich frage mich, wer denn in-

nerhalb der Branche entscheiden soll, wer diese nun vertritt. So klar ist das dann auch wieder nicht. Handhaben wir es doch so wie in vielen anderen Bereichen. Die BDP-Fraktion wird bei Artikel 5 also für den Antrag der Mehrheit stimmen.
Den Minderheitsantrag Schwaab zu Artikel 12 Absätze 4 bis 6 lehnt die BDP-Fraktion ab. Was der Antrag verlangt, kommt mir wie ein Pranger vor. Wenn einmal eine Fehlfunktion eintritt, soll gemäss Minderheit umgehend die Öffentlichkeit informiert werden, damit dann alle, die diese Vorlage sowieso ablehnen, sagen können: «Händer's gseh, ich ha's scho immer gseit.» Nein, die BDP-Fraktion wird dem nicht zustimmen. Wenn wir eine Informationspflicht definieren wollen, dann soll das im Datenschutzgesetz geschehen.
Bei Artikel 21 unterstützt die BDP-Fraktion die Minderheit Rickli Natalie. Geburtsdatum und Beruf werden heute nicht standardmässig erfasst, sodass dies zu einer Nacherfassung führen würde. An sich hätte man Artikel 21 Absatz 1 in den Übergangsbestimmungen erwähnen müssen, sodass diese Angaben ab Inkrafttreten zu erfassen gewesen wären.
Zuletzt noch zu Artikel 269 Absatz 2 Buchstabe k: Ich bitte Sie, hier der Minderheit Vogler zu folgen. Es ist wichtig, dass wir wirklich nur grobe und keine fahrlässigen Verletzungen ausnehmen.
Das war's, kurz und knapp, von der BDP-Fraktion zu Block 3.

Chevalley Isabelle (GL, VD): Je vais me concentrer sur deux articles. A l'article 22 alinéa 4, la proposition de la minorité I (Rickli Natalie) vise à dispenser les fournisseurs qui n'ont pas un grand nombre d'utilisateurs. Cette demande n'est pas réaliste, car les criminels auraient tôt fait de comprendre les failles du système et de les utiliser. Je m'étonne que cette proposition provienne d'un parti qui ne cesse de prôner plus de sécurité, que ce soit avec les policiers ou avec l'armée, et que dans le même temps on laisse une faille pareille dans la loi.
A l'article 279 du Code de procédure pénale, la proposition de la minorité Schwander vise à ce que toute personne dont les conversations ont été mises sur écoute soit informée. Que la personne qui a subi l'écoute soit informée, c'est logique, mais que tous ces interlocuteurs le soient aussi va simplement bloquer tout le système. Imaginez que la personne téléphone à sa mère, cette dernière devra aussi être informée. Là aussi, ce parti est d'habitude connu pour demander moins de bureaucratie et pas pléthore de bureaucratie, alors que cette dernière grippera simplement le système.
La majorité du groupe vert'libéral soutiendra la proposition de la minorité Vogler à l'article 269 alinéa 2 lettre k et les propositions de la majorité de la commission aux autres articles.

Glättli Balthasar (G, ZH): Wir sind am Ende einer langen Debatte, und ich erlaube mir, statt auf die einzelnen Anträge einzugehen, nochmals kurz einen Rückblick zu machen. Wir haben in einer langen Debatte uns nun der Illusion hingegeben, es sei die richtige Antwort auf die tatsächlich bestehende Bedrohung durch Verbrechen, wenn man Bürgerrechte erster Klasse wie das Recht auf Privatsphäre, wie das Recht auf nichtüberwachte Kommunikation ausser Kraft setzt. Wir haben es nicht geschafft, Kompromisse zu finden, die aus grüner Sicht dem Anliegen einer verhältnismässigen Bekämpfung des Verbrechens und Stärkung der Untersuchungsmassnahmen entsprochen hätten. Stattdessen haben wir – partout eigentlich, kann man sagen – in diesen Stunden jetzt die Wünsche der Hardliner erfüllt.
Ein Argument bezüglich Vorratsdatenspeicherung, das war ja eine der Hauptauseinandersetzungen, möchte ich doch noch korrigieren. Ich habe mir die Mühe genommen, bei zwei Telekomanbietern nachzufragen. Einen davon musste ich nicht fragen, er hat sich sogar entrüstet bei mir gemeldet und sich darüber beschwert, dass hier den ganzen Tag behauptet wurde, diese Daten würden von den Anbietern sowieso gespeichert. Man speichert die Nummern, ja. Man speichert sie dreissig Tage lang, so steht es in den AGB, falls die Rechnung bestritten wird. Der ganze Rest ist wegen unserer Überwachungsmanie, das gilt ebenso für IP-Adressen, ebenso für die gesamten Ortsangaben. Die braucht es für die Abrechnung nicht.
Bei der Swisscom haben zwei Drittel der Abonnenten im Postpaid-Bereich – also nicht im Prepaid-Bereich – bereits ein Infinity-Abo. Das heisst, da muss man überhaupt keine Anrufe und Anrufdauern speichern, um beweisen zu können, wer wie viel und wie lang telefoniert hat, sondern die Abonnenten kriegen eine Pauschalrechnung. Das sind 2,1 Millionen Personen alleine bei der Swisscom; auch bei den anderen Anbietern gibt es solche Abos.
Enttäuscht hat mich natürlich vor allem jener Teil des Parlamentes, der sich liberal nennt und die Freiheiten hier einschränkt. Es gibt Ausnahmen, ja, Ruedi Noser, aber eine Schwalbe macht noch keinen Frühling. Enttäuscht haben mich aber nicht nur die Liberalen. Enttäuscht hat mich auch die SVP. Sie ist wirklich als Wachhund für die Bürgerfreiheiten in der Kommission aufgetreten, und sie ist hier im Plenum als zahnloses Stoffhündchen Willy gelandet. *(Teilweise Heiterkeit)*
Le groupe des Verts soutient la sécurité et est favorable à ce que les autorités de poursuite pénale disposent de moyens nécessaires et proportionnés. Mais nous ne céderons pas, en tant que Verts, à la tentation de noyer les libertés individuelles dans un déluge sécuritaire.
Pour cette raison, nous rejetterons cette révision de la loi sur la surveillance de la correspondance par poste et télécommunication.

Stamm Luzi (V, AG): Die SVP-Fraktion mag tatsächlich nicht einheitlich stimmen, aber das scheint mir auch normal, weil diese Fragen, die wir hier auf dem Tisch haben, nicht den Rechts-links-Gegensatz betreffen, nicht parteiabhängig sind. Frau Bundespräsidentin, Sie haben zu Beginn des Nachmittags gesagt, dass vor allem diejenigen zuhören sollen, die von den Abwägungen der Grundrechte sprechen. Es geht tatsächlich um Grundrechte und Grundsätzliches, darum: Freiheit einerseits, effiziente Strafverfolgung andererseits. Es geht aber auch um Staatsmacht einerseits und Individuum andererseits. Da kann man in guten Treuen verschiedene Meinungen haben. Es gibt keinen Grund, Frau Bundespräsidentin, diejenigen zu kritisieren, die gegenüber dieser Vorlage misstrauisch sind. Misstrauisch sind immer diejenigen und müssen alle diejenigen sein, welche die Macht nicht haben. Das war immer so in der Geschichte. Alexander Solschenizyn, der berühmte Kritiker der UdSSR, hat gesagt: «In der UdSSR wird die Durchschnittsbevölkerung kriminalisiert, und die Kriminellen werden durch das System geschützt oder sitzen sogar drin.» Wenn Sie von der politischen Linken Edward Snowden anschauen, müssen Sie zu Recht sagen: Da wehrt sich einer gegen die riesige Macht der Amerikaner.
Selbstverständlich ist die SVP immer dafür, dass die Polizei effizient bleiben kann und sogar bessere Mittel bekommt. Aber wenn ich zum Fussballspiel gehe und am Eingang einfach drei Stunden warten muss, mir sogar der Schirm weggenommen wird und ich gleichzeitig sehen kann, wie sich Leute zusammenschlagen und niemand eingreift, bin ich nicht mehr bereit, der Polizei mehr Mittel zukommen zu lassen. Nun geht es um die technischen Mittel. Selbstverständlich sind wir von der SVP grundsätzlich für bessere technische Mittel, wenn wir an das Attentat auf «Charlie Hebdo» in Paris denken. Aber ob Sie an Fussballspiele oder an den Strassenverkehr denken, immer müssen Sie sich fragen, ob die Polizei wirklich die Kriminellen verfolgt, überall ist die Frage: Was macht der Staat mit diesen Mitteln?
Ich gehe auf die internationale Ebene. Frau Bundespräsidentin, Sie haben gesagt: «Zeigen Sie mir die Missbräuche.» Herr Vischer hat Ihnen das richtig beantwortet: Woher sollen wir die kennen? Ich hatte z. B. jemanden aus dem Nahen Osten in meiner kleinen Kanzlei, der sagte zu mir: «Mit wem arbeitet die Schweiz zusammen? Liefert die Schweiz meine Daten aus?» Ich war zu wenig vorsichtig. Ich habe anderthalb Jahre später von seiner Familie die Mitteilung erhalten, der Mann sei erschossen worden.

Ich weiss nicht, ob die Schweiz – ich erinnere an die Debatte von letzter Woche – im Falle von Ägypten mit Mubarak, Mursi oder mit as-Sisi zusammenarbeitet. Ich weiss nicht, ob dieser Ermordete, den ich kannte, ans Messer geliefert worden ist, weil wir den Amerikanern Bankdaten geliefert haben. Ich weiss es nicht, aber mit der Erhebung und Herausgabe von Daten, muss man vorsichtig sein.
Frau Bundespräsidentin, ich fordere Sie auf, uns Erfolgsbeispiele zu nennen. Wo sind denn die Beispiele, wonach wir z. B. via Trojaner Kriminalität aufdecken können? Ich habe von den Amerikanern gesprochen. Wenn man den Deutschen Informationen gibt, dann klingelt man vielleicht Herrn Zumwinkel – das war der Vorstandsvorsitzende der Deutschen Post AG – um sechs Uhr morgens aus dem Bett, filmende Kameras bereits vor Ort; aber man geht nur denjenigen Leuten nach, die einige Franken in die Schweiz transferiert haben. Der schweren Kriminalität in Kosovo sind die Deutschen aber nicht nachgegangen. Als wir die Information lieferten, dass dort Heroinhandel aufgebaut wird, als Dick Marty sogar schilderte, dass dort Leute ermordet und ihnen Organe entnommen würden, so hat das die Deutschen nicht interessiert.
Ich habe jetzt von Kosovo gesprochen; beziehen Sie es für die heutige Zeit vielleicht auf die Geldbeschaffungsmechanismen in Sri Lanka oder in Eritrea: Wohin geht das Geld, das hier in der Schweiz zusammengesucht wird? Wenn die Schweiz mit Trojanern wirklich organisierte Kriminalität aufdecken kann, wenn Sie mir melden, dass man einen dem «Charlie Hebdo»-Attentat ähnlichen Anschlag verhindern könne, dann sage ich Ja dazu. Wenn wir aber gar nicht aufgezeigt erhalten, wo die Schweiz mit Trojanern effizient sein kann, wenn man mir einfach sagt, man müsse den Bürger jetzt besser überwachen, damit man die Kriminalität und den Terrorismus in den Griff bekomme, bleibe ich skeptisch.
Ich schliesse mit der Bemerkung zu den vielen Minderheitsanträgen: Ein grosser Teil der SVP-Fraktion ist dafür, einige der Minderheitsanträge zu unterstützen; das aus den Gründen, die ich soeben zusammenzufassen versucht habe.

Sommaruga Simonetta, Bundespräsidentin: Zum Schluss ist diese Debatte jetzt noch einmal ein bisschen grundsätzlich geworden. Es ist noch einmal die Frage nach dem Recht auf Privatsphäre gestellt worden. Das ist eine sehr wichtige Frage. Das Recht auf Privatsphäre ist ein wichtiges Recht, das wir hochhalten wollen. In diesem Gesetz geht es um Strafverfahren wegen eines konkreten Verdachts auf eine schwere kriminelle Handlung. In dieser Situation wird das Recht auf Privatsphäre eingeschränkt, das ist so. Heute wird es in dieser Situation zum Beispiel eingeschränkt – wenn ein Zwangsmassnahmengericht dies bewilligt –, indem Hausdurchsuchungen durchgeführt werden. Das ist, so würde ich einmal sagen, auch ein ziemlich grosser Eingriff in die Privatsphäre. Es wird in dieser Situation eingeschränkt, indem Beschlagnahmungen erfolgen; auch das ist ein ziemlich grosser Eingriff, und zwar nicht nur in die Privatsphäre, sondern auch in das Eigentum.
In dieser Situation soll es eben auch möglich sein – das haben Sie heute im Wesentlichen beschlossen –, dass Überwachungen stattfinden, allerdings nur dann, ich sage es noch einmal, wenn wegen eines konkreten und dringlichen Verdachts auf eine schwere kriminelle Handlung ein Strafverfahren eröffnet worden ist. Wenn ein Gericht festgestellt hat, dass man mit anderen Massnahmen nicht weiterkommt, und die entsprechende Massnahme bewilligt, ist eine gewisse Einschränkung des Rechts auf Privatsphäre richtig.
Herr Stamm, Sie haben wieder davon gesprochen, dass der Bürger besser überwacht wird. Besser überwacht wird eben der Bürger, gegen den ein konkreter Verdacht auf schwere kriminelle Handlungen besteht und gegen den ein Strafverfahren eröffnet worden ist. Sie haben Snowden erwähnt. Ich verweise gerne noch einmal auf das Nachrichtendienstgesetz. Sie haben gesagt, Sie wüssten nicht, mit welchen Diensten die Schweiz zusammenarbeite. Auch da verweise ich auf das Nachrichtendienstgesetz. Das haben Sie dort besprochen, dort geht es um die präventive Überwachung. Heute sprechen wir von der Strafverfolgung.
Ich komme jetzt noch zu Block 3, dort gibt es verschiedene Anliegen, bei denen allerdings kein unmittelbarer innerer Zusammenhang besteht. Ich beschränke mich im Folgenden auf die aus meiner Sicht wichtigsten Punkte.
Zuerst zu den Aufbewahrungsfristen gemäss Artikel 11: Diesem Artikel liegt der allgemeine Grundsatz zugrunde, dass die Fristen des anwendbaren Verfahrensrechts, also insbesondere der Strafprozessordnung, jenen des Büpf vorgehen. Im Büpf sind also nur Maximalfristen vorgesehen.
Die Minderheit I (Reimann Lukas) verlangt im Rechtshilfebereich eine Verkürzung auf zehn Jahre. Das wäre nicht sachgerecht, weil einerseits Rechtshilfeverfahren oft mehr als zehn Jahre dauern und andererseits, ich denke, das ist wichtig, die vorgesehene Frist von dreissig Jahren den maximalen Fristen für die Verfolgungs- und Vollstreckungsverjährung entspricht. Sie können doch nicht für die Verfolgungsverjährung dreissig Jahre vorsehen und dann sagen, dass man die Mittel für die Strafverfolgung aber einfach nach zehn Jahren abklemmt.
Die Minderheit II (Vischer Daniel) verlangt, dass die Daten aus dem System des Dienstes ÜPF gelöscht werden, sobald die Gründe für die Überwachung weggefallen sind oder das Verfahren abgeschlossen ist. Sie wissen alle, dass es manchmal auch Revisionen gibt, dass man ein abgeschlossenes Verfahren noch einmal überprüft. Was haben Sie dann? Dann haben Sie die Grundlagen nicht mehr, aufgrund derer ein Entscheid gefällt worden ist. Das heisst, Sie würden eigentlich eine Revision eines Urteils verunmöglichen. Ich denke nicht, dass das im Interesse der Betroffenen ist.
Bei Artikel 16 Buchstabe b möchte die Minderheit Reimann Lukas den Dienst ÜPF verpflichten, eine Verfügung zu erlassen, wenn eine angeordnete Überwachung nicht durchführbar oder ungeeignet erscheint. Der Dienst ÜPF ist aber eine Schnittstelle, er macht nicht selber Überwachungen. Er überlegt sich nicht, ob eine Überwachung jetzt sinnvoll ist. Er macht vielmehr das, was die Strafverfolgungsbehörde in Auftrag gibt und was vom Zwangsmassnahmengericht bewilligt worden ist. Der Dienst ÜPF ist eine Schnittstelle zwischen der Staatsanwaltschaft und der Fernmeldedienstanbieterin und überprüft Entscheide eines Zwangsmassnahmengerichtes nicht. Eine Verfügung müsste zudem zu einem Rechtsmittelverfahren führen. Ein solches lässt sich aber nicht durchführen, weil ja die Fernmeldedienstanbieterin durch einen solchen Entscheid keinen Nachteil hätte und damit auch nicht beschwert wäre. Aber auch ein Beschwerderecht für die Staatsanwaltschaft wäre unsinnig, weil diese ja die Erkenntnisse des Dienstes ÜPF einfach umsetzen kann, indem sie eine neue Überwachungsanordnung erlässt.
Zur Frage der Einschränkung des Geltungsbereichs bzw. des Umfangs der mittels Überwachung zu erhebenden Informationen habe ich mich bereits in Block 1 geäussert.
Ich bitte Sie, die Minderheitsanträge bei Artikel 21 Absatz 1 und Artikel 22 Absatz 4 abzulehnen. Es ist nicht einzusehen, weshalb das von den Fernmeldedienstanbieterinnen registrierte Geburtsdatum oder die zu einem Abonnenten gehörende Telefonnummer nicht bekanntgegeben werden soll. Was übrigens den Beruf anbelangt, so steht ja im Entwurf des Bundesrates, dass dieser nur angegeben werden muss, falls er bekannt ist. Wir verlangen also nichts, was nicht ohnehin bekannt ist.
Die für die kleineren Anbieterinnen verlangte Ausnahme für die Ausdehnung der Pflichten gemäss Artikel 22 Absatz 4 ist ebenfalls nicht sachgerecht. Schauen Sie, auch kleinere Anbieter können ihre Dienstleistungen für eine grosse Benutzerschaft anbieten. Die verlangte Einschränkung würde die Strafverfolgung empfindlich schwächen. Zu meinen, weil jemand ein kleiner Anbieter sei – so ein herziger, kleiner Anbieter –, würden sicher keine Kriminellen seinen Dienst benutzen, wäre ein bisschen naiv.
Bei Artikel 42 Absatz 3 will eine Minderheit, dass Beschwerden gegen Verfügungen des Dienstes eine aufschiebende Wirkung zukommt. Gemäss dem Entwurf des Bundesrates

soll eine Beschwerde nur dann eine aufschiebende Wirkung erhalten, wenn die Beschwerdeinstanz das anordnet. Falls dem nicht so wäre, würden bis zum Entscheid über die aufschiebende Wirkung wichtige Beweismittel unwiderruflich verlorengehen. Auch die Fahndung oder die Suche nach entflohenen oder nach vermissten Personen würde dadurch wesentlich erschwert.
Ich komme zum Schluss und fasse zusammen: Ich bitte Sie auch in diesem Block, der Mehrheit Ihrer Kommission zu folgen.

Rickli Natalie Simone (V, ZH): Frau Bundespräsidentin, Sie haben in Bezug auf Artikel 21 Absatz 1 Buchstabe a gesagt, das Geburtsdatum der Teilnehmerin oder des Teilnehmers sei allen Fernmeldedienstanbietern bekannt. Das ist nicht immer der Fall, wie ich bereits vorhin ausgeführt habe. Bei älteren, bereits bestehenden Abos, bei Geschäftskundenabos usw. ist das Geburtsdatum nicht bekannt. Es würde einen erheblichen Mehraufwand für die Firmen bedeuten, wenn sie diese Angaben liefern müssten. Ist der Bund bereit, dafür die Kosten zu übernehmen? Können Sie ausführen, was mit der Formulierung «weitere vom Bundesrat bezeichnete administrative, technische und die Identifikation von Personen erlaubende Daten über Fernmeldedienste» in Buchstabe d gemeint ist?

Sommaruga Simonetta, Bundespräsidentin: Besten Dank, Frau Rickli. Wenn die Fernmeldedienstanbieterinnen die Kosten ausweisen können, die entstehen, weil sie das Geburtsdatum von Kundinnen und Kunden liefern müssen, die so lange schon bei Ihnen sind, dass sie das Geburtsdatum nie erhoben haben, würde ich sagen, dass wir da dieses Geld dann schon noch aufbringen würden. Es sind nämlich nur wenige Leute. Das Geburtsdatum wird wirklich standardmässig verlangt. Wenn das aber wirklich der grosse Zusatzaufwand wäre, würden wir das schon anschauen. Ich muss Ihnen einfach sagen: Bis jetzt habe ich von den Fernmeldedienstanbieterinnen relativ häufig laute Klagen über die Kosten gehört, und wenn wir sie dann gebeten haben, diese Kosten auszuweisen, ist dann jeweils nicht wahnsinnig viel gekommen. Aber ich schaue das gerne an.
Zu Ihrer zweiten Frage, was diese vom Bundesrat zu bezeichnenden administrativen, technischen Daten sind, die eben die Identifikation der Person erlauben: Das sind eben gerade diese Dinge, die in einer Verordnung festgelegt werden müssten. Das sind aber nicht neue Dinge, die jetzt noch nicht bestehen, sondern einfach Daten, die sicherstellen, dass der Zugriff auf die gesuchten Personen funktioniert. Aber ich denke, die Verordnung – das wird ja auch in einer Verordnung festgehalten – erarbeiten wir zusammen mit den betroffenen Branchen, das machen wir nicht einfach im Büro. Wir werden hier schauen, was wir brauchen und was die Fernmeldedienstanbieterinnen liefern können, damit man eben erkennt, was man hier aufgrund dieses Gesetzes braucht – Sie unterstützen das ja auch – und was hier möglich ist. Hier kann ich Ihnen also anbieten, dass wir das zusammen mit den Fernmeldedienstanbieterinnen besprechen und vorbereiten, wenn wir das dann in der Verordnung festlegen.

Ruiz Rebecca Ana (S, VD): Madame la présidente de la Confédération, un arrêt récent du Tribunal fédéral concernant la durée pendant laquelle le nom et l'adresse d'un abonné à la téléphonie ou à Internet peuvent être obtenus a mis en évidence le fait que la durée de conservation de ce type d'information était de dix ans en vertu du Code des obligations. Or il se trouve que le Conseil des Etats a modifié l'alinéa 2 de l'article 21 de la loi sur la surveillance de la correspondance par poste et télécommunication en introduisant une durée de conservation de douze mois, partant du principe qu'à la fin du contrat d'abonnement, le fournisseur pouvait effacer les informations relatives à l'abonné. Ensuite, la Commission des affaires juridiques de notre conseil a, par analogie, procédé à une modification de l'alinéa 2 de l'article 22, en ajoutant là aussi un délai de conservation de douze mois. Alors que ce délai est actuellement de dix ans, si on en croit du moins le Tribunal fédéral, n'est-il pas incohérent d'avoir introduit ici une durée de conservation moindre, qui pourrait dès lors poser des problèmes aux autorités de poursuite pénale?

Sommaruga Simonetta, Bundespräsidentin: Frau Ruiz, besten Dank für diese Frage. Es gab diesen Bundesgerichtsentscheid in der Tat. Ich muss Ihnen sagen, es ist im Moment zu früh, wir müssen diesen Entscheid noch analysieren, um abzuschätzen, ob das einen Einfluss auf Artikel 22 hat. Ich habe aber Verständnis für Ihre Befürchtung, dass Artikel 22 Absatz 2, so, wie er jetzt formuliert ist, zu einer Einschränkung der geltenden Auskunftspflicht führen könnte. Ich schlage Ihnen vor, dass wir jetzt den Bundesgerichtsentscheid genau analysieren und schauen, was die Auswirkungen sind. Sie haben jetzt in Artikel 22 Absatz 2 eine Differenz geschaffen. Ich schlage Ihnen vor, dass wir im Erstrat, wenn die Vorlage zurückgeht, zusammen mit der Analyse des Bundesgerichtsentscheides diese Frage noch einmal anschauen.

Flach Beat (GL, AG), für die Kommission: Ich versuche, mich möglichst kurz zu halten, das meiste ist schon gesagt worden.
Zu Artikel 5 Absatz 1 liegt ein Antrag der Minderheit Reimann Lukas vor, die will, dass die Telekommunikationsanbieter selbst bestimmen können, wer in diesem vom EJPD zusammengerufenen Gremium Einsitz nimmt. Das gab in der Kommission 8 Punkte für Demokratieverständnis, aber 15 Minuspunkte für Praktikabilität. Die Kommission hat diesen Antrag abgelehnt, weil sie fand: Das funktioniert mit 300 verschiedenen Anbietern wahrscheinlich nicht.
Zu Artikel 11 haben wir zwei Minderheitsanträge, die beide die sogenannte Aktenaufbewahrung beschlagen. Das Büpf ist ja eigentlich eine Ausführungsgesetzgebung zur Strafprozessordnung, und in der Strafprozessordnung ist die Aktenaufbewahrung in Artikel 103 geregelt. Aus diesem Grund hat die Kommission diese beiden Anträge abgelehnt, den Antrag Reimann Lukas mit 15 zu 8 Stimmen bei 2 Enthaltungen, den Antrag Vischer Daniel mit 16 zu 8 Stimmen bei 1 Enthaltung.
Zu Artikel 12 gibt es einen Minderheitsantrag Schwaab auf neue Absätze 4 bis 6. Dabei geht es um die Sicherheit des Verarbeitungssystems. Artikel 12 regelt die Aufgaben des Dienstes für die Überwachung des Post- und Fernmeldeverkehrs. Die Minderheit schlägt vor, dass für Fälle, in denen der Dienst feststellt, dass ein Datenverarbeitungssystem fehlerhaft arbeitet, allenfalls von einem Virus oder Ähnlichem befallen ist, es eine Meldepflicht geben soll, via Bundesrat und allenfalls auch an die Öffentlichkeit mit Einbezug des Eidgenössischen Datenschutzbeauftragten. Dieser Antrag ist ganz knapp, mit 11 zu 11 Stimmen und Stichentscheid des Präsidenten, abgelehnt worden. Ich glaube, die Mehrheit hat vor allen Dingen ausgeführt, dass man wahrscheinlich nicht am richtigen Ort regelt, wenn der Dienst für die Überwachung des Post- und Fernmeldeverkehrs nur in diesen Fällen, in denen er überhaupt etwas erfährt – er bekommt ja diese Daten einfach ausgeliefert –, einen Auftrag haben soll, tätig zu werden.
Bei Artikel 16 Buchstabe b haben wir eine Minderheit, die in eine ähnliche Richtung geht. Sie will, dass der Dienst für die Überwachung des Post- und Fernmeldeverkehrs Überwachungsanordnungen, wenn sie nicht funktionieren oder allenfalls widerrechtlich sind, per Verfügung ablehnen könnte. Das ist beim Büpf einfach am falschen Ort, weil das ja quasi eine materielle Prüfung einer Überwachungsanordnung wäre, die von einem Zwangsmassnahmengericht bereits geprüft und genehmigt worden ist. Hier geht es vielmehr darum, dass der Dienst die Möglichkeit hat, bei technischen Problemen halt eben bei der zuständigen Staatsanwaltschaft vorstellig zu werden und dann abzuklären, wie man das dort handhaben will. Dieser Antrag wurde mit 18 zu 5 Stimmen bei 2 Enthaltungen abgelehnt.
Bei Artikel 21 Absatz 1 hat die Frau Bundespräsidentin bereits Auskunft gegeben zu den verschiedenen Angaben, die

da zu machen sind, über die Lieferung der Geburtsdaten usw.
Ich möchte nur noch ganz kurz Artikel 22 Absatz 4 Büpf erwähnen: Hier gibt es die beiden Minderheiten I und II (Rickli Natalie), wo es wieder darum geht, wie man mit abgeleiteten Diensten und Unternehmen umgeht, die nicht selbst, aber doch irgendwo in abgeleiteter Art und Weise Kommunikationsdienstleistungen anbieten. Auch hier geht es wieder darum, dass die grosse Benutzerschaft oder das wirtschaftliche Kriterium eben nicht die einzigen Kriterien sein können und dass es nicht sein kann, dass man hier kleinere Dienste, die aber allenfalls eine grosse Benutzerschaft haben, auch wenn sie wirtschaftlich noch nicht erfolgreich sind, komplett davon ausnimmt. Es kommt eben darauf an, wer sich dann dort in so einem Netzwerk tummelt.
Der von der Minderheit I aufgenommene Antrag wurde mit 17 zu 5 Stimmen bei 3 Enthaltungen und der der Minderheit II aufgenommene mit 15 zu 4 Stimmen bei 3 Enthaltungen abgelehnt.

Schwaab Jean Christophe (S, VD), pour la commission: Au bloc 3, je m'exprimerai sur les propositions de minorité aux articles 23 à 42 de la loi ainsi qu'aux dispositions qui concernent le Code de procédure pénale.
A l'article 23 de la loi, il s'agit de donner la possibilité au Conseil fédéral de régler les modalités de la saisie des données destinées à identifier les auteurs de crimes sur Internet. La minorité Brand propose de biffer l'alinéa 1 et, à l'alinéa 3, de créer la possibilité de verser une indemnité aux opérateurs qui doivent effectuer ces surveillances. La majorité de la commission vous demande d'en rester à la version du Conseil fédéral à laquelle a adhéré le Conseil des Etats. La commission a rejeté cette proposition défendue par la minorité Brand par 14 voix contre 3 et 3 abstentions. Il est en effet nécessaire de donner au Conseil fédéral la compétence de définir lui-même les spécifications techniques. Pour de plus amples détails, je renvoie au message. Quant à la question de l'indemnité, elle est inutile ici, d'une part parce qu'il ne s'agit que de la possibilité pour le Conseil fédéral de prévoir la livraison gratuite des données, et d'autre part parce que dans le droit en vigueur le Conseil fédéral a déjà prévu une indemnisation.
A l'article 26 alinéa 6, la minorité Rickli Natalie souhaite exempter certains fournisseurs de télécommunication de faible importance de l'obligation de prendre les mesures préparatoires à une surveillance. Le projet du Conseil fédéral dispose déjà que certains fournisseurs, notamment dans le domaine de l'éducation, sont exemptés de l'obligation de fournir certaines données. La précision que souhaite Madame Rickli n'est cependant pas pertinente. Elle est même dangereuse, car elle empêcherait que l'on assujettisse un petit exploitant qui présente un risque particulier. Certes, les petits exploitants n'ont en règle générale pas à effectuer eux-mêmes les surveillances, mais il peut arriver que certains soient particulièrement susceptibles de voir leurs services utilisés à des fins criminelles. On peut penser par exemple à l'accès gratuit à Internet mis à la disposition des clients du café du coin, qui se trouve être le stamm de la pègre locale. Il faut donc que dans ces cas très particuliers, une surveillance reste possible, même si elle ne sera pas la règle, car il s'agit dans tous les cas d'une formulation potestative. Par ailleurs, l'alinéa 6 prévoit certes l'obligation de livrer les données secondaires dont disposent ces petits opérateurs, mais pas de les conserver. Cela reste donc une obligation de moindre portée que celle imposée aux grands opérateurs.
C'est donc par 13 voix contre 7 et 2 abstentions que la commission a rejeté la proposition défendue par la minorité Rickli Natalie.
A l'article 32, il est question d'obliger tous les fournisseurs de services de télécommunication à collaborer avec le service pour mettre en oeuvre une mesure de surveillance non standardisée, pour en garantir une exécution sans difficulté. Une proposition défendue par la minorité Reimann Lukas vise à ce que l'on se limite aux mesures utiles et raisonnables sur le plan technique. La commission l'a rejetée par 14 voix contre 8 et 1 abstention, car elle est redondante. En effet, le principe de proportionnalité doit s'appliquer en tout temps et il n'est donc pas nécessaire de le spécifier lors de chaque nouvelle étape du processus.
L'article 39 alinéa 1 lettre a constitue la base légale pour punir celui qui ne donne pas suite à une décision du service d'exécuter une surveillance. Une minorité Reimann Lukas a repris la proposition visant à limiter la possibilité de sanctions à la non-observation d'une décision entrée en force. La commission a rejeté cette proposition par 16 voix contre 5 et 2 abstentions. En effet, il y a un très grand risque que cette proposition retarde les enquêtes pénales. S'il faut attendre l'échéance du délai de recours, puis le résultat de l'éventuel recours, les criminels qu'il s'agit de surveiller auront depuis longtemps commis leur méfaits, en auront même commis d'autres, auront fait disparaître des preuves, voire carrément pris la poudre d'escampette. Les autorités auraient pu l'éviter, pour autant qu'elles aient su ce qui se tramait. Or, cela est impossible, faute de pouvoir exécuter la surveillance requise.
Rejeter la proposition de la minorité Reimann Lukas ne veut pas dire que toute voie de recours est fermée. Au contraire, cela reste possible. Au cas où une surveillance illégale serait ordonnée, il serait possible de la faire annuler et de prononcer les sanctions idoines.
Avec la minorité Reimann Lukas à l'article 42 alinéa 3, nous sommes un peu dans la même thématique que celle de la rapidité de l'utilisation des moyens d'enquête. Monsieur Reimann souhaite que les recours contre les décisions de surveillance du service aient l'effet suspensif. Voilà qui risquerait à nouveau d'entraver le bon fonctionnement de la poursuite pénale et de permettre aux criminels d'avoir plusieurs coups d'avance sur les autorités. Il y a d'ailleurs un parallèle avec les décisions procédurales du Code de procédure pénale qui n'ont, à juste titre, pas non plus d'effet suspensif. C'est donc par 15 voix contre 8 et 1 abstention que la commission s'est prononcée en faveur de la version du Conseil fédéral à laquelle a adhéré le Conseil des Etats. Elle vous demande d'en faire de même.
A l'article 269 alinéa 2 lettre k du Code de procédure pénale, la majorité de la commission reprend une idée évoquée lors des débats du premier conseil, afin que le trafic d'armes à titre non professionnel fasse aussi partie des infractions qui permettent d'ordonner une surveillance. En effet, il s'agit de pouvoir enquêter sur des groupes ou individus, par exemple des djihadistes, qui se livrent au trafic d'armes sans but lucratif, ce qui n'enlève rien à la dangerosité de ce trafic. Une minorité Vogler reprend la proposition d'en rester à la version adoptée par le premier conseil. La commission s'y est opposée par 12 voix contre 9 et 5 abstentions.
Enfin, à l'article 279 du Code de procédure pénale, une minorité Schwander demande aux alinéas 1 et 1bis que toute personne concernée par une mesure de surveillance reçoive copie de toutes les données personnelles rassemblées au cours de la surveillance. De l'avis de la majorité de la commission, cette disposition serait contraire à la systématique de la législation en vigueur concernant la procédure pénale. En effet, les personnes concernées ont déjà le droit de consulter les documents qui les concernent et d'obtenir copie de tout ce qu'elles souhaitent, mais il serait totalement disproportionné que le procureur leur fournisse d'office tous les documents en question.
En outre, cette disposition concernerait soit les tiers qui partagent un moyen de communication avec la personne surveillée, au nombres desquels les membres de la famille, les colocataires et les collègues, soit les tiers avec qui la personne surveillée a eu une quelconque télécommunication, y compris les livreurs de pizzas, les chauffeurs de taxis, ceux d'Uber, ceux d'UberPOP, les amis et connaissances, etc. Communiquer l'ensemble des données à toutes ces personnes serait contraire au principe de la proportionnalité.
La proposition de la minorité Schwander prévoit par ailleurs à l'article 279 alinéa 2 du Code de procédure pénale qu'il ne soit possible de renoncer à informer la personne concernée

qu'elle a fait l'objet d'une mesure de surveillance que pour un an au plus. Or il peut arriver, par exemple pour le besoin d'autres enquêtes ou en cas de nouveaux soupçons portant sur cette personne, qu'il faille renoncer à l'en informer pour une plus longue durée afin d'éviter qu'elle ne dissimule des preuves ou qu'elle ne se mette à faire preuve d'encore plus de prudence, ce qui entraverait bien entendu une éventuelle inculpation, voire une éventuelle condamnation. Il se peut aussi que ne pas informer la personne concernée soit indispensable pour garantir la sécurité d'un tiers, par exemple un informateur.
Quant à l'alinéa 3, il serait aussi contraire à la systématique de la loi de prévoir ici une voie de recours pour toutes les personnes qui ont participé une fois à une communication avec la personne soupçonnée; cela n'existe du reste nulle part ailleurs dans le Code de procédure pénale.
Au final, la commission vous invite à rejeter la proposition défendue par la minorité Schwander par 15 voix contre 3 et 3 abstentions, sauf à l'alinéa 2, où elle vous invite à le faire par 14 voix contre 4 et 3 abstentions.

Art. 1, 3, 4
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 5
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Brand, Egloff, Nidegger, Rickli Natalie, Schwander, Stamm, Vischer Daniel)
Abs. 1
... Post- und Fernmeldediensten angehören. Die Akteure bestimmen ihre Vertreterinnen und Vertreter eigenständig.

Art. 5
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Brand, Egloff, Nidegger, Rickli Natalie, Schwander, Stamm, Vischer Daniel)
Al. 1
... services postaux et de télécommunication. Ces différents acteurs choisissent eux-mêmes les personnes qui les représentent.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 120)
Für den Antrag der Mehrheit ... 118 Stimmen
Für den Antrag der Minderheit ... 61 Stimmen
(3 Enthaltungen)

Art. 6; 7; 8 Bst. a, c; 9; 10
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Art. 6; 7; 8 let. a, c; 9; 10
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 11
Antrag der Mehrheit
Abs. 1–5
Zustimmung zum Beschluss des Ständerates
Abs. 6
... Fristen zu gewährleisten ist ...

Antrag der Minderheit I
(Reimann Lukas, Brand, Egloff, Nidegger, Schwander, Stamm, Vischer Daniel)
Abs. 2
... längstens aber bis zehn Jahre nach Abschluss der Überwachung.

Antrag der Minderheit II
(Vischer Daniel, Brand, Egloff, Nidegger, Pardini, Reimann Lukas, Schwander)
Die Daten werden von Amtes wegen aus dem System gelöscht, sobald die Gründe für die entsprechende Überwachung weggefallen sind. Dies ist der Fall bei Abschluss der Fahndung, Einstellung der Untersuchung oder der Notsuche oder durch Erwachsen des Strafurteils in Rechtskraft.

Art. 11
Proposition de la majorité
Al. 1–5
Adhérer à la décision du Conseil des Etats
Al. 6
Adhérer à la décision du Conseil des Etats
(la modification ne concerne que le texte allemand)

Proposition de la minorité I
(Reimann Lukas, Brand, Egloff, Nidegger, Schwander, Stamm, Vischer Daniel)
Al. 2
... mais dix ans au plus depuis la fin de la surveillance.

Proposition de la minorité II
(Vischer Daniel, Brand, Egloff, Nidegger, Pardini, Reimann Lukas, Schwander)
Les données sont supprimées d'office du système dès qu'il n'y a plus de raison de poursuivre la surveillance. C'est le cas lors de la clôture de la recherche, lors de l'arrêt de l'enquête ou de la recherche en cas d'urgence ou lors de l'entrée en force du jugement.

Erste Abstimmung – Premier vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 121)
Für den Antrag der Mehrheit ... 112 Stimmen
Für den Antrag der Minderheit I ... 58 Stimmen
(14 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 122)
Für den Antrag der Mehrheit ... 112 Stimmen
Für den Antrag der Minderheit II ... 71 Stimmen
(1 Enthaltung)

Art. 12
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Schwaab, Brand, Egloff, Kiener Nellen, Nidegger, Pardini, Reimann Lukas, Rickli Natalie, Ruiz Rebecca, Schneider Schüttel, Schwander, Stamm)
Abs. 4
Werden dem Dienst Sicherheitslücken bekannt, so informiert er den Bundesrat, den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und die Öffentlichkeit.
Abs. 5
Bei erheblichen Sicherheitslücken ordnet der Bundesrat die Einstellung des Betriebes des betroffenen Verarbeitungssystems bis zur Behebung der Sicherheitslücken an.
Abs. 6
Die Einstufung und Behebung der Sicherheitslücke wird durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten begutachtet.

Art. 12
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Schwaab, Brand, Egloff, Kiener Nellen, Nidegger, Pardini, Reimann Lukas, Rickli Natalie, Ruiz Rebecca, Schneider Schüttel, Schwander, Stamm)
Al. 4
Si le service a connaissance de lacunes de sécurité, il en informe le Conseil fédéral, le préposé fédéral à la protection des données et à la transparence ainsi que le public.
Al. 5
En cas d'importantes lacunes de sécurité, le Conseil fédéral ordonne l'arrêt de l'exploitation du système de traitement des données concerné jusqu'à ce que ces lacunes soient comblées.
Al. 6
La classification et la correction des lacunes de sécurité sont contrôlées par le préposé fédéral à la protection des données et à la transparence.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 123)
Für den Antrag der Minderheit ... 90 Stimmen
Dagegen ... 90 Stimmen
(4 Enthaltungen)

Mit Stichentscheid des Präsidenten
wird der Antrag der Minderheit angenommen
Avec la voix prépondérante du président
la proposition de la minorité est adoptée

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 13–15
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 16
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Brand, Nidegger, Schwander, Stamm)
Bst. b
b. Ist die von der Behörde bzw. der Genehmigungsbehörde angeordnete Überwachung seiner Ansicht nach technisch ungeeignet, technisch nicht durchführbar, gehört sie nicht zu den im Gesetz und in den Ausführungsbestimmungen vorgesehenen Überwachungstypen oder ist sie mit unverhältnismässigem technischem Aufwand verbunden, so stellt er dies in einer Verfügung fest.

Art. 16
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Brand, Nidegger, Schwander, Stamm)
Let. b
b. S'il estime que la surveillance ordonnée par l'autorité, respectivement l'autorité d'approbation, est techniquement inappropriée, qu'elle n'est pas techniquement exécutable, qu'elle ne fait pas partie des types de surveillance prévus par la loi et les dispositions d'exécution ou que son exécution technique occasionnerait une charge disproportionnée, il le constate dans une décision.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 124)
Für den Antrag der Mehrheit ... 148 Stimmen
Für den Antrag der Minderheit ... 35 Stimmen
(0 Enthaltungen)

Art. 17, 18, 20
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 21
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Rickli Natalie, Brand, Egloff, Müri, Nidegger, Vischer Daniel)
Abs. 1
... über bestimmte Fernmeldedienste von bestimmten Teilnehmern:
a. Name, Vorname, Adresse und, falls bekannt, Geburtsdatum und Beruf ...
b. ... FMG), soweit verfügbar;
...
d. Streichen

Art. 21
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Rickli Natalie, Brand, Egloff, Müri, Nidegger, Vischer Daniel)
Al. 1
... sur des services déterminés fournis à des usagers précis:
a. le nom, le prénom, l'adresse et, si celles-ci sont connues, la date de naissance et la profession ...
b. ... LTC), pour autant qu'elles soient disponibles;
...
d. Biffer

Abs. 1 Einleitung, Bst. a – Al. 1 introduction, let. a

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 125)
Für den Antrag der Mehrheit ... 103 Stimmen
Für den Antrag der Minderheit ... 76 Stimmen
(5 Enthaltungen)

Abs. 1 Bst. b – Al. 1 let. b

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 136)
Für den Antrag der Mehrheit ... 103 Stimmen
Für den Antrag der Minderheit ... 68 Stimmen
(13 Enthaltungen)

Abs. 1 Bst. d – Al. 1 let. d

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 137)
Für den Antrag der Mehrheit ... 100 Stimmen
Für den Antrag der Minderheit ... 80 Stimmen
(4 Enthaltungen)

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Art. 22 Abs. 1, 2, 4
Antrag der Mehrheit
Abs. 1, 4
Zustimmung zum Beschluss des Ständerates
Abs. 2
... zum Zweck der Identifikation während der Dauer der Kundenbeziehung sowie während zwölf Monaten nach deren Beendigung bereithalten und liefern müssen. Sie müssen dem Dienst ...

Antrag der Minderheit I
(Rickli Natalie, Brand, Müri, Nidegger)
Abs. 4
Der Bundesrat kann Anbieter abgeleiteter Kommunikationsdienste, die Dienstleistungen von grosser wirtschaftlicher Bedeutung erbringen, verpflichten, alle oder ...

Antrag der Minderheit II
(Rickli Natalie, Brand, Müri, Nidegger)
Abs. 4
Streichen

Art. 22 al. 1, 2, 4
Proposition de la majorité
Al. 1, 4
Adhérer à la décision du Conseil des Etats
Al. 2
... de services de télécommunication doivent, durant toute la durée de la relation commerciale ainsi que douze mois après la fin de celle-ci, posséder et livrer aux fins de l'identification. Ils doivent également livrer ...

Proposition de la minorité I
(Rickli Natalie, Brand, Müri, Nidegger)
Al. 4
... d'une grande importance économique à posséder et fournir tout ou partie des indications ...

Proposition de la minorité II
(Rickli Natalie, Brand, Müri, Nidegger)
Al. 4
Biffer

Erste Abstimmung – Premier vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 126)
Für den Antrag der Mehrheit ... 129 Stimmen
Für den Antrag der Minderheit I ... 53 Stimmen
(2 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 127)
Für den Antrag der Mehrheit ... 131 Stimmen
Für den Antrag der Minderheit II ... 50 Stimmen
(2 Enthaltungen)

Art. 23
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Brand, Nidegger, Rickli Natalie)
Abs. 1
Streichen
Abs. 2
Der Bundesrat regelt ...
Abs. 3
... Uhr zu erfolgen hat. Er regelt die entsprechende Entschädigung.

Art. 23
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Brand, Nidegger, Rickli Natalie)
Al. 1
Biffer
Al. 2
Le Conseil fédéral règle ...
Al. 3
... et en tout temps. Il règle l'indemnité correspondante.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 128)
Für den Antrag der Mehrheit ... 137 Stimmen
Für den Antrag der Minderheit ... 47 Stimmen
(0 Enthaltungen)

Art. 24
Antrag der Kommission
... Überwachungsanordnung notwendigen technischen Informationen liefern.

Art. 24
Proposition de la commission
... les informations techniques nécessaires pour ordonner une surveillance.

Angenommen – Adopté

Art. 25
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 26 Abs. 6
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Rickli Natalie, Egloff, Leutenegger Oberholzer, Müri, Nidegger, Reimann Lukas, Vischer Daniel)
Der Bundesrat kann Anbieterinnen von Fernmeldediensten bezüglich Diensten von geringer Bedeutung für die Aufklärung strafbarer Handlungen sowie Anbieterinnen von Fernmeldediensten im Bildungsbereich von bestimmten gesetzlichen Verpflichtungen befreien. Er ...

Art. 26 al. 6
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Rickli Natalie, Egloff, Leutenegger Oberholzer, Müri, Nidegger, Reimann Lukas, Vischer Daniel)
Le Conseil fédéral peut dispenser de certaines obligations légales des fournisseurs de services de télécommunication pour ce qui est de services de faible importance pour élucider des infractions ainsi que des fournisseurs de services de télécommunication dans le domaine de l'éducation. Il ...

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 129)
Für den Antrag der Mehrheit ... 114 Stimmen
Für den Antrag der Minderheit ... 66 Stimmen
(3 Enthaltungen)

Art. 30, 31
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 32
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Schneider Schüttel, Schwaab, Vischer Daniel)
Abs. 2
... und alle geeigneten und in technischer und finanzieller Hinsicht verhältnismässigen Massnahmen ...

Art. 32
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Kiener Nellen, Leutenegger Oberholzer, Schneider Schüttel, Schwaab, Vischer Daniel)
Al. 2
... et prendre toute mesure utile et raisonnable sur les plans technique et financier pour ...

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 130)
Für den Antrag der Mehrheit ... 100 Stimmen
Für den Antrag der Minderheit ... 81 Stimmen
(3 Enthaltungen)

Art. 33–38
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 39 Abs. 1 Einleitung, Bst. a, c, d, 2, 3
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Reimann Lukas, Büchel Roland, Leutenegger Oberholzer, Nidegger, Schwander)
Abs. 1 Bst. a
a. ... an ihn gerichteten rechtskräftigen Verfügung ...

Art. 39 al. 1 introduction, let. a, c, d, 2, 3
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Reimann Lukas, Büchel Roland, Leutenegger Oberholzer, Nidegger, Schwander)
Al. 1 let. a
a. ... à une décision entrée en force à lui signifiée ...

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 131)
Für den Antrag der Mehrheit ... 120 Stimmen
Für den Antrag der Minderheit ... 63 Stimmen
(1 Enthaltung)

Art. 40, 41
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 42
Antrag der Mehrheit
Abs. 1, 3
Zustimmung zum Beschluss des Ständerates
Abs. 2
Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit
(Reimann Lukas, Büchel Roland, Leutenegger Oberholzer, Nidegger, Rickli Natalie, Schwander, Stamm, Vischer Daniel)
Abs. 3
Die Beschwerde hat aufschiebende Wirkung. Die Beschwerdeinstanz kann der Beschwerde die aufschiebende Wirkung entziehen.

Art. 42
Proposition de la majorité
Al. 1, 3
Adhérer à la décision du Conseil des Etats
Al. 2
Adhérer au projet du Conseil fédéral

Proposition de la minorité
(Reimann Lukas, Büchel Roland, Leutenegger Oberholzer, Nidegger, Rickli Natalie, Schwander, Stamm, Vischer Daniel)
Al. 3
Le recours a un effet suspensif. L'autorité de recours peut lui retirer l'effet suspensif.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 132)
Für den Antrag der Mehrheit ... 106 Stimmen
Für den Antrag der Minderheit ... 78 Stimmen
(0 Enthaltungen)

Art. 43, 44, 46
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

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

Ziff. II Ziff. 1 Art. 269 Abs. 2
Antrag der Mehrheit
Bst. a
... 192 Absatz 1, 195 bis 197 ...
Bst. k
k. Waffengesetz vom 20. Juni 1997: Artikel 33.

Antrag der Minderheit
(Vogler, Barazzone, Eichenberger, Guhl, Lüscher, Merlini, Rickli Natalie)
Bst. k
Zustimmung zum Beschluss des Ständerates

Ch. II ch. 1 art. 269 al. 2
Proposition de la majorité
Let. a
... 192 alinéa 1, 195 à 197 ...
Let. k
k. loi fédérale du 20 juin 1997 sur les armes: article 33.

Proposition de la minorité
(Vogler, Barazzone, Eichenberger, Guhl, Lüscher, Merlini, Rickli Natalie)
Let. k
Adhérer à la décision du Conseil des Etats

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 133)
Für den Antrag der Minderheit ... 119 Stimmen
Für den Antrag der Mehrheit ... 58 Stimmen
(7 Enthaltungen)

Übrige Bestimmungen angenommen
Les autres dispositions sont adoptées

Ziff. II Ziff. 1 Art. 270 Einleitung, Bst. b Ziff. 1; 271; 272 Abs. 2, 3; 278 Abs. 1bis
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. II ch. 1 art. 270 introduction, let. b ch. 1; 271; 272 al. 2, 3; 278 al. 1bis
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Ziff. II Ziff. 1 Art. 279
Antrag der Mehrheit
Abs. 3
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Schwander, Nidegger, Stamm)
Abs. 1
Die Staatsanwaltschaft teilt allen von der Überwachungsmassnahme betroffenen Personen, insbesondere auch solchen, die nicht selbst Ziel der Überwachung waren, spätestens mit Abschluss des Vorverfahrens Grund, Art, Dauer sowie Orte und Zeiten der Überwachung mit.
Abs. 1bis
Die Staatsanwaltschaft übergibt der betroffenen Person:
a. Kopien aller Personendaten der betreffenden Person aus der Überwachung;
b. Kopien aller von der betreffenden Person ausgehenden Kommunikationsinhalte aus der Überwachung.
Abs. 2
Die Mitteilung kann mit Zustimmung des Zwangsmassnahmengerichtes um maximal ein Jahr aufgeschoben werden, wenn dies zum Schutze überwiegender öffentlicher oder privater Interessen notwendig ist.
Abs. 3
Personen, die von der Überwachungsmassnahme betroffen sind oder waren, können Beschwerde nach den Artikeln 393 bis 397 führen ...

Ch. II ch. 1 art. 279
Proposition de la majorité
Al. 3
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Schwander, Nidegger, Stamm)
Al. 1
... communique aux personnes concernées par les mesures de surveillance, notamment celles qui ne font pas directement l'objet de cette surveillance, les motifs, le mode et la durée, le lieu et les horaires de la surveillance.
Al. 1bis
Le ministère public remet à la personne concernée:
a. des copies de toutes les données personnelles rassemblées sur la personne concernée au cours de la surveillance;
b. des copies du contenu de l'ensemble des communications émises par la personne concernée obtenues au cours de la surveillance.
Al. 2
... de différer la communication d'un an au plus, si la protection d'intérêts publics ou privés prépondérants l'exige.
Al. 3
Les personnes qui sont, ou ont été, concernées par les mesures de surveillance peuvent interjeter recours conformément aux articles 393 à 397 ...

Le président (Rossini Stéphane, président): Le vote vaut également pour le chiffre II chiffre 2 articles 70j et 70k.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 13.025/12 134)
Für den Antrag der Mehrheit ... 132 Stimmen
Für den Antrag der Minderheit ... 45 Stimmen
(5 Enthaltungen)

Ziff. II Ziff. 1 Art. 286 Abs. 2 Bst. i
Antrag der Kommission
i. Waffengesetz vom 20. Juni 1997: Artikel 33.

Ch. II ch. 1 art. 286 al. 2 let. i
Proposition de la commission
i. loi du 20 juin 1997 sur les armes: article 33.

Angenommen – Adopté

Ziff. II Ziff. 2 Art. 70a Einleitung, Bst. b Ziff. 1; 70b; 70c Abs. 2, 3
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. II ch. 2 art. 70a introduction, let. b ch. 1; 70b; 70c al. 2, 3
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Ziff. II Ziff. 2 Art. 70j
Antrag der Minderheit
(Schwander, Nidegger, Stamm)
Abs. 1
Der Untersuchungsrichter teilt allen von der Überwachungsmassnahme betroffenen Personen, insbesondere auch solchen, die nicht selbst Ziel der Überwachung waren, spätestens mit Abschluss des Vorverfahrens Grund, Art, Dauer sowie Orte und Zeiten der Überwachung mit.
Abs. 1bis
Der Untersuchungsrichter übergibt der betroffenen Person:
a. Kopien aller Personendaten der betreffenden Person aus der Überwachung;
b. Kopien aller von der betreffenden Person ausgehenden Kommunikationsinhalte aus der Überwachung.
Abs. 2
Die Mitteilung kann mit Zustimmung des Präsidenten des Militärkassationsgerichts um maximal ein Jahr aufgeschoben werden, wenn dies zum Schutze überwiegender öffentlicher oder privater Interessen notwendig ist.

Ch. II ch. 1 art. 70j
Proposition de la minorité
(Schwander, Nidegger, Stamm)
Al. 1
... communique aux personnes concernées par les mesures de surveillance, notamment celles qui ne font pas directement l'objet de cette surveillance, les motifs, le mode et la durée, le lieu et les horaires de la surveillance.
Al. 1bis
Le juge d'instruction remet à la personne concernée:
a. des copies de toutes les données personnelles rassemblées sur la personne concernée au cours de la surveillance;
b. des copies du contenu de l'ensemble des communications émises par la personne concernée obtenues au cours de la surveillance.
Al. 2
... de différer la communication d'un an au plus, si la protection d'intérêts publics ou privés prépondérants l'exige.

Le président (Rossini Stéphane, président): La proposition de la minorité Schwander a déjà été rejetée au chiffre II chiffre 1 article 279.

Ziff. II Ziff. 1 Art. 70k
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Schwander, Nidegger, Stamm)
Personen, die von der Überwachungsmassnahme betroffen sind oder waren, können innert zehn Tagen ...

Ch. II ch. 1 art. 70k
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Schwander, Nidegger, Stamm)
Les personnes qui sont, ou ont été, concernées par les mesures de surveillance peuvent interjeter recours ...

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. II Ziff. 3
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. II ch. 3
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Gesamtabstimmung – Vote sur l'ensemble
(namentlich – nominatif; Beilage – Annexe 13.025/12 135)
Für Annahme des Entwurfes ... 110 Stimmen
Dagegen ... 65 Stimmen
(9 Enthaltungen)

Abschreibung – Classement

Antrag des Bundesrates
Abschreiben der parlamentarischen Vorstösse gemäss Brief an die eidgenössischen Räte
Proposition du Conseil fédéral
Classer les interventions parlementaires selon lettre aux Chambres fédérales

Angenommen – Adopté

Schluss der Sitzung um 18.55 Uhr
La séance est levée à 18 h 55