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

CHRONOLOGIE

STÄNDERAT/CONSEIL DES ETATS 10.03.14 (ERSTRAT - PREMIER CONSEIL)
STÄNDERAT/CONSEIL DES ETATS 19.03.14 (FORTSETZUNG - SUITE)
NATIONALRAT/CONSEIL NATIONAL 17.06.15 (ZWEITRAT - DEUXIÈME CONSEIL)
NATIONALRAT/CONSEIL NATIONAL 17.06.15 (FORTSETZUNG - SUITE)
STÄNDERAT/CONSEIL DES ETATS 07.12.15 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 03.03.16 (DIFFERENZEN - DIVERGENCES)
STÄNDERAT/CONSEIL DES ETATS 08.03.16 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 14.03.16 (DIFFERENZEN - DIVERGENCES)
STÄNDERAT/CONSEIL DES ETATS 16.03.16 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 16.03.16 (DIFFERENZEN - DIVERGENCES)
NATIONALRAT/CONSEIL NATIONAL 18.03.16 (SCHLUSSABSTIMMUNG - VOTE FINAL)
STÄNDERAT/CONSEIL DES ETATS 18.03.16 (SCHLUSSABSTIMMUNG - VOTE FINAL)

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

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

AB 2015 N 1161 / BO 2015 N 1161

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; 13.025/12093)
Für den Antrag der Mehrheit ... 128 Stimmen
Für den Antrag der Minderheit ... 41 Stimmen
(15 Enthaltungen)

AB 2015 N 1163 / BO 2015 N 1163

Abs. 2 – Al. 2

Abstimmung – Vote
(namentlich – nominatif; 13.025/12094)
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; 13.025/12095)
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.

AB 2015 N 1164 / BO 2015 N 1164

Erste Abstimmung – Premier vote
(namentlich – nominatif; 13.025/12096)
Für den Antrag der Mehrheit ... 104 Stimmen
Für den Antrag der Minderheit I ... 80 Stimmen
(1 Enthaltung)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; 13.025/12097)
Für den Antrag der Mehrheit ... 106 Stimmen
Für den Antrag der Minderheit III ... 68 Stimmen
(11 Enthaltungen)

Dritte Abstimmung – Troisième vote
(namentlich – nominatif; 13.025/12098)
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; 13.025/12099)
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

AB 2015 N 1165 / BO 2015 N 1165

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; 13.025/12100)
Für den Antrag der Minderheit I ... 128 Stimmen
Für den Antrag der Minderheit II ... 49 Stimmen
(8 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; 13.025/12101)
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; 13.025/12102)
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; 13.025/12103)
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; 13.025/12104)
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; 13.025/12105)
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; 13.025/12106)
Für den Antrag der Mehrheit ... 127 Stimmen
Für den Antrag der Minderheit ... 43 Stimmen
(15 Enthaltungen)

AB 2015 N 1166 / BO 2015 N 1166

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

AB 2015 N 1167 / BO 2015 N 1167

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

AB 2015 N 1168 / BO 2015 N 1168

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

Arbeit 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

einem 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.

AB 2015 N 1171 / BO 2015 N 1171

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 Datenverarbeitungssy-

stem 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

AB 2015 N 1173 / BO 2015 N 1173

Risikogesellschaft. 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 Gov-

ware-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

AB 2015 N 1176 / BO 2015 N 1176

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

AB 2015 N 1177 / BO 2015 N 1177

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; 13.025/12107)
Für den Antrag der Mehrheit ... 121 Stimmen
Für den Antrag der Minderheit I ... 60 Stimmen
(0 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; 13.025/12108)
Für den Antrag der Mehrheit ... 119 Stimmen
Für den Antrag der Minderheit II ... 53 Stimmen
(9 Enthaltungen)

Dritte Abstimmung – Troisième vote
(namentlich – nominatif; 13.025/12109)
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; 13.025/12110)
Für den Antrag der Mehrheit ... 109 Stimmen
Für den Antrag der Minderheit ... 71 Stimmen
(1 Enthaltung)

Abs. 1bis – Al. 1bis

Abstimmung – Vote
(namentlich – nominatif; 13.025/12111)
Für den Antrag der Minderheit ... 54 Stimmen
Dagegen ... 125 Stimmen
(2 Enthaltungen)

Abs. 4 – Al. 4

Abstimmung – Vote
(namentlich – nominatif; 13.025/12112)
Für den Antrag der Mehrheit ... 127 Stimmen
Für den Antrag der Minderheit ... 52 Stimmen
(2 Enthaltungen)

Abs. 5 – Al. 5

Abstimmung – Vote

(namentlich – nominatif; 13.025/12113)
Für den Antrag der Minderheit ... 78 Stimmen
Dagegen ... 103 Stimmen
(0 Enthaltungen)

Abs. 6 – Al. 6

Abstimmung – Vote
(namentlich – nominatif; 13.025/12114)
Für den Antrag der Minderheit ... 41 Stimmen
Dagegen ... 131 Stimmen
(9 Enthaltungen)

Abs. 1–3 – Al. 1–3

Erste Abstimmung – Premier vote
(namentlich – nominatif; 13.025/12115)
Für den Antrag der Mehrheit ... 113 Stimmen
Für den Antrag der Minderheit I ... 64 Stimmen
(4 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; 13.025/12116)
Für den Antrag der Mehrheit ... 114 Stimmen
Für den Antrag der Minderheit II ... 66 Stimmen
(1 Enthaltung)

Dritte Abstimmung – Troisième vote
(namentlich – nominatif; 13.025/12117)
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.

AB 2015 N 1179 / BO 2015 N 1179

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; 13.025/12118)
Für den Antrag der Mehrheit ... 132 Stimmen
Für den Antrag der Minderheit ... 44 Stimmen
(5 Enthaltungen)

Abs. 6 – Al. 6

Abstimmung – Vote
(namentlich – nominatif; 13.025/12119)
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

AB 2015 N 1182 / BO 2015 N 1182

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

AB 2015 N 1184 / BO 2015 N 1184

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

innerhalb 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.

AB 2015 N 1186 / BO 2015 N 1186

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

AB 2015 N 1187 / BO 2015 N 1187

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 Bundes-

gerichtsentscheid 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

AB 2015 N 1189 / BO 2015 N 1189

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; 13.025/12120)
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; 13.025/12121)
Für den Antrag der Mehrheit ... 112 Stimmen

Für den Antrag der Minderheit I ... 58 Stimmen
(14 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; 13.025/12122)
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

AB 2015 N 1190 / BO 2015 N 1190

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; 13.025/12123)
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; 13.025/12124)
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; 13.025/12125)
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; 13.025/12136)
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; 13.025/12137)
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 ...

AB 2015 N 1191 / BO 2015 N 1191

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; 13.025/12126)
Für den Antrag der Mehrheit ... 129 Stimmen
Für den Antrag der Minderheit I ... 53 Stimmen
(2 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; 13.025/12127)
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; 13.025/12128)
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; 13.025/12129)
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

AB 2015 N 1192 / BO 2015 N 1192

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; 13.025/12130)
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; 13.025/12131)
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; 13.025/12132)
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; 13.025/12133)
Für den Antrag der Minderheit ... 119 Stimmen
Für den Antrag der Mehrheit ... 58 Stimmen
(7 Enthaltungen)

AB 2015 N 1193 / BO 2015 N 1193

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; 13.025/12134)
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 Militärkassationsgerichtes 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.

AB 2015 N 1194 / BO 2015 N 1194

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; 13.025/12135)
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

AB 2015 N 1195 / BO 2015 N 1195