13.025

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Änderung

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

Zweitrat – Deuxième Conseil

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)

Antrag der Mehrheit
Eintreten

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

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

Proposition de la majorité
Entrer en matière

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

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

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

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

Schwaab Jean Christophe (S, VD), pour la commission: Les télécommunications ont évolué. Les criminels s'en sont aperçus et font usage des nouveaux moyens de communication. Ils utilisent des logiciels ou des applications cryptées. Ils planifient leurs mauvais coups par consoles de jeu interconnectées. Et lorsqu'ils se savent écoutés, la dernière chose qu'entendront les forces de l'ordre, c'est "finissons cette conversations sur Skype, sur Facebook Messenger ou sur World of Warcraft", ou encore sur un autre service crypté.
Parfois, ils n'ont même pas besoin de changer d'appareil. Avec ce simple téléphone intelligent, que nous sommes bon nombre à posséder dans cette salle, il n'y a qu'à changer d'application, à appuyer sur le logo bleu doté d'un "S" ou sur le logo bleu arborant un "F" au lieu du logo vert orné d'un combiné téléphonique pour passer d'un mode que les autorités de poursuite pénale peuvent écouter à un autre qu'il est actuellement impossible de surveiller, à part peut-être la NSA, mais je m'écarte du sujet.
Il n'est d'ailleurs pas certain que je m'en écarte autant que cela, car l'exemple de ce que peut – enfin, pouvait et pourra certainement bientôt de nouveau – faire la NSA est révélateur de la mauvaise compréhension qu'ont certains de la loi sur la surveillance de la correspondance par poste et télécommunication révisée et de ses instruments. Jusqu'à il y a peu, en effet, la NSA récupérait les données secondaires de télécommunications de la totalité de la population des Etats-Unis, sans aucun contrôle, si ce n'est celui d'un pseudo-tribunal secret. Comme nous le verrons plus tard, la différence entre le droit en vigueur et la loi révisée est de taille: ni la loi actuelle, ni la future loi sur la surveillance de la correspondance par poste et télécommunication n'autorisent une autorité étatique à stocker des données secondaires de l'entier de la population. Personne d'ailleurs ne peut conserver, encore moins utiliser à des fins de surveillance, les données de toute la population. Lorsque l'Etat peut les obtenir, ce n'est pas à des fins de surveillance préventive de n'importe qui, mais c'est pour mener une surveillance d'une personne soupçonnée d'un délit important, sous le contrôle d'un tribunal.
J'en reviens aux objectifs de la loi qui nous est soumise aujourd'hui. Un des objectifs de la révision que nous traitons aujourd'hui est de donner aux autorités de poursuite pénale les moyens d'écouter ces télécommunications actuellement inaudibles et de pouvoir pour cela faire usage des instruments adéquats. Ces instruments font peur. Peut-être est-ce à cause de leurs noms barbares: IMSI-Catcher, Govware, chevaux de Troie, "Vorratsdatenspeicherung". Mais c'est surtout à cause des craintes légitimes qu'ils provoquent dans la population, craintes renforcées par les récentes affaires d'espionnage et de surveillance massive des télécommunications par des services secrets étrangers.
Il y a aussi des craintes – légitimes là aussi – que ces instruments perturbent les télécommunications, en particulier les services d'urgence, voire permettent de mener de véritables perquisitions en ligne, de falsifier des contenus et donc des preuves. Le danger est en effet réel que ces instruments soient utilisés à tort et à travers pour surveiller les communications d'honnêtes citoyens, ou de personnes vaguement soupçonnées d'avoir commis un délit mineur.
La commission s'est donc penchée avec beaucoup d'attention sur ce problème. Le projet du Conseil fédéral contenait déjà des garanties solides. La commission les a renforcées, pour ne pas dire bétonnées, en particulier en ce qui concerne les "programmes informatiques spéciaux", nom juridique des chevaux de Troie ou Govware.
Comme nous le verrons lors de la discussion par article, le cadre légal que vous propose la commission, qui a passé beaucoup de temps sur ce point en particulier, est extrêmement étroit et toujours guidé par les principes élémentaires suivant:
– la subsidiarité: l'instrument n'est utilisé que lorsque d'autres, moins invasifs, ont échoué;
– la proportionnalité: on ne s'en sert pas pour traquer la petite criminalité;
– l'autorisation par un juge: la police ne peut mettre en oeuvre une surveillance invasive de sa seule initiative;

– l'inexploitabilité des preuves obtenues en dehors du cadre légal: si l'instrument de surveillance sert à autre chose qu'à surveiller la communication autorisée, les règles habituelles de la procédure pénale en matière d'exploitation des preuves s'appliquent;
– l'établissement d'un procès-verbal et le contrôle de chaque étape de la surveillance, afin de pouvoir garantir le respect des principes précédemment énumérés.
La mise en oeuvre de ces principes est un point important de la révision, car il faut bien admettre que les moyens de surveillance proposés constituent une atteinte grave aux droits fondamentaux. Il est donc capital que cette atteinte se fasse dans le strict respect des conditions de l'article 36 de la Constitution fédérale. La commission y a veillé, et la majorité est convaincue qu'elle y est parvenue. Le Conseil fédéral avait placé la barre très haut en matière de respect des droits fondamentaux, la commission l'a mise encore plus haut.
Il y a d'autres points où la révision de la loi vise à adapter les instruments de poursuite pénale à l'évolution des technologies. Il doit être désormais possible d'identifier les utilisateurs de télécommunications qui se servent de moyens aussi banals que des cartes SIM à prépaiement ou des réseaux sans fil mis à la disposition du public. Il va sans dire que cette obligation d'identification doit respecter le principe de la proportionnalité et qu'il n'est pas question d'accabler les particuliers ou les petites entreprises avec les charges qu'entraîne la mise sur pied de la surveillance. Ceux qui sont trop petits pour fournir les données eux-mêmes seront uniquement obligés de tolérer la surveillance qui sera effectuée par les autorités. Cette obligation de collaborer est précisée et échelonnée en fonction de qui est obligé de collaborer et sous quelles conditions.
Mais il ne s'agit pas seulement de surveiller ceux qui commettent des crimes graves dans le monde réel. Il s'agit aussi de combattre la criminalité en ligne: pédophilie, sextorsion, hameçonnage, etc. Là aussi, les criminels savent faire usage des moyens qui échappent à nos autorités par manque de bases légales. Combattre ces délits exige souvent des procédures longues, car ils ont souvent des ramifications internationales. Le projet en tient compte, notamment au niveau de la durée de conservation des données secondaires.
La nouvelle loi précise également l'utilisation des nouvelles technologies en cas de recherche d'une personne disparue en dehors d'une procédure pénale. Il ne s'agit cependant pas de supprimer le droit de tout un chacun à "disparaître des écrans radars" sans donner de nouvelles, si bon lui semble. Il s'agit plutôt de pouvoir tout mettre en oeuvre, y compris une surveillance des télécommunications, pour retrouver une personne disparue dont il y a lieu de croire qu'elle court ou qu'elle fait courir un danger sérieux. La nouvelle loi permet par ailleurs de rechercher une personne qui

AB 2015 N 1141 / BO 2015 N 1141

doit effectuer une peine privative de liberté, mais qui a plutôt choisi de prendre la clé des champs.
Le projet de loi repose sur le principe de la neutralité technologique. Ses dispositions doivent s'appliquer quelle que soit la technologie appliquée. Nous sommes en effet à des lieues d'imaginer ou de pouvoir prédire l'évolution des technologies que les prochaines années, que dis-je, les prochains mois pourraient apporter. La télécommunication évolue en effet avec une célérité incroyable.
Moins de vingt ans après la fin du monopole public sur le téléphone, les acteurs qui sont aujourd'hui dominants – et leurs technologies – pourraient être remplacés demain par d'autres acteurs dont l'objectif premier n'est pas d'être un opérateur de télécommunication. Pensez à Facebook par exemple, à la base un réseau social, qui, outre le rachat de Whatsapp, développe désormais son propre instrument de communication instantanée. Evoquer le géant de Palo Alto me permet d'évoquer l'obligation de collaborer des entreprises étrangères. Bon nombre des opérateurs actuels et futurs ne sont en effet pas suisses et n'y ont ni siège, ni succursale. Comment donc leur faire appliquer les règles que nous vous proposons d'adopter aujourd'hui? Comment éviter l'écueil de la territorialité du droit?
Ce n'est pas facile. Je vous donne un exemple. Facebook, encore elle, clame partout qu'elle collabore avec les autorités de poursuite pénale de tous les pays. Mais voyons comment cela se passe en pratique. En pratique, Facebook collabore, mais exige pour cela une décision de justice; décision qu'il est souvent impossible d'obtenir si les conditions de l'entraide pénale internationale ne sont pas remplies. Le Tribunal fédéral vient de le rappeler. Dans ces conditions, si elles ne peuvent pas toujours compter sur la collaboration de ces nouveaux acteurs, nos autorités de poursuite pénale doivent pouvoir tout mettre en oeuvre, notamment les instruments qui permettent d'écouter des conversations en cas de soupçons de crimes graves, dans le respect des droits fondamentaux. C'est ce que permet la nouvelle loi. Et c'est aussi ce que contrôle la nouvelle loi.
La commission – cela a été dit par le rapporteur de langue allemande, Monsieur Flach – a fourni un travail conséquent. Nous nous sommes concentrés sur les aspects les plus controversés, dans notre conseil comme dans le grand public, que sont les données secondaires et les chevaux de Troie.
Nous nous sommes aussi penchés sur les développements judiciaires internationaux, notamment dans l'Union

Européenne, où la conservation des données secondaires donne lieu à un débat juridique et politique nourri qui, s'il est mal compris, peut faire naître quelques fantasmes à propos de la constitutionnalité de nos propres règles.
La commission vous propose d'entrer en matière, par 15 voix contre 6 et 1 abstention. Une minorité Vischer Daniel vous demande de ne pas entrer en matière, ce qui est un peu contradictoire, car une autre minorité Vischer Daniel – la minorité IV, à l'article 19 alinéa 4 – propose de biffer la disposition qui prévoit de conserver les données secondaires, ce qui ne sera pas possible si nous n'entrons pas en matière aujourd'hui. En effet, la loi actuelle permet la conservation des données secondaires.
Une autre minorité Vischer Daniel propose de renvoyer le projet au Conseil fédéral. La commission a rejeté cette proposition, par 16 voix contre 6 et 3 abstentions, car elle trouve absurde de faire deux fois un travail que le Parlement peut faire lui-même à l'occasion du débat sur les données secondaires. La commission a déjà fait ce travail et la minorité s'est d'ailleurs ralliée à ce résultat, mais j'aurai l'occasion d'y revenir.
Au vote sur l'ensemble, la commission a soutenu le projet tel qu'elle l'a modifié et le présente aujourd'hui, par 15 contre 6 et 1 abstention. Je vous remercie d'en faire autant.

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

Le président (Rossini Stéphane, président): Vous l'avez entendu, la proposition de non-entrée en matière de

la minorité Vischer Daniel a été retirée.

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

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

Guhl Bernhard (BD, AG): Das Ziel der Revision ist es, ganz kurz gesagt, die Überwachungsmöglichkeiten der Strafverfolgungsbehörden an die neuen technischen Gegebenheiten anzupassen. Die BDP-Fraktion ist

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

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

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

Concernant la proposition de renvoi: celle-ci n'est pas nécessaire, car les critiques faites par les auteurs sont déjà présentées dans les différentes propositions soumises au conseil. De plus, la proposition de renvoi prévoit de limiter l'utilisation des Govware, ce qui réduirait drastiquement la possibilité de surveiller les trafiquants de drogue ou les réseaux du crime organisé par exemple. Ce n'est pas acceptable.
La majorité du groupe vert'libéral entrera en matière sur ce projet.

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

Vogler Karl (CE, OW): Sie haben es gehört: Unser Rat behandelt als Zweitrat die Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs und die in diesem Zusammenhang gleichsam notwendige Revision der Schweizerischen Strafprozessordnung und des Militärstrafprozesses.
Die Totalrevision des Büpf soll die Voraussetzungen dafür schaffen, dass der Post- und Fernmeldeverkehr, wenn der dringende Verdacht auf Begehung einer schweren Straftat besteht, zum Zwecke der Strafverfolgung

besser – nicht mehr, aber besser – überwacht werden kann. Es geht darum, das Gesetz an die enormen technologischen Fortschritte der letzten Jahre anzupassen und damit eine effiziente Strafverfolgung zu gewährleisten. Anders gesagt: Der Gesetzgeber soll im Bereich der Strafverfolgung durch die rasanten technologischen Fortschritte nicht überholt werden.
Um es klarzustellen – es wurde bereits gesagt -: Bei der Revision des Büpf geht es nicht um eine flächendeckende präventive Überwachung der Bürgerinnen und Bürger oder um nachrichtendienstliche Tätigkeiten; es geht vielmehr um die Sicherstellung einer effizienten Kriminalitätsbekämpfung bei schweren und schwersten Delikten, beispielsweise im Bereich der organisierten Kriminalität, bei Kinderpornografie, bei Tötungs- oder schweren Vermögensdelikten.
Was macht dieses Geschäft, auch aus Sicht unserer Fraktion, schwierig und damit letztlich auch umstritten? Es sind dies gegenläufige Interessen, Spannungsfelder, die man nicht einfach auflösen kann, nämlich der legitime Schutz der Grundrechte, das heisst der Persönlichkeitsrechte auf der einen Seite und das öffentliche Interesse an einer wirksamen Kriminalitätsbekämpfung auf der anderen Seite. Diese

Interessen wiederum kollidieren mit den Interessen der Provider, die ihr Geschäftsmodell möglichst ungehindert, ohne weitere Kostenfolgen kommerziell anbieten wollen. In diesem mehrfachen Spannungsfeld befinden wir uns. Es gilt einen Weg zu finden, der es ermöglicht, im Rahmen des Gesetzmässigkeits- und Verhältnismässigkeitsprinzips gerade so viel wie nötig, aber so wenig wie möglich in die Grundrechte, aber auch in die Interessen der Fernmeldedienste einzugreifen.
Die Revision verläuft damit auch auf einem schmalen Grat zwischen dem, was technisch möglich ist, und dem, was rechtlich zulässig sein soll. Gerade der Einsatz der sogenannten Govware bzw. von Staatstrojanern macht den Konflikt deutlich: Nicht alles, was technisch möglich ist, soll rechtlich auch zulässig sein, und nicht alles, was rechtlich zulässig ist, ist technisch ohne Weiteres umsetzbar.
Ich habe es gesagt: Das vorliegende Geschäft betrifft die Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs sowie gleichzeitig die Revision der Strafprozessordnung und des Militärstrafprozesses.
Was sind die wichtigsten Änderungen? Das Büpf erweitert den persönlichen Geltungsbereich erheblich. Neu umfasst der Kreis der Mitwirkungspflichtigen sechs Kategorien mit entsprechenden, im Sinne der Verhältnismässigkeit klar definierten Pflichten, seien diese aktiver oder passiver Art. Das Büpf regelt weiter die Aufbewahrung der Daten und sieht eine Ausdehnung der Aufbewahrungspflicht von sechs auf zwölf Monate für die Randdaten vor. Geregelt werden schliesslich die Rechtsmittel gegen Verfügungen des Überwachungsdienstes. Das Büpf enthält ausserhalb des Strafverfahrens Bestimmungen betreffend die Notsuche für vermisste Personen und die Fahndung nach verurteilten Personen.
Mit den Änderungen in der Strafprozessordnung wird geregelt, unter welchen Voraussetzungen welche Überwachungsmassnahmen angeordnet werden können. Vorausgesetzt sind dabei ein dringender Verdacht und das Vorliegen eines schweren Delikts. Zudem müssen die bisherigen Untersuchungshandlungen erfolglos geblieben oder die Ermittlungen sonst aussichtslos sein, und schliesslich müssen diese Massnahmen durch das Zwangsmassnahmengericht genehmigt werden.
Umstritten ist dabei insbesondere auch die sogenannte Govware, landläufig unter dem Begriff "Staatstrojaner" bekannt. Unter strengen Voraussetzungen sollen damit verschlüsselte Daten mittels Einschleusen von besonderen Informatikprogrammen abgefangen werden. In diesem Kontext ist auch die gesetzliche Grundlage für den Einsatz der sogenannten Imsi-Catcher zu nennen, mit denen Gespräche mitgehört oder aufgenommen werden können.
Ich habe es eingangs gesagt: Wir bewegen uns in diesem Gesetz im Spannungsfeld verschiedener und entgegengesetzter Interessen, und mögliche Missbräuche können nicht ausgeschlossen werden. Allein deswegen die gesetzlichen Grundlagen für eine effektive und effiziente Strafverfolgung nicht zu schaffen und damit das Feld für die Kriminalität weiter zu öffnen wäre nicht zu verantworten.
Zusammengefasst lässt sich sagen, dass die Vorlage den sich ständig verändernden Bedürfnissen der Strafverfolgung Rechnung trägt. Sie beachtet die grundrechtlichen Anforderungen und schafft eine saubere gesetzliche Grundlage für notwendige Ermittlungen im Post- und Fernmeldeverkehr. Die CVP/EVP-Fraktion ist klar für Eintreten auf die Vorlage.
Erlauben Sie mir noch zwei, drei Hinweise zum Antrag auf Rückweisung. Natürlich ist es so – ich habe es gesagt –, dass das Gesetz Missbräuche nicht völlig ausschliessen kann. Das kann übrigens kein Gesetz. Die von Herrn Vischer geäusserten Bedenken können nicht einfach in den Wind geschlagen werden, aber es gilt eine Interessenabwägung zwischen möglichen Missbräuchen und dem öffentlichen Interesse an einer

zeitgemässen Kriminalitätsbekämpfung vorzunehmen. Bei einer entsprechenden Abwägung dieser Interessen überwiegt für uns klar das letztere. Kriminalität ist allgegenwärtig, und wir müssen den Strafverfolgungsbehörden die notwendigen Instrumente für eine wirksame Strafverfolgung in die Hand geben. Das entspricht auch rechtsstaatlicher Notwendigkeit.
Der Rückweisungsantrag beinhaltet vier Forderungen, nämlich erstens keine Vorratsdatenspeicherung, zweitens die Einschränkung des Katalogs der Straftaten für Govware und Imsi-Catcher, drittens die Beschränkung der Verwendung von Informationen, die so erlangt wurden, auf die Strafverfolgung, und viertens verlangt dieser Rückweisungsantrag Sicherheitsmassnahmen, damit die Govware auf die Live-Kommunikation beschränkt ist. Ohne im Detail auf diese Forderungen einzugehen, halte ich Folgendes fest: Würde man diesen Forderungen stattgeben, so würde man, was die ersten beiden Forderungen betrifft, die Möglichkeit der Kriminalitätsbekämpfung deutlich einschränken. Das wollen wir, wie gesagt, nicht. Was die dritte Forderung betrifft, so würde diese zu stossenden Ergebnissen führen. Beispielsweise dürfte man diese Methode bei der Fahndung nach einem flüchtigen Gefangenen nicht anwenden, weil es sich dabei nicht um eine Ermittlung, sondern um eine Fahndung handelt. Und würde man der vierten Forderung stattgeben, so hiesse das, dass damit auch die Erhebung von Randdaten ausgeschlossen würde. Diese Forderungen gehen zu weit. Wir lehnen sie ab.
Zusammengefasst: Ich ersuche Sie, auf die im Gesamten ausgewogene Vorlage einzutreten, und ich ersuche Sie um Ablehnung des Rückweisungsantrages.

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

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

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

einmal ausführen?

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

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

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

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

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

AB 2015 N 1146 / BO 2015 N 1146

Es ist für den normalen Bürger und die normale Bürgerin wahrscheinlich kaum verständlich, aber es ist tatsächlich so: Unser Gesetz erlaubt es der Strafverfolgungsbehörde nicht, die modernen Telekommunikationsmittel zu überwachen. Wenn ich also als Strafrechtsprofessor nicht unbescholtene Studierende unterrichten, sondern ein Seminar für Kriminelle machen würde, dann wäre das für mich ein ganz zentraler Themenblock: ihnen zu erklären, wie sie untereinander kommunizieren können, ohne dass die Strafverfolgungsbehörde sie überwachen kann. Das ist ein Missstand, bei dem wir unbedingt Abhilfe schaffen müssen. Deshalb sind wir heute hier und beraten über dieses Gesetz.
Nun wird uns vorgegaukelt – Sie haben es gehört –, es gehe um die Verteidigung gegenüber dem Überwachungsstaat. Mit diesem Gesetz werde der unbescholtene Bürger überwacht, und es finde eine präventive Überwachung statt. Das ist definitiv nicht so. Es geht hier einzig und allein um die Überwachung im Rahmen der Strafverfolgung. Damit also eine entsprechende Überwachung stattfinden kann, muss zuerst einmal ein Tatverdacht vorliegen, und es muss ein Strafverfahren eröffnet sein; es muss geprüft werden, ob ein Delikt vorliegt, das so schwer wiegt, dass die Überwachung stattfinden kann, und es muss eine entsprechende Bewilligung vorliegen, damit sie durchgeführt werden kann. Nur wenn das alles gegeben ist, nur dann kann die Überwachung stattfinden. Das heisst, es besteht keine Gefahr, dass der unbescholtene Bürger überwacht wird. Es besteht keine Gefahr, dass Leute ausserhalb des Strafverfahrens zu präventiven Zwecken überwacht werden.
Die Ironie respektive das Erstaunliche besteht darin – darauf hat selbst Herr Vischer vorher hingewiesen -: Die ganze Grundrechtsdebatte, die wir hier führen, hätten wir vor kurzer Zeit, als wir das Nachrichtendienstgesetz beraten haben, tatsächlich führen können; denn gemäss Nachrichtendienstgesetz findet die Überwachung im präventiven Bereich statt. Hier aber geht es nur um die Überwachung in Rahmen von Strafverfahren.
Man kann im politischen Prozess ja verschiedener Ansicht sein. Sie können, wie das beispielsweise Herr Vischer macht oder Herr Reimann macht oder Herr Schwander macht, grundsätzlich dagegen sein und konsequenterweise das Nachrichtendienstgesetz und das Büpf ablehnen. Sie können konsequenterweise dafür sein, wie es andere sind. Was Sie aber nicht machen können, ist, das Nachrichtendienstgesetz unterstützen und das Büpf ablehnen – das macht definitiv keinen Sinn!
Und wenn ich schaue, wer diese Position offenbar einnimmt, dann muss ich sagen – und da schaue ich zur SVP-Fraktion -: Es hat offenbar mit dem zuständigen Bundesrat zu tun, dass Sie im einen Fall zustimmen und in diesem Fall jetzt ablehnen wollen. Das ist aber weiss Gott kein Grund, ein Gesetz abzulehnen! Oder es hat damit zu tun, dass Sie der Telekommunikationsbranche nahestehen, die das Gesetz nicht will.
Deshalb ersuche ich Sie, einzutreten – das scheint unbestritten zu sein – und den Rückweisungsantrag der Minderheit Vischer Daniel abzulehnen.

Reimann Lukas (V, SG): Herr Kollege Jositsch, Sie haben bei der Debatte über das Nachrichtendienstgesetz

gehört, dass es dort um weniger als zehn Fälle pro Jahr geht. Um wie viele Fälle pro Jahr geht es beim Büpf?

Jositsch Daniel (S, ZH): Es geht beim Büpf um wesentlich mehr Fälle, und der Grund ist evident. Wir haben Gott sei Dank in unserem Land weniger Terrorverdächtige als Leute, die sich einer strafbaren Handlung verdächtig gemacht haben. Ich nehme an, Sie wollen mit Ihrer Frage darauf hinweisen, dass diese Vorlage aufgrund der Zahl der Überwachungen nun wesentlich wichtiger sei. Wichtiger ist sie, weil wir uns natürlich in allererster Linie mit dem Strafverfahren auseinandersetzen müssen. Nichtsdestotrotz ist aber der Unterschied evident, und deshalb ist es wichtig, dass Sie mir die Gelegenheit geben, das noch einmal kurz zu erläutern.
Im Nachrichtendienstgesetz geht es um den präventiven Bereich, und deshalb muss man wesentlich einschränkender sein. Deshalb haben wir im Nachrichtendienstgesetz auch sehr viel mehr Hürden eingebaut. Hier aber haben wir mit dem Strafverfahren einen wesentlichen Bereich, in dem wir aber grundsätzlich die Hürde haben, dass die Überwachung im Rahmen eines laufenden Strafverfahrens erfolgen muss; ausserhalb eines Strafverfahrens bestehen diese Überwachungsmöglichkeiten im Rahmen des Büpf nicht.

Leutenegger Oberholzer Susanne (S, BL): Ich spreche für eine knappe Mehrheit der SP-Fraktion, die für die Rückweisung dieser Vorlage ist, und zwar aus grundrechtlichen Überlegungen. Wir sind klar der Meinung, dass auch im Namen der Strafverfolgung bzw. der Sicherheit nicht jeder Grundrechtseingriff gerechtfertigt werden kann. Die Vorratsdatenspeicherung ist ein Grundrechtseingriff. Was hier so harmlos daherkommt, ist in der Realität ein Archiv unserer gesamten Telefon- und Internetkommunikation der letzten Monate oder des letzten Jahres. Wer meint, erst der Zugriff auf die Inhalte sei ein Grundrechtseingriff, der liegt falsch. Bereits die Sammlung dieser Daten ist ein Eingriff in die Grundrechte, zumal die Sammlung ohne Verdacht auf eine strafbare Handlung erfolgt. Das ist ein Verstoss gegen die persönliche Freiheit, verletzt den Schutz des privaten Familienlebens und insbesondere das informationelle Selbstbestimmungsrecht. Wir haben diese Debatte eigentlich erst nach dem Urteil des Europäischen Gerichtshofes vom 8. April 2014 geführt. Interessanterweise haben wir sie aber nicht à fond geführt. Die Dimension der geplanten Datensammlung übersteigt die seinerzeitige Fichenaffäre bei Weitem. Damals wurden 900 000 Bürgerinnen und Bürger fichiert. Ich wurde ebenfalls fichiert und habe meine Fiche im Hinblick auf diese Debatte noch einmal angeschaut. Da wurden auch nur Rahmendaten erfasst: Mit wem habe ich telefoniert, wohin bin ich gegangen. Nicht erfasst war der Inhalt der Kommunikation.
Bei der Speicherung der Rahmendaten geht es um Milliarden von Kommunikationen, um die Verbindungen von weit über 10 Millionen Kommunikationseinheiten. Stellen Sie sich vor, wie viele Handys, wie viele Festnetzverbindungen, wie viele Computer wir haben. Alle Verbindungen über diese Geräte werden erfasst. Rechtlich braucht es für jeden Grundrechtseingriff eine Rechtsgüterabwägung, eine Rechtfertigung; darin sind sich nicht nur die Juristen einig, sondern auch alle Bürgerinnen und Bürger. Zu prüfen sind dabei nicht nur die Gesetzmässigkeit und die Wahrung des Grundgehalts, sondern auch die Verhältnismässigkeit: absolut und in Bezug auf die Ziel-Mittel-Relation und das öffentliche Interesse.
Ich möchte mich nicht zur Wahrung des Grundgehalts äussern, aber zum öffentlichen Interesse und zur Verhältnismässigkeit. Es wurde behauptet, wir bräuchten das; Frau Chevalley, Frau Huber und Herr Vogler haben das betont. Das Max-Planck-Institut kommt in einer Untersuchung aus dem Jahr 2011 klar zum gegenteiligen Schluss.
Ich möchte Ihnen nahelegen, eine Plausibilitätsüberlegung zu machen. Die Wahrscheinlichkeit, aufgrund der weit über 10 Millionen – wahrscheinlich sind es 20 Millionen – erfassten Kommunikationseinheiten einen Straftäter zu finden, liegt im Promillebereich. Heute werden 5000 bis 6000 solcher Kommunikationseinheiten für ein Strafverfahren angefordert. Wenn Sie es hochrechnen: Sie haben insgesamt vielleicht 10 bis 20 Millionen Kommunikationseinheiten, 5000 bis 6000 davon werden inhaltlich überprüft. Sie können sich ausrechnen, dass das im Promillebereich liegt. Das belegt doch ganz klar: Das öffentliche Interesse an dieser massiven Verletzung der Grundrechte bzw. die Verhältnismässigkeit ist zu verneinen. Das Verfahren kostet sehr viel Geld – das Geld zu verbrennen wäre wahrscheinlich effizienter als diese flächendeckende Fichierung unserer Bürgerinnen und Bürger.
Ich komme noch kurz auf die Staatstrojaner zu sprechen. Es ist interessant, wie sich die Diskussion in der Kommission entwickelt hat. Ich verweise nochmals auf das

Grundsätzliche. Wir haben immer noch keine befriedigende Antwort auf die Frage, was mit dem Einsatz von Govware verändert werden kann und wer den Einsatz kontrolliert. Für mich entscheidend ist: Die Staatstrojaner können eingeschleust werden, sie können Programme zerstören, sie können Computersysteme zerstören. In der Botschaft des Bundesrates wird auf Seite 2775 vermerkt: "Aus Sicht der kontaktierten Fachleute aus

dem wissenschaftlichen Bereich ist es jedoch nicht möglich, Govware zu entwickeln und in Betrieb zu halten, die unter allen Umständen korrekt funktioniert, d. h. keinen Einfluss auf andere Programme oder Funktionen hat." Das wäre vielleicht auch meine Antwort an Herrn Naef. Auch in der Kommission konnten wir diese Frage nicht klären, trotz aller Abklärungen.
Zum Schluss: Es stellt sich doch auch beim Büpf ganz grundsätzlich die Frage, ob beim Staat der Einsatz aller Überwachungsmittel geheiligt werden kann. Unter dem Siegel der Verfolgung von kriminellen Straftaten könnte man alles bewilligen. Jede und jeder im Saal muss eine Rechtsgüterabwägung vornehmen. Ich bitte Sie um eines: Sorgen Sie mit dem gesunden Menschenverstand für eine Rückweisung des Gesetzes. Helfen Sie mit, die Kommunikationsüberwachung auf ein rechtsstaatlich vertretbares Mass zurückzustutzen. Dazu gehört auch eine Überprüfung der geltenden Praxis der Rahmendatenspeicherung; deswegen ist auch die Rückweisung wichtig. Die Rahmendatenspeicherung ist nämlich in Bezug auf die Grundrechtsfrage bislang noch nicht überprüft worden, vor allem nicht von unserem Parlament.
Ich danke Ihnen für die Rückweisung.

Reimann Lukas (V, SG): Ich nehme es vorweg: Die SVP-Fraktion beschloss mit einer Zweidrittelmehrheit, mit 22 zu 11 Stimmen, die Rückweisung dieses Geschäftes zu unterstützen. Der liberale Freiheitsdenker Roland Baader schrieb in seinem bemerkenswerten Buch "Freiheitsfunken": "Das einzig wahre Menschenrecht ist das Recht, in Ruhe gelassen zu werden – von jedem, den man nicht eingeladen hat oder den man nicht willkommen heisst." Genau über dieses Recht debattieren wir heute. Es geht heute nicht darum, ob ein Terrorist überwacht wird oder nicht, sondern es geht darum, ob Sie alle überwacht werden oder nicht. Es geht darum, auch wenn heute das Gegenteil behauptet wurde, ob unbescholtene Bürger bespitzelt werden oder nicht. Nur darum geht es, wenn auf Vorrat alle Daten von allen Bürgern erhoben werden. Zudem gibt es immer wieder Menschen, die über Jahre bespitzelt und beschattet wurden und die am Schluss unschuldig waren und freigesprochen wurden. Denken wir nur an den Fall Holenweger.
Der Staat hat kein Recht, welches die Bürger nicht auch gegenüber dem Staat hätten. Lässt sich der Staat überwachen? Nein! Die Verwaltung beschliesst in Hinterzimmern, der Bundesrat ebenso. Der Staat soll doch die Bürger schützen und sie nicht allgemein verurteilen. Was ist das eigentlich für ein negatives Menschenbild, das hier gepflegt wird? Was ist das für ein Rechtsverständnis, das die Menschen kriminalisiert, bevor sie schuldig gesprochen wurden? Dieses enorme Misstrauen gegenüber den Bürgern seitens des Staates ist absolut unschweizerisch. "Einen Staat, der mit der Erklärung, er wolle Straftaten verhindern, seine Bürger ständig überwacht, kann man als Polizeistaat bezeichnen." Dies sagte Ernst Benda, der ehemalige Präsident des Bundesverfassungsgerichtes. Ja, heute entscheiden wir tatsächlich, ob die Schweiz weiterhin ein Land der Freiheit und der Bürgerrechte sein will oder ob sie zu einem Polizei- und Überwachungsstaat verkommt.
Was sind die Kennzeichen eines Überwachungsstaates? Im Überwachungsstaat sollen die Erkenntnisse aus der Überwachung laut ihren Fürsprechern hauptsächlich zur Verhinderung und Ahndung von Gesetzesverstössen verwendet werden. Die Prävention von Straftaten und anderen unliebsamen Verhaltensweisen der Bürger findet im Überwachungsstaat durch einen hohen Überwachungsdruck statt. In diversen überwachenden Staaten waren bzw. sind präventive Festnahmen überwachter Personen vor Veranstaltungen üblich, um das öffentliche Erscheinungsbild der Veranstaltung zu beeinflussen. Der Überwachungsstaat zeichnet sich durch die Einschränkung des Datenschutzes, der Privatsphäre und der informationellen Selbstbestimmung aus.
Als Beispiele für rechtliche Massnahmen eines Überwachungsstaates werden immer wieder Telekommunikationsüberwachung und Vorratsdatenspeicherung genannt. Es war nie das Schweizer Staatsverständnis, dass man alle Bürger überwacht. Der Bürger in der Schweiz ist Kunde, und der Staat handelt im Interesse der Bürger, nicht gegen die Interessen der Bürger. Der Bürger ist nicht der Untertan, den man überwachen kann, wie man will. Frei sein und frei bleiben, das ist die Tugend, die in der Schweiz gilt und der Schweiz über Jahrhunderte Erfolg gebracht hat.
Was ich heute wieder gehört habe und nicht mehr hören kann: Wer nichts zu verbergen hat, der kann ja die Rechte zum Schutz der Privatsphäre aufgeben. Ja, und wer nichts zu sagen hat, kann auch das Recht auf freie Meinungsäusserung aufgeben – das wäre etwa gleich dumm.
Worum geht es bei der Revision des Büpf? Das Büpf sieht eine massive Ausweitung der staatlichen Überwachung vor: die Speicherung von personenbezogenen Daten aller unbescholtenen Bürger auf Vorrat, rückwirkend auf zwölf Monate; die Speicherung sämtlicher Verbindungsdaten Ihrer Telefonate und E-Mails ohne – ohne! – irgendeinen Verdacht; das Einschleusen von Programmen auf Ihre Computer, sogenannte Staatstrojaner, um unbemerkt Inhalte, Bilder, Texte, Aussagen mit- oder auszulesen sowie Ihre Kamera zu steuern, vorläufig nur im Verdachtsfall.

Kommen wir zum Kosten-Nutzen-Verhältnis: Derart weitgehende Eingriffe sollten doch mehr Nutzen als Kosten mit sich bringen. Sie wissen, dass die Revision des Büpf Millionen von Franken kostet. Zu beachten ist dabei, dass jede Datensammlung im Ausmass mehrerer Petabytes Kosten verursacht, welche schlussendlich auf die Allgemeinheit überwälzt werden. Die betroffenen Provider werden ihre Telekommunikations- und Internetangebote entsprechend verteuern, der Konsument zahlt mehr. Bereits heute müssen Provider die Verbindungsdaten der letzten sechs Monate speichern und sie den Ermittlungsbehörden auf richterlichen Beschluss hin übergeben; es stehen also bereits ausreichend Daten zur Verfügung. Im Berichtsjahr 2014 betrafen gerade einmal 0,8 Prozent der durch das Büpf erlaubten Anfragen Terrorverdachtsfälle – in jedem Votum hörte ich heute das Wort "Terror" –, und nur bei 41 von 10 000 überwachten Personen ging es um Kinderpornografie.
Die Ausweitung der Vorratsdatenspeicherung auf zwölf Monate bietet keinen Mehrwert. Das zeigt ganz klar auch die Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Sie verglich nämlich die Aufklärungsquoten von Staaten mit Vorratsdatenspeicherung und von Staaten ohne Vorratsdatenspeicherung. Es ist schlicht kein Mehrwert zu erkennen. Die Programmierung von Staatstrojanern wird ebenfalls Millionen verschlingen. Dort, wo effektiv Investitionen nötig wären, nämlich beim Personal, das die Daten auswertet, und bei den Auswertungstools für diese riesigen Datenmengen, werden mit Sicherheit noch weitere Kosten für Personal und Infrastruktur anfallen. Es käme am Schluss zu einem Kontroll- und Freiheitsverlust ohne Mehrwert.
Die Privatsphäre ist ein Grundrecht jedes Bürgers in einer Demokratie. Die elektronische Datensammlung birgt weit grössere Risiken als einst die Fichensammlung. Es ist eine grosse Datensammlung, es ist wie bei Schleppnetzfängen. Zahlreiche Informationen, die beispielsweise für fremde Geheimdienste, kommerzielle oder politische Zwecke ausgeschlachtet werden könnten, fallen an. Es stellt sich die Frage: Wer überwacht denn die Datensammler und die Datenauswerter? Und wer stellt sicher, dass der möglicherweise im Ausland programmierte Staatstrojaner nicht zum Vollstreckungsgehilfen anderer Nationen wird? Schon heute gibt es klare Anzeichen dafür, dass auch ausländische Geheim- und Nachrichtendienste auf die in der Schweiz auf Vorrat gespeicherten Daten Zugriff haben.

AB 2015 N 1148 / BO 2015 N 1148

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

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

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

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

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

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

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

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

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

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

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

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

Reimann Lukas (V, SG): Es ist genauso ein Widerspruch, wenn Sie das Nachrichtendienstgesetz ablehnen,

hingegen dem Büpf zustimmen. Die Gesetze hängen ja in verschiedenen Bereichen zusammen. Der Nachrichtendienst kriegt auch Zugriff auf die Daten, die durch das Büpf erhoben werden. Es gibt aber einen grossen Unterschied zwischen dem Nachrichtendienstgesetz und dem Büpf, und zwar ist das die Anzahl der Fälle. Wir sprechen beim Büpf von mehreren zehntausend Fällen, während wir beim

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

Sommaruga Simonetta, Bundespräsidentin: Was schlägt Ihnen der Bundesrat mit dieser Vorlage eigentlich ganz genau vor? Es sind im Wesentlichen zwei Neuerungen: Erstens geht es darum, die Randdatenspeicherung, die es heute schon gibt, von sechs Monaten auf zwölf Monate zu erhöhen. Zweitens geht es darum, dass wir die rechtlichen Grundlagen dafür schaffen, dass wir Kommunikation, die verschlüsselt ist, ebenfalls überwachen können – überwachen können in dem Fall, in dem es einen konkreten Verdacht auf eine schwere Straftat gibt. Ist das eine massive Ausweitung der Überwachung?
Herr Nationalrat Reimann hat es gesagt: Jeder Schwerkriminelle wird seine Daten verschlüsseln. Ja, das ist so. Die Polizei hat mir erzählt, wie das heute am Telefon tönt. Schwerkriminelle sagen: "Wir wechseln jetzt auf Skype, denn da kann man uns nicht überwachen." So einfach ist das. Jetzt gibt es Kräfte in diesem Parlament, die sagen: "Dann lassen wir den Schwerkriminellen diesen geschützten Raum, damit sie in Ruhe kommunizieren können und keine Angst haben müssen, dass sie überwacht werden können, wenn sie verschlüsselt kommunizieren."
Es geht also bei dieser Vorlage in erster Linie darum, dass wir die Mittel, die es in der Kommunikation gibt und die wir alle brauchen, die wir alle auch geniessen, für die Strafverfolgung im Falle von schwerer Kriminalität so anpassen, dass sie adäquat sind und mit den technologischen Entwicklungen übereinstimmen. Wir reden hier von potenziellen Dschihadisten, wir reden von Terroristen; vorher wurde gesagt, es sei zu spät, wenn der Terrorist schon tot sei. Der Terrorismus wird finanziert von irgendjemandem, und darum geht es in diesem Gesetz auch. Wir sprechen hier von Pädokriminellen, von einem Thema, bei dem Sie gerne heftig sind, vehement sind, das Strafrecht verschärfen, das Tätigkeitsverbot ausweiten. Hier geht es darum, die Mittel dafür zu schaffen, dass diese Pädokriminellen gefunden werden, damit sie nachher bestraft werden können.
Wir reden hier auch von Ermittlungsmethoden, die nur dann eingesetzt werden können, wenn bereits ein Strafverfahren eröffnet worden ist. Dazu muss ich jetzt doch das eine oder andere klarstellen. Verdachtsunabhängige Überwachung ist kein Thema des Büpf, sondern das ist das Thema des Nachrichtendienstgesetzes, das Sie in der letzten Session doch mit beträchtlicher Mehrheit angenommen haben. Ich lese Ihnen gerne aus der Strafprozessordnung vor – einfach damit es gesagt ist, weil Sie vielleicht die Strafprozessordnung heute nicht dabeihaben. Dort ist nämlich ganz konkret festgehalten, in welchen Fällen überhaupt die Überwachung der Telekommunikation möglich ist. Es muss erstens einen dringenden Verdacht geben; es muss eine schwere Straftat sein, und die bisherigen Untersuchungsmethoden müssen erfolglos geblieben sein. Das sind die Voraussetzungen, damit überhaupt die Anwendung einer Überwachungsmethode infrage kommt. Dann muss die Strafverfolgungsbehörde einen Antrag stellen. Dieser muss vom Zwangsmassnahmengericht bewilligt werden. Sprechen Sie von "verdachtsunabhängig" am richtigen Ort, aber beim Büpf ist das kein Thema; diese Aussage ist schlicht und einfach falsch.
Eine Minderheit Ihrer Kommission möchte diese Vorlage zurückweisen – übrigens nicht an die Verwaltung, sondern an den Bundesrat; sie möchte, dass der Bundesrat diese Vorlage noch einmal überarbeitet. Mit dieser Rückweisung verlangt die Minderheit erstens, dass die Randdaten nicht mehr gespeichert werden dürfen. Einige von Ihnen haben es bereits gesagt: Die Randdaten werden heute schon gespeichert, und zwar während sechs Monaten. Das Einzige, was wir hier vorsehen, ist, dass die Randdatenspeicherung auf zwölf Monate verlängert wird. Dazu habe ich heute auch ein paar abenteuerliche Sachen gehört; das muss ich Ihnen sagen. Wer speichert eigentlich diese Randdaten? Es sind die Fernmeldedienstanbieter, die diese Randdaten speichern. Es geht dabei unter anderem um die Frage: Wer hat mit wem wie lange telefoniert? Diese Daten werden von der Swisscom, von Salt, von verschiedensten Fernmeldedienstanbietern gespeichert. Warum tun sie das? Damit sie Ihnen am Ende des Monats eine Rechnung stellen können. Nicht der Staat speichert diese Daten, sondern private Anbieter.

Was wir in diesem Gesetz regeln, ist die Frage, unter welchen Voraussetzungen die Strafverfolgungsbehörde das Recht hat, diese Randdaten zu überwachen respektive einzuholen, um bei Verdacht auf eine schwere kriminelle Handlung die Möglichkeit zu haben, den Täter zu finden; darum geht es in diesem Gesetz. Hören Sie also auf zu sagen, der Staat würde hier Daten speichern – es sind die Privaten, die das tun. Denjenigen, die sich darüber ärgern und die es stört, dass ihre Daten gespeichert werden, möchte ich vielleicht sagen: Ja, machen Sie den Vorschlag, dass die Fernmeldedienstanbieter diese Daten auch nicht mehr speichern dürfen! Oder stört es Sie nicht, wenn ausgerechnet private, kommerzielle Unternehmen Ihre sensiblen Daten speichern? Also ich bitte Sie, hier diese Unterscheidung zu machen.
Warum wollen wir diese Erhöhung von heute sechs auf neu zwölf Monate bei der Randdatenspeicherung? Weil die Erfahrung gezeigt hat, dass es bei der Ermittlung von Straftaten oft eine gewisse Zeit braucht! Damit diese Zeit auch vorhanden ist, zum Beispiel wenn es um Rechtshilfeersuchen, um komplexe Fälle geht, möchten wir eine Erhöhung auf zwölf Monate. Sie haben ja gesehen, dass zuerst auch anders ermittelt werden muss. Diese Daten können erst angefordert werden, wenn es sich gezeigt hat, dass andere Ermittlungsmethoden nicht zum Resultat geführt haben. Dann kann es eben sein, dass diese sechs Monate nicht reichen, und deshalb möchten wir diese Zugriffsmöglichkeiten auf zwölf Monate erhöhen.
Wenn es Sie dermassen stört, dass der Staat, die Strafverfolgungsbehörde während zwölf Monaten auf diese Daten zurückgreifen kann: Stört es Sie dann nicht, wenn Private diese Daten während zehn Jahren speichern? Darüber sprechen wir! Die Banken speichern übrigens jede Ihrer Bankbewegungen während zehn Jahren, und das sind bekanntlich ja auch sensible Daten. Stört Sie das nicht? Und wenn es eine Strafverfolgung gibt, hat die Strafverfolgungsbehörde Zugriff auf diese Daten. Bei einem Strafverfahren gibt es die Herausgabepflicht; es gibt die Editionspflicht. Wenn Sie also bezüglich Ihrer Randdaten in der Telekommunikation sensibel sind, müssten Sie doch auch sensibel sein, wenn es um Ihre Bankbewegungen geht. Ich bitte Sie einfach, hier diese Unterscheidung zu machen. Wir sprechen von schweren Straftaten, wir sprechen von eröffneten Strafverfahren, und nach der Bewilligung durch das Zwangsmassnahmengericht ist die Möglichkeit vorhanden, dass auf diese Daten zurückgegriffen wird.
Ich sage Ihnen noch, welche Folgen ein Verzicht auf die Erhebung von Randdaten haben kann. Der Verzicht darauf würde bedeuten, dass Sie dann in einem Strafverfahren oder eben auch im Falle einer Kindesentführung – ja, das gibt es leider auch in unserem Land – die Möglichkeit nicht mehr haben, auf die Randdaten zurückzugreifen. Den Zugriff auf die Randdaten haben wir ja auch hierfür vorgesehen. Ich möchte dann das nächste Mal, wenn ein Kind entführt wird, sehen, wenn man sagt, leider habe das Parlament entschieden, dass man nicht auf diese Randdaten zurückgreifen kann; man habe deshalb diese Möglichkeit leider nicht zur Verfügung, obwohl vielleicht gerade solche Daten helfen könnten, ein entführtes Kind zu finden.
Es gibt aber noch eine weitere Folge der Entscheidung, die Randdatenspeicherung nicht mehr zu ermöglichen respektive den Zugriff für die Strafverfolgungsbehörden zu

verweigern. Wenn ein Verurteilter aus dem Gefängnis entweicht, suchen wir ihn mit allen Mitteln. Dann kann der Zugriff auf diese Randdaten ebenfalls dazu dienen, den entwichenen, verurteilten Straftäter zu finden. Wenn Sie die Randdatenspeicherung, hier den Zugriff auf die Randdatenspeicherung, verweigern, haben Sie in diesem Fall die erwähnte Möglichkeit nicht.
Ich komme noch zum Entscheid des Europäischen Gerichtshofes, der hier immer wieder zitiert worden ist. Ich sage Folgendes dazu: Dieser Entscheid, der jetzt offenbar die höchste aller Massnahmen und Entscheide ist, sagt nicht, dass die Randdatenspeicherung generell unzulässig sei. Der Entscheid des Europäischen Gerichtshofes verlangt jedoch, dass es eine konkrete rechtliche Grundlage braucht. Diese schaffen wir in diesem Gesetz. Wir schaffen Klarheit, wer unter welchen Voraussetzungen auf diese Daten zugreifen kann. Genau das ist in dieser Vorlage geregelt. Es sind eben die Strafverfolgungsbehörden, es ist nicht irgendwer, der darauf zugreifen kann, und zwar – wie ich es bereits gesagt habe – erst nach dem Entscheid eines Gerichtes, das eine solche Massnahme bewilligen muss.
Ich sage Ihnen mal, wer heute in Europa eine solche Vorratsdatenspeicherung hat und wie lange sie dauert: Belgien ein Jahr, Dänemark ein Jahr, Finnland ein Jahr, Frankreich ein Jahr, Italien bis zu zwei Jahre, Niederlande ein Jahr, Portugal ein Jahr, Spanien und Grossbritannien ein Jahr. Deutschland ist daran, diese Frage ebenfalls zu regeln, Österreich ebenfalls. Der Europäische Gerichtshof hat verlangt, dass die Voraussetzungen geklärt sein müssen, dass sie restriktiv sein müssen und dass sie gesetzlich geregelt sein müssen – genau das, was Sie heute beschliessen können.
Im Übrigen sieht auch die Cybercrime-Konvention des Europarates einen Minimalstandard vor, nämlich dass die verfügbaren Randdaten für Zwecke der Strafverfolgung beigezogen werden können, weil das bei der Be-

kämpfung von Cyberkriminalität etwas Wichtiges für die Strafverfolgungsbehörden ist.
Noch etwas zum Persönlichkeitsschutz: Wir haben in diesem Gesetz dem Persönlichkeitsschutz grosse Bedeutung beigemessen. So muss die überwachte Person über die Überwachung informiert werden. Damit verhindern wir, dass die Strafverfolgungsbehörden einfach möglichst oft und breit überwachen lassen, weil sie wissen, dass ihre Massnahmen nicht nur vor einem Gericht bestehen müssen, sondern allenfalls auch von der betroffenen Person beurteilt werden.
Ich komme jetzt noch zu einem zweiten Punkt des Rückweisungsantrages, den ich, das muss ich Ihnen sagen, ebenfalls schwer nachvollziehen kann. Es wurde bereits gesagt: In der letzten Session haben Sie mit 119 zu 65 Stimmen das Nachrichtendienstgesetz angenommen. Sie haben damit entschieden, dass der Nachrichtendienst in Zukunft präventiv mit den sogenannten Staatstrojanern in Computer eindringen kann, um zum Beispiel – Sie haben das gesagt – potenziellen Dschihadisten auf die Spur zu kommen. Heute entscheiden Sie, ob die Strafverfolgungsbehörden, falls sich der Verdacht des Nachrichtendienstes bestätigt hat, ihre Arbeit überhaupt aufnehmen können, um diese potenziellen Täter dann auch vor Gericht bringen zu können. Der Nachrichtendienst kann nicht vor Gericht gehen. Dazu braucht es eine Strafverfolgungsbehörde, dazu braucht es einen Staatsanwalt. Da müssen Sie doch den Strafverfolgungsbehörden die gleichen Instrumente in die Hand geben, die Sie vorher dem Nachrichtendienst in die Hand gegeben haben, sonst kommt es so weit, dass die Strafverfolgungsbehörde die entsprechenden Beweismittel nicht hat. Stellen Sie sich das einmal vor! Da entdeckt der Nachrichtendienst einen potenziellen Täter. Das Gericht muss den Täter laufen lassen, weil die Strafverfolgungsbehörde die Beweismittel nicht beibringen konnte. Stellen Sie sich einmal eine solche Absurdität vor! Das sind die Folgen, wenn Sie heute im Büpf den Einsatz der Govware ablehnen.
Ich sage gerne noch etwas zu den Staatstrojanern. Ohne sie hat die Strafverfolgung keinen Zugriff auf die verschlüsselte Kommunikation. Das heisst ganz simpel und einfach, Kriminelle, Schwerverbrecher, Pädokriminelle, Dschihadisten, Drogenbosse können sicher sein, dass es keine Überwachungsmöglichkeit gibt, wenn sie über die verschlüsselte Kommunikation kommunizieren. Diese verschlüsselte Kommunikation ist nicht irgendetwas, was nur wenige kennen. Sie alle in diesem Saal, kommunizieren vermutlich auch verschlüsselt, indem Sie nämlich Skype verwenden, indem Sie Whatsapp verwenden, indem Sie mit Ihrem i-Phone über Facetime telefonieren. Das heisst, ohne diese Staatstrojaner gibt es keinen Zugang der Strafverfolgungsbehörden zu dieser Kommunikation. Das ist eigentlich eine Einladung an die Kriminellen, sich auf diesen Kanälen auszutauschen.
Ich möchte noch etwas zu den Staatstrojanern sagen. Sie wurden in unserem Land schon mehrmals angewendet, mit der Genehmigung des zuständigen Zwangsmassnahmengerichtes. Man kann sich darüber streiten, ob es heute schon eine gesetzliche Grundlage für die Verwendung von Govware durch die Strafverfolgungsbehörde gibt. Der Vorschlag des Bundesrates enthält aber nicht nur eine explizite rechtliche Grundlage für die Verwendung von Govware, sondern auch die entsprechenden Bestimmungen und, damit verbunden, enge Schranken. Es wird also der Tatsache Rechnung getragen, dass die Überwachung mittels Govware besonders sensibel ist. Ich würde eigentlich sagen: All diejenigen unter Ihnen, die hier sehr kritisch sind, müssen doch ein Interesse daran haben, dass jetzt in diesem Gesetz die rechtlichen Schranken gesetzt werden. Sie sind eng, die rechtlichen Schranken. Und Sie müssten auch ein Interesse daran haben, dass dieser Schwebezustand – ob die Govware dann halt angewendet wird, je nach Ansicht, ob dafür die gesetzlichen Grundlagen bestehen oder nicht –, dass diese Unsicherheit beseitigt wird, indem Sie, der Gesetzgeber, sagen, was gemacht werden darf und was nicht.
Ich komme zum Schluss. Der Antrag auf Nichteintreten ist zurückgezogen worden. Der Rückweisungsantrag besteht nach wie vor. Ich sage es Ihnen noch einmal, in aller Deutlichkeit: Wenn Sie auf die Vorratsdatenspeicherung verzichten wollen, wie das die Kommissionsminderheit will, dann verzichten Sie darauf, dass die Strafverfolgungsbehörden überhaupt die Möglichkeit haben, Straftätern auf die Spur zu kommen. Und ich sage all denjenigen, die dem Nachrichtendienstgesetz zugestimmt haben – es sind auch hier viele –, noch einmal: Wenn Sie hier dem Rückweisungsantrag zustimmen, dann ist das, was Sie beim Nachrichtendienstgesetz beschlossen haben, nämlich der Zugriff auf die Randdaten, auch weg; dann können Sie beim Nachrichtendienstgesetz die präventive Überwachung auch vergessen, da Sie im Nachrichtendienstgesetz explizit auf das Büpf verwiesen haben. Passen Sie also auf! Wenn Sie dem Nachrichtendienstgesetz zugestimmt haben und jetzt den Rückweisungsantrag unterstützen, torpedieren Sie das, was Sie beim Nachrichtendienstgesetz unterstützt haben.
Ich bitte Sie, auf die Vorlage einzutreten und den Rückweisungsantrag abzulehnen. Wenn Sie Feinkorrekturen machen wollen, weil Sie mit gewissen Dingen nicht einverstanden sind, dann tun Sie das in der Detailberatung – dort haben Sie die Möglichkeit dazu.

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

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

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

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

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

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

Sommaruga Simonetta, Bundespräsidentin: Schauen Sie, Herr Schwander: Hier sprechen wir nicht davon, wie lange jemand die Daten aufbewahren muss, sondern davon, wie lange der Zugriff für die Strafverfolgungsbehörden garantiert werden muss. Darum geht es. Heute müssen die Fernmeldedienstanbieter während sechs Monaten garantieren, dass ein Zugriff möglich ist; deshalb müssen sie die Daten so lange aufbewahren. Neu müssen sie sie zwölf Monate aufbewahren. Ich kann Ihnen aber sagen, dass die Fernmeldedienstanbieter die

Daten heute länger aufbewahren; dies wegen der Telefonrechnungen, bei welchen es manchmal Reklamationen gibt. Bei den Banken ist im Bankengesetz geregelt, wie lange sie Daten aufbewahren müssen; das regeln wir nicht hier. Die Banken müssen die Daten ohnehin herausgeben. Sie kennen die Editionspflicht in der Strafprozessordnung: Die Banken müssen diese Daten herausgeben, unabhängig davon, ob sie das wollen oder nicht.

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

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

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

que l'on puisse vérifier que le cheval de Troie a seulement surveillé une télécommunication et n'a rien fait d'autre.
J'en viens maintenant à la proposition de renvoi de la minorité Vischer Daniel. Je pense qu'il vaut la peine de relire attentivement cette proposition de renvoi dont le but est le renvoi du projet non pas à l'administration comme cela a été dit, mais au Conseil fédéral, ce qui lui confère une portée tout de même un petit peu plus importante.
La demande vise à un renvoi au Conseil fédéral pour recommencer les travaux qui ont déjà été faits sur deux points. Le premier point consiste à ne plus prévoir la possibilité de conserver des données secondaires. Cette position est tout ce qu'il y a de plus légitime, c'est un débat que nous devons mener et que nous allons d'ailleurs mener. Mais pourquoi demander au Conseil fédéral de recommencer les travaux sur ce point? Celles et ceux

qui ne souhaitent pas que soit prévue la conservation des données secondaires n'ont pas besoin d'attendre que le Conseil fédéral revienne à la charge, puisqu'il suffit d'accepter – certes ce n'est pas ce que va vous recommander la commission – les propositions de minorité IV et V (Vischer Daniel) aux articles 19 et 26. Il ne s'agit que de votes, c'est vite fait, c'est facile et cela évite de recommencer les travaux de zéro.
Le second point visé par la proposition de renvoi au Conseil fédéral concerne l'obtention de garanties supplémentaires sur l'emploi des chevaux de Troie. Là encore, à mon avis et de l'avis de la majorité de la commission, il n'est pas nécessaire que le Conseil fédéral recommence à zéro des travaux qui ont été menés en commission. La commission vous propose l'introduction de l'article 269quater du Code de procédure pénale, article non contesté qui contient justement les garanties demandées par Monsieur Vischer. Ce dernier, d'ailleurs, ne s'y oppose pas puisqu'il a accepté la proposition de la commission qui, en l'espèce, a pris sa décision à l'unanimité.
Reste la question de l'exploitation des preuves qui auraient été obtenues frauduleusement par un usage interdit des chevaux de Troie. Je vous demande ici de considérer l'article 141 alinéa 2 du Code de procédure pénale en vigueur qui répond justement à cette question, puisqu'il y est écrit que "les preuves qui ont été administrées d'une manière illicite ou en violation de règles de validité par les autorités pénales ne sont pas exploitables, à moins que leur exploitation soit indispensable pour élucider des infractions graves". "Ne sont pas exploitables": je crois que ces quatre mots sont absolument capitaux. Ce que demande la minorité Vischer Daniel par sa proposition de renvoi, c'est que le Conseil fédéral planche à nouveau sur quelque chose qui existe déjà dans la législation. Et même si ce quelque chose ne devait pas convenir au conseil, il aurait toujours la possibilité, sans passer par la case renvoi, d'accepter la proposition de la minorité Vischer Daniel à l'article 269quater.
Je vous invite à rejeter la proposition de renvoi au Conseil fédéral, comme le suggère la majorité de la commission.

Flach Beat (GL, AG), für die Kommission: Der Rückweisungsantrag Vischer Daniel lag der Kommission vor. Wir haben sehr lange, an mehreren Sitzungen, über all diese Fragen diskutiert. Ich möchte Sie bitten, diesen Rückweisungsantrag abzulehnen, wie das auch die Kommission gemacht hat; die Kommission hat den Antrag im Übrigen mit 16 zu 9 Stimmen abgelehnt.
Worum geht es? Es geht nicht einzig darum, dass man hier ein neues Konzept machen soll. Vielmehr müssen Sie sich im Klaren darüber sein, dass Sie mit dem Rückweisungsantrag eine Sammlung an Aufträgen übernehmen. Der Rückweisungsantrag beantragt nicht nur, dass es keine Vorratsdatenspeicherung mehr geben soll, sondern auch, dass der Imsi-Catcher und die sogenannte Government Software nur noch bei schweren Gewaltverbrechen eingesetzt werden können.
Sie haben es vorhin gehört, auch Frau Bundespräsidentin hat es ausgeführt: Die Rückweisung hätte zur Folge, dass sehr viele Delikte dann nicht mehr erfasst wären. Es gibt im Strafgesetzbuch ja keinen Deliktekatalog für besonders schwere Gewaltverbrechen. Das Bundesamt für Statistik unterscheidet bei all diesen vielen Delikten zwischen Raub, Vergewaltigung, Geiselnahme usw., die alle zu diesen schweren Gewaltverbrechen gehören. Doch was gehörte dann nicht mehr zu dieser Gruppe? Es wären beispielsweise das Verbreiten von Falschgeld oder die Flucht nicht dabei – wir haben es gehört -; das Verbreiten von Kinderpornografie, Cyberkriminalität, auch schwere Fälle von Betrug würden nicht dazugehören.
Damit komme ich auch gleich auf die Randdatenspeicherung zu sprechen. Wenn Sie auf die Randdatenspeicherung verzichten – ich erinnere daran, dass wir sie heute haben, und zwar für sechs Monate –, dann verliert die Strafverfolgungsbehörde ein sehr, sehr wichtiges Instrument. Es wurde ausgeführt, dass das gar nicht so wichtig und für die Strafverfolgung von wenig Belang sei. Das ist nicht so. Es gibt schliesslich nicht nur die schweren Fälle, sondern auch ganz Profanes. Da müssen Sie mir schon erklären, weshalb Sie diese nicht verfolgen wollen. Die Staatsanwaltschaften haben uns verschiedene Fälle vorgestellt: Ich erinnere beispielsweise an die Bande der Enkeltrickbetrüger, welche alte Frauen abgezockt hat. Da hat irgendeine Person an der Türe einer alten Frau geklingelt und behauptet, er sei im Namen ihres Enkels gekommen, um das Geld abzuholen, das der Enkel leider nicht persönlich abholen könne, worauf die alte Frau mit dem Betrüger zur Bank gegangen ist. Wenn man diese Person dann befragt hat, hat sie gesagt, dass sie nichts mit der Sache zu tun habe und nur gebeten worden sei, das Geld abzuholen. Wenn man über die Randdaten verfügt, kann man feststellen, dass die Verdächtigen sehr wohl miteinander in Kontakt gestanden sind, sodass man den Fall aufklären kann.
Dann muss ich noch etwas anderes sagen: Diese Randdaten dienen nicht nur dazu, jemanden, der in einem Strafverfahren angeklagt ist, zu überführen – dazu braucht es viele kleine Indizien –, sondern sie können auch helfen, jemanden zu entlasten. Stellen Sie sich vor, Sie haben einen schweren Autounfall, und zwei oder drei Monate später taucht ein Zeuge auf, der sagt: Ich habe Sie gesehen, Sie waren am Telefonieren, als der Unfall passierte. Sie können dann schon behaupten, Sie hätten nicht telefoniert; vielleicht sind Sie dann aber wirklich

froh, wenn Sie auf solche Randdaten zurückgreifen und belegen können, dass zumindest mit Ihrem Handy zu jenem Zeitpunkt nicht telefoniert wurde.
Die ganze Diskussion kommt mir ein klein wenig vor, als spiele sie sich hundert Jahre früher ab, als hätten wir gerade die Einführung des Automobils erlebt und würden nun sagen: Jetzt haben zwar auch Verbrecher Autos, aber der Polizei geben wir keine, um die Verbrecher zu verfolgen, denn diese sind sowieso zu schlau und zu schnell; wir verzichten darauf, die Polizei soll weiterhin mit Pferden auf Verbrecherjagd gehen.
Noch eine Bemerkung betreffend Staatstrojaner: Im Rückweisungsantrag wird gefordert, dass Staatstrojaner sicher sein müssen, dass Sicherheitsmassnahmen zu treffen sind und dass die erhobenen Daten nicht für andere Zwecke gebraucht werden. Wir sind hier im Strafprozessrecht; es gibt in der Strafprozessordnung ganz klare Regeln, wie man mit sogenannten Zufallsfunden umzugehen hat. Das gilt hier ebenso wie an andern Orten. Es ist ganz klar, dass es hier nicht um ein Ausschnüffeln irgendwelcher Leute geht, gegen die kein Verdacht besteht. Es geht darum, in einem eröffneten Strafverfahren nach der Genehmigung durch ein Strafmassnahmengericht eine Government Software einzuführen.
Herr Vischer hat ausgeführt, dass in der Kommissionsberatung nicht klar herausgekommen sei, wie es dann funktioniere. Es ist tatsächlich so, dass wir hier ein Gesetz machen, das nicht nur auf den Status quo zielt, sondern auch in die Zukunft gerichtet ist. Die digitale Kommunikation und die digitale Welt sind eine Realität. Ich habe mir in den vergangenen Wochen einen Spass daraus gemacht, im Umfeld und bei Kollegen zu schauen, was für kleine Apps sie auf ihren Handys haben und welche Funktionen sie diesen zugestehen. Ich kann Ihnen sagen, dass es auch in diesem Saal

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

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

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

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

Abstimmung – Vote
(namentlich – nominatif; 13.025/12092)
Für den Antrag der Minderheit ... 50 Stimmen
Dagegen ... 128 Stimmen
(7 Enthaltungen)

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

Detailberatung – Discussion par article

Titel und Ingress
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

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

Angenommen – Adopté

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

Block 1 – Bloc 1
Randdaten
Données secondaires

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

Leutenegger Oberholzer Susanne (S, BL): Die Minderheit I verlangt bei Artikel 19 Absatz 4, dass die Randdaten des Postverkehrs maximal während sechs Monaten aufbewahrt werden müssen. Das entspricht dem Beschluss des Ständerates. Es handelt sich hier um ganz wenige Fälle. Bereits die sechs Monate sind, wenn man sich die Fallzahlen vor Augen führt, an der Grenze der Verhältnismässigkeit. Es handelt sich hier vor al-

lem um Postsachen mit Zustellnachweis, z. B. die LSI-Zustellungen. Es macht aber weder sicherheitstechnisch noch ökonomisch Sinn, eine längere Aufbewahrungsfrist zu verlangen.
Ich bitte Sie deshalb – für den Fall, dass die Aufbewahrung nicht generell gestrichen wird –, mit der Minderheit die Verhältnismässigkeit zu wahren und mit dem Ständerat auf sechs Monate zurückzugehen; das genügt.

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

AB 2015 N 1154 / BO 2015 N 1154

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

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

Vischer Daniel (G, ZH): Ich habe hier zwei Minderheitsanträge zu vertreten. Mit dem ersten, mit meinem Minderheitsantrag V bei Artikel 26 Absatz 5, soll nun die Vorratsdatenspeicherung abgeschafft werden. Es wurde mir ja, nicht zuletzt von Leuten aus der SP, gesagt, sie seien für die Abschaffung der Vorratsdatenspeicherung, aber nicht für die Rückweisung. Das ist jetzt der Moment, wo wir handeln müssen, nachdem Sie die Rückweisung nicht beschlossen haben.
Die Argumente über die Vorratsdatenspeicherung wurden ausgetauscht. Ich habe nicht ganz begriffen, was Herr Schwaab meinte, als er vorhin darlegte, warum dieser Entscheid des Europäischen Gerichtshofes für uns nicht anwendbar und massgebend sein soll. Vor allem habe ich nicht begriffen, was kritisiert wird, wenn wir sagen, der Hauptgrund des Entscheides sei gewesen, dass eine Präventivüberwachung stattfindet, bei der keine Kriterien obwalten, welche Personen nach welchen Kriterien überwacht werden. Wie schon gesagt, entscheidend ist das Moment des Beginns der Überwachung und der Speicherung und nicht das Moment des

rückwirkenden Zugriffs auf Daten nach dem richterlichen Entscheid.
Sie wissen, welche Profile über diese Randdaten erstellt werden können. Und nun ist es in der Tat ein Abwägen. Es hat keinen Sinn, jetzt so zu tun, als seien diejenigen, die gegen die Vorratsdatenspeicherung sind, gegen die Verbrechensbekämpfung. Gut, ich würde diese Schiene auch fahren, wenn ich Bundesrat wäre und diese Vorlage zu vertreten hätte; da muss man natürlich mit den Beispielen kommen, die alle im Land dann an einer "Arena"-Sendung hellhörig machen: "Ja gut, wenn ihr die Vorratsdatenspeicherung nicht wollt, dann wollt ihr keine Dschihadisten-Verfolgung, dann wollt ihr die Pädophilie nicht bekämpfen." Aber es ist durch das Gutachten des Max-Planck-Institutes eben gerade nicht nachgewiesen worden, dass über die Vorratsdatenspeicherung tatsächlich eine effizientere Verbrechensbekämpfung erfolgt.
Die Schweiz hat – obwohl sie die Vorratsdatenspeicherung kennt – gerade in den vorgenannten Bereichen keine grösseren Fahndungserfolge als beispielsweise Deutschland. In Deutschland gibt es heute, nachdem der SPD-Parteichef den Justizminister aus seiner Partei genötigt hat, die Vorratsdatenspeicherung einzuführen, auch in SPD-Kreisen eine immer breitere Diskussion über die Vorratsdatenspeicherung. Die ehemalige Justizministerin, eine ausgewiesen liberale Person, Frau Leutheusser-Schnarrenberger, ist eine der profiliertesten Kritikerinnen dieses Instruments. Es ist eigentlich die gleiche Diskussion, wie wir sie hier führen. Es ist eine Diskussion über die Frage: Welche Eingriffe in den Grundrechtsschutz sind uns potenzielle Verbrechensbekämpfungserfolge wert? Da sagen wir: Es muss schon ein plausibler Nachweis da sein, dass grössere Erfolge möglich sind, bevor wir einem solchen Eingriff zustimmen.
Mein zweiter Minderheitsantrag will die Vorratsdatenspeicherung nicht abschaffen, sondern sie auf drei Monate reduzieren. Das ist gewissermassen die Eventualargumentation. Sie hat auch ein bisschen damit zu tun, dass man sagen kann: Okay, diese Daten werden eh gespeichert, also kommt es jetzt darauf an, wie lange sie gespeichert werden dürfen. Da meinen wir eben, dass drei Monate eine vertretbare Obergrenze sind, ab der die Verhältnismässigkeit nicht mehr gewahrt ist.
Es ist übrigens ein qualitativer Unterschied mit Bezug auf das informationelle Selbstbestimmungsrecht, ob ich einfach gedankenlos über weiss ich was für Karten und Beteiligungen an weiss ich was für Aktionen von Facebook bis weiss ich wohin mich freiwillig einlogge oder ob ich unabhängig davon, wie ich mich verhalte, dulden muss, dass Daten zugunsten des Staates zwangsgespeichert werden. Das ist ein qualitativer Unterschied; ich bitte Sie, diesen zu beachten. Das macht die Vorratsdatenspeicherung letztlich suspekt. In diesem Sinne war die Frage von Frau Badran bestenfalls gut gemeint, aber sie zielte eben genau an dieser qualitativen Unterscheidung vorbei.
Ich ersuche Sie mithin, hier nun Farbe zu bekennen und entweder die Vorratsdatenspeicherung abzuschaffen oder die Speicherung nur für drei Monate zu bewilligen. Hier zeigt es sich, wer rechtsstaatliche Erwägungen in den Vordergrund stellt und wer nicht.

AB 2015 N 1155 / BO 2015 N 1155

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

Ruiz Rebecca Ana (S, VD): Le but des propositions de minorité Schwaab aux articles 19 et 26 est d'améliorer le respect des droits fondamentaux liés à la conservation des données secondaires. Concrètement, il s'agit de faire en sorte que leur stockage se fasse ici en Suisse. On s'assurerait ainsi que leur conservation soit conforme aux règles en matière de protection des données et de la sphère privée prévalant dans notre pays. Alors qu'il s'agit de données passablement sensibles puisqu'elles permettent d'identifier quand ont eu lieu des télécommunications, quelle a été leur durée et où se trouvaient les personnes lors de ces échanges, il paraît pertinent de pouvoir les conserver ici. Les raisons sont assez simples.
Si on décidait de ne pas inscrire dans la loi cette nécessité, nous prendrions le risque que le stockage se fasse dans d'autres pays à travers des entreprises qui, bien que soumises au droit suisse, pourraient faire appel à des services de "cloud computing". De quoi s'agit-il concrètement? Il s'agit d'infrastructures dans lesquelles le stockage est géré par des serveurs à distance auxquels on se connecte de manière sécurisée, via Internet. On pourrait alors imaginer que les pays qui hébergeraient ces infrastructures de "cloud computing" n'aient pas les mêmes standards de protection des données que ceux que prévoit notre législation. On pourrait aussi imaginer qu'une entreprise stockant des données soit rachetée par une entreprise soumise à un droit étranger peu soucieux de la protection des données, tel que par exemple le droit américain. On sait en effet que le matériel informatique et les logiciels qui servent au stockage de données et à gérer les réseaux informatiques d'entreprises proviennent en grande partie de sociétés américaines. Le problème qui se poserait alors réside

dans le fait que les entreprises américaines peuvent être obligées de fournir la totalité des données en leur possession aux services secrets, sans en informer les titulaires. Il s'agirait donc de se prémunir contre ce type de risque qu'on ne peut, hélas, exclure.
Je vous donne un exemple qui concerne mon canton et qui illustre bien la problématique. En février de cette année, le support informatique, qui avait été développé en Europe, gérant les dossiers informatiques des patients de l'hôpital universitaire vaudois, a été racheté par une société américaine. Lorsque l'annonce de ce rachat a été connue, des craintes ont été émises, notamment celle que les données gérées par ce support soient soumises au "Patriot Act" qui, comme je le disais, donne aux services américains de sécurité un accès aux données informatiques détenues par des entreprises ou des particuliers, de manière quasi discrétionnaire et sans autorisation préalable. Mais, au final, ces craintes se sont avérées infondées. Pourquoi donc? Précisément parce que les contrats prévoyaient que les données seraient stockées en Suisse, selon notre droit.
C'est exactement le but visé par les propositions de minorité Schwaab, que je vous remercie donc de soutenir.

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

Chevalley Isabelle (GL, VD): Je parlerai principalement de l'article 26 alinéa 5, qui concerne en partie aussi l'article 19 alinéa 4.
L'article 26 alinéa 5 concerne le délai durant lequel les fournisseurs de services de télécommunication doivent conserver les données secondaires. Si la majorité du groupe vert'libéral estime que six mois sont suffisants, une minorité estime que douze mois sont nécessaires. En effet, la majorité de notre groupe est sceptique sur le bénéfice réel que pourrait apporter une conservation de douze mois en regard des atteintes à la liberté individuelle.

Les autorités de poursuite pénale que nous avons entendues nous ont demandé un délai de douze mois. Selon les cas, ils n'arrivent pas à obtenir toutes les autorisations en six mois. Pour le cas, par exemple, d'un pédophile pour lequel nos autorités devraient requérir l'entraide d'un autre pays, on a pu observer que le délai de six mois n'était pas suffisant. C'est très frustrant pour les enquêteurs de se retrouver, pour une question de délai, dans l'incapacité d'analyser des données qui auraient pu faire condamner un criminel.
Par ailleurs, il faut mentionner le risque de stockage de toutes ces données pour la protection de la sphère privée, car si certes seules les données d'une toute petite minorité de personnes soupçonnées seront finalement écoutées et analysées, il n'en demeure pas moins que toutes les données, y compris les miennes et celles de tous mes collègues et citoyens résidant en Suisse seront également stockées.
D'un côté, on double la durée de conservation des données et, de l'autre, on pourra attraper quelques criminels en plus. Il s'agit donc de faire une pesée d'intérêts entre protection

AB 2015 N 1156 / BO 2015 N 1156

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

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

Huber Gabi (RL, UR): Die Vorlage sieht sowohl im Bereich des Postverkehrs wie auch im Bereich des Fernmeldeverkehrs eine Verlängerung der Aufbewahrungsfrist der Randdaten von sechs auf zwölf Monate vor, denn das Problem des Verlusts von für die Strafverfolgung wichtigen Daten stellt sich nicht nur im Fernmeldeverkehr, sondern auch im Postverkehr. Somit muss die Verlängerung der Aufbewahrungsfrist logischerweise für beide Bereiche gelten. Aus der Praxis der Staatsanwaltschaften hat sich nämlich ergeben, dass eine Aufbewahrungsfrist von sechs Monaten zu kurz bemessen bzw. so kurz ist, dass Daten bei der Bekämpfung gewisser Formen von Kriminalität verlorengehen. Im Vordergrund stehen hier Fälle von Kinderpornografie, von organisiertem Verbrechen und Terrorismus, bei denen die Meldungen oft aus dem Ausland eintreffen und die Eröffnung der Verfahren erst mit Verzögerung stattfindet. Die Frist ist dann in solchen Fällen abgelaufen, ehe die Behörde überhaupt in der Lage ist zu sagen, gegen welche beschuldigte Person das Verfahren laufen soll oder welches Opfer genau identifiziert werden muss.
Die in Artikel 26 Absatz 5 festgelegte Pflicht bedeutet, dass die Anbieter von Fernmeldediensten wie nach der geltenden Regelung die Randdaten des gesamten Fernmeldeverkehrs quasi auf Vorrat für allfällige künftige

Strafuntersuchungen aufbewahren müssen. Gestützt auf die in Artikel 31 enthaltene Kompetenz bezeichnet der Bundesrat die Randdaten, die aufzubewahren sind. Die Möglichkeit der Vorratsdatenspeicherung gleich ganz aus der Vorlage zu streichen, wie dies die Minderheit IV (Vischer Daniel) bei Artikel 19 Absatz 4 und die Minderheit V (Vischer Daniel) bei Artikel 26 Absatz 5 vorschlagen, würde also einer enormen Schwächung der Strafverfolgungsbehörden gleichkommen.
Die Minderheiten III (Reimann Lukas) und IV (Reimann Lukas) wollen bei den beiden erwähnten Artikeln das sogenannte Quick-Freeze-Modell ins Gesetz einführen. Das würde dann bedeuten, dass die Daten im Moment der Anordnung quasi vorübergehend aufbewahrt würden. Wie lange "vorübergehend" sein soll, geht aus dem Minderheitskonzept nicht hervor, und die Vorzüge dieses Modells gegenüber demjenigen des Bundesrates erschliessen sich uns nicht.
Die Minderheitsanträge Schneider-Schüttel, welche bei beiden Artikeln die Löschung der Daten nach der Aufbewahrungsfrist anordnen wollen, wurden offenbar zurückgezogen.
Schliesslich gibt es noch eine Minderheit Schwaab, welche in Artikel 26 Absatz 5bis geografische Vorgaben zum Aufbewahrungsort der Randdaten macht. Damit mischt sich diese Minderheit in die interne Organisation der Post ein, und das hätte einen Wettbewerbsnachteil gegenüber anderen Unternehmen zur Folge. Es kommt dazu, dass die Post gleichwohl schweizerischem Recht unterstellt ist, auch wenn sie Daten im Ausland aufbewahren würde.
Die FDP-Liberale Fraktion wird grossmehrheitlich sämtliche Minderheitsanträge in diesem Block ablehnen, und ich lade Sie ein, Gleiches zu tun.

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

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

Geltungsbereich, der ganz bewusst erweitert werden soll. Mit der Streichung von Litera c schafft man eine Lücke und damit quasi eine Einladung an Kriminelle, auf diese Art zu kommunizieren. Unsere Fraktion lehnt solches ab. Was die Ergänzung in Absatz 2 gemäss Antrag der Minderheit Reimann Lukas betrifft, so lehnen wir dies ebenfalls ab. Man würde damit sogar einen Rückschritt machen und hinter die heutige Regelung gemäss Strafprozessordnung fallen sowie einen entsprechenden Widerspruch stipulieren.
Was den Antrag der Minderheit Reimann Lukas bei Artikel 8 Litera b betrifft, so ist dieser ebenfalls abzulehnen. Es geht hier letztlich wiederum um die Frage, ob man Täter unnötig schützen will oder nicht. Unsere Fraktion will das nicht und unterstützt eine wirkungsvolle Strafverfolgung.

Kurz zu den verschiedenen Minderheiten bei Artikel 19 Absatz 4: Hier geht es um die Dauer der Aufbewahrungspflicht von Randdaten der Postdienste und deren allfällige anschliessende Löschung beziehungsweise um den Antrag der Minderheit IV (Vischer Daniel), die Vorratsdatenspeicherung generell zu streichen. Vorab, es geht hier um Postranddaten und damit um sehr wenige Fälle, und trotzdem ist es halt wichtig, dass diese gemäss Bundesrat für die Dauer von zwölf Monaten aufbewahrt werden. Es muss verhindert werden, dass bei schweren Delikten – wir sprechen hier, es wurde gesagt, von Kinderpornografie, von organisiertem Verbrechen, von Terrorismus usw. – Täter der Strafverfolgung entgehen, nur weil solche Daten nicht mehr zur Verfügung stehen. Der entsprechende Mehraufwand für die Postdienste wie auch die Dauer von zwölf Monaten sind angesichts des öffentlichen Interesses absolut vertretbar und auch verhältnismässig.
Die Anträge der Minderheiten I, III und IV sind somit abzulehnen, ebenfalls der Antrag der Minderheit II, der zwischenzeitlich allerdings zurückgezogen worden ist. Zustimmen wird unsere Fraktion dem Minderheitsantrag Schwaab betreffend Artikel 19 Absatz 4bis. Es geht hier um den Ort der Aufbewahrung der Randdaten aus dem Postverkehr. Wir haben uns hier für die Schweiz als Aufbewahrungsort entschieden.
Was die Aufbewahrungsfrist der Randdaten im Fernmeldeverkehr betrifft, und damit komme ich zu den Minderheiten bei Artikel 26 Absatz 5, so kann ich im Wesentlichen auf meine Hinweise zu den Minderheiten bei Artikel 19 Absatz 4 verweisen. Ergänzend feststellen möchte ich, dass der Entscheid des Europäischen Gerichtshofes in Luxemburg zur Vorratsdatenspeicherung letztlich für die Schweiz ohne Belang ist; die entsprechenden Ausführungen wurden heute hinreichend gemacht.
Was die Pflicht zur Aufbewahrung der Randdaten durch die Fernmeldedienste in der Schweiz gemäss Minderheitsantrag zu Artikel 26 Absatz 5bis betrifft, so gelten analog die gemachten Hinweise zu den Randdaten im Postverkehr. Unsere Fraktion wird dem Minderheitsantrag Schwaab zustimmen. Schliesslich lehnen wir die Minderheitsanträge bei Artikel 27 ab. Auch diese Minderheitsanträge untergraben letztlich eine effiziente Strafverfolgung, was wir, ich habe es gesagt, nicht wollen.
Zusammengefasst ersuche ich Sie, in Block 1 immer der Mehrheit zu folgen, mit Ausnahme der Artikel 19 Absatz 4bis und 26 Absatz 5bis, wo ich Sie bitte, den Minderheiten zuzustimmen.

Ruiz Rebecca Ana (S, VD): Les données secondaires permettent de savoir qui a été en communication avec qui, quand, pendant combien de temps et d'où ont eu lieu ces échanges. Comme il s'agit de données de facturation, elles sont à l'heure actuelle d'ores et déjà conservées par les opérateurs. Elles sont aussi déjà parfois utilisées à des fins d'enquête, lorsqu'il s'agit de poursuivre des infractions graves. Mais une telle utilisation ne peut se faire que dans le cadre d'une procédure pénale, enclenchée après la commission d'un crime, avec l'autorisation du Tribunal des mesures de contrainte ou alors pour rechercher une personne disparue en grand danger, par exemple un enfant.
Les données secondaires ne peuvent aucunement être obtenues à titre préventif ou pour surveiller Madame ou Monsieur Tout-le-Monde en l'absence de tout soupçon. Non, la surveillance d'individus au travers de ces données secondaires ne peut concerner que des personnes fortement soupçonnées d'avoir commis un crime grave – la liste des infractions en question étant énumérée à l'article 269 alinéa 2 du Code de procédure pénale –, comme les homicides, les assassinats, différents délits économiques, la traite d'êtres humains, l'enlèvement ou encore les délits sexuels.
Une des nouveautés du projet en lien avec les données secondaires concerne leur durée de conservation. Actuellement, la loi prévoit six mois, dans le projet douze mois sont jugés nécessaires, six mois étant considérés comme insuffisants. Autre nouveauté, il est prévu de pouvoir désormais obliger sur demande les fournisseurs de services de communication dérivés à conserver les données secondaires, ce qui est actuellement impossible. Il s'agit par exemple des purs fournisseurs de services e-mail, des fournisseurs tels que Facebook, Dropbox, des plates-formes de "chat", ainsi que des fournisseurs de téléphonie Internet tels que Skype.
En lien avec ces deux points, plusieurs propositions de minorité ont été déposées. Concernant la conservation, notre groupe vous invite à soutenir les propositions de minorité Schwaab qui exigent le stockage des données en Suisse pour s'assurer que la conservation se fasse dans le respect de nos règles en matière de protection des données.
La durée de conservation divise passablement le groupe socialiste. Une partie s'oppose à la prolongation de six à douze mois en mettant en évidence que le faible gain en matière de poursuite pénale qu'une telle prolongation amènera n'est pas suffisant pour justifier une pareille atteinte aux droits fondamentaux.
Ainsi une partie du groupe socialiste soutiendra les propositions de la minorité I (Leutenegger Oberholzer), III (Reimann Lukas) et IV (Vischer Daniel) à l'article 19 alinéa 4, ainsi que les propositions de la minorité I (Schwaab), II (Vischer Daniel), IV (Reimann Lukas) et V (Vischer Daniel) à l'article 26 alinéa 5. Une autre partie du groupe soutiendra les propositions de la minorité II (Schneider Schüttel) à l'article 19 alinéa 4 et

III (Schneider Schüttel) à l'article 26 alinéa 5, qui visent à maintenir la durée de conservation à douze mois, tout en exigeant l'effacement des données après l'échéance du délai. Pour cette partie du groupe, le délai de douze mois se justifie, car il permettra de mieux pouvoir poursuivre la criminalité en ligne, notamment la pédocriminalité, ou les activités criminelles à ramifications internationales, puisqu'il apparaît que les six mois actuels sont trop courts et que ce délai est souvent totalement, ou en grande partie échu, lorsque l'autorité est en mesure d'ordonner une surveillance.
Le groupe socialiste vous invite par ailleurs à rejeter la proposition de la minorité Reimann Lukas à l'article 8 lettre b qui vise à supprimer des données secondaires les informations relatives aux tentatives de communication.
Notre groupe vous invite également à rejeter les propositions de la minorité Reimann Lukas à l'article 2 lettre c, à l'article 2 alinéa 2 et à l'article 27, ainsi que la proposition de la minorité Rickli Natalie à l'article 27. Ces propositions concernent les nouvelles obligations de collaborer imposées aux fournisseurs de services de communication dérivés. Ces derniers étant susceptibles de détenir des données pouvant intéresser les autorités de poursuite pénale, par exemple un échange de messages sur Facebook, il paraît légitime que ces acteurs soient aussi soumis à des obligations dans le domaine de la surveillance.

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

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

Glättli Balthasar (G, ZH): Im Namen der Grünen möchte ich jetzt einen kleinen Appell an all jene richten, die vorher gesagt haben, dass unser Rückweisungsantrag eine Selbstkapitulation des Parlamentes darstelle, und die uns quasi formaljuristisch angegriffen haben, indem sie sagten, wir hätten ja für die Detailberatung Minderheitsanträge für eine Verkürzung oder Abschaffung der Vorratsdatenspeicherung stellen können: Sie haben jetzt solche Minderheitsanträge vorliegen. Das ist jetzt der Moment der Wahrheit. Hier zeigt sich, ob das vorher nur rhetorische Ausflüchte gewesen sind oder ob Sie – ich denke jetzt zum Beispiel an Herrn Lüscher, der mir die Frage gestellt hat – es wirklich ernst meinen mit dem Schutz der Privatsphäre.
In diesem Block sehen wir aber auch noch etwas anderes: Wir sehen, wie absurd es ist, über die gesteigerte Sicherheit und die Möglichkeit zu debattieren, Verbrechen einfacher aufzuklären, indem man die Randdaten speichern würde. Wir haben es hier nämlich nicht nur mit den Randdaten im Fernmeldeverkehr zu tun, sondern auch mit jenen im Postverkehr. Entweder meinen Sie es so – das steht nicht im Text –, dass wir alle künftig

nur noch eingeschriebene Briefe verschicken und auf dem Postweg nur noch eingeschrieben miteinander kommunizieren dürften, weil man dort auch den Absender angeben muss, denn ansonsten sind das völlig lächerliche Bestimmungen! Die Randdaten des Briefpostverkehrs aufzubewahren ist lächerlich, weil doch auf einem Brief in den meisten Fällen – vor allem bei jenen Briefen, mit denen irgendetwas Problematisches oder rechtlich nicht Korrektes kommunizieren werden soll – nicht der Absender dick draufsteht. Im Prinzip zeigen Sie hier eigentlich auch eine gewisse Hilflosigkeit. Und Sie zeigen auch, dass das Versprechen der totalen Sicherheit – oder zumindest das Versprechen einer grösstmöglichen Sicherheit – schon an sehr viel einfacheren Orten als im Internetbereich, der jetzt immer genannt wird, nicht gehalten werden kann.
Wenn ich ein Krimineller wäre, der sich mit anderen austauschen müsste, dann würde ich eine CD mit verschlüsselten Daten oder einen USB-Stick mit verschlüsselten Daten per normale Briefpost verschicken, ohne den Absender darauf, und dann wäre diese ganze Randdaten-Geschichte im Postverkehr ausser Kraft gesetzt. Also, nehmen Sie zumindest den Antrag der Minderheit IV (Vischer Daniel) an, wenn es um die Randdaten im Postverkehr geht. Sonst ist das dann wirklich nichts anderes als Bürokratie pur und Mehraufwand pur.
Nochmals zurück zur Telekommunikation, über die wir vorher gesprochen haben. Ich muss Ihnen sagen, ich hätte eigentlich von den Verteidigern einer besseren Möglichkeit, die Strafverfolgung vornehmen zu können, erwartet, dass sie nicht einfach nur wild mit den Reizwörtern "Pädophilie", "Terrorismus", "Kinderschänder" um sich geschlagen hätten. Ich hätte vielmehr erwartet, dass sie vielleicht auch zur Kenntnis genommen hätten, dass es in anderen europäischen Staaten durchaus ernsthafte Bemühungen von Verantwortlichen für die Justiz gibt – in der Diskussion fiel das eine oder andere Mal der Name Leutheusser-Schnarrenberger, der Name der FDP-Politikerin –, eine bessere Strafverfolgung sicherzustellen, ohne dass man dabei generell auf das Grundrecht auf geschützte Kommunikation und das Grundrecht auf Privatsphäre aller, die sich der elektronischen Kommunikation bedienen, verzichtet. Ich hätte mir hier eigentlich auch vom Bundesrat, von der Bundespräsidentin, einen etwas differenzierteren Approach gewünscht.

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

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

AB 2015 N 1159 / BO 2015 N 1159