Vierte Sitzung – Quatrième séance

Mittwoch, 2. März 2011
Mercredi, 2 mars 2011

15.00 h

10.058

Übereinkommen des Europarates über die Cyberkriminalität. Genehmigung und Umsetzung

Convention du Conseil de l'Europe sur la cybercriminalité. Approbation et mise en oeuvre

Fortsetzung – Suite

Botschaft des Bundesrates 18.06.10 (BBl 2010 4697)
Message du Conseil fédéral 18.06.10 (FF 2010 4275)
Ständerat/Conseil des Etats 29.11.10 (Erstrat – Premier Conseil)
Nationalrat/Conseil national 02.03.11 (Zweitrat – Deuxième Conseil)
Nationalrat/Conseil national 02.03.11 (Fortsetzung – Suite)
Ständerat/Conseil des Etats 18.03.11 (Schlussabstimmung – Vote final)
Nationalrat/Conseil national 18.03.11 (Schlussabstimmung – Vote final)
Text des Erlasses (BBl 2011 2765)
Texte de l'acte législatif (FF 2011 2587)

Schwander Pirmin (V, SZ): Ich bitte Sie namens der SVP-Fraktion, dem Antrag der Minderheit Heer auf Nichteintreten zuzustimmen.
Die unterbreitete Vorlage fokussiert auf die Computerkriminalität, auf das Strafprozessrecht im Bereich der elektronischen Beweismittel und auf das Rechtshilfeverfahren. Warum in diesem Zusammenhang das Zusatzprotokoll gegen Rassismus und Fremdenfeindlichkeit nicht behandelt werden soll, ist mehr als fragwürdig, denn das hängige Revisionsverfahren hat mit Computerkriminalität nichts zu tun, weswegen das genannte Zusatzprotokoll auch zur Ratifizierung hätte vorgelegt werden können. Offenbar folgt die Aufteilung politischem Kalkül. Eine solche Salamitaktik tragen wir nicht mit. In der Botschaft hält der Bundesrat denn auch fest: «Jedoch darf die Bedeutung des Übereinkommens über die Cyberkriminalität zum heutigen Zeitpunkt nicht überschätzt werden.» Wir hätten also Zeit gehabt, auch über das genannte Zusatzprotokoll zu befinden. Im Übrigen ist die Vorlage schlecht vorbereitet und nicht durchdacht. Sie spricht von neuen Herausforderungen und von grenzüberschreitender Bekämpfung der Cyberkriminalität. Dazu zwei Punkte:
1. Die Konvention stammt aus dem Jahre 2001 und ist damit schon lange veraltet, wissen wir doch alle hier im Saal um die Quantensprünge, welche die Elektronik in den letzten zehn Jahren erlebt hat.
2. Wie wollen wir die Kriminalität über die Grenzen hinweg bekämpfen, wenn keine Grenze vorhanden ist? Internet ist ein weltweiter Freiraum. Entweder wir zensurieren diesen lokal, oder wir setzen klare Grenzen bei den Internet-Service-Providern. Beides ist nicht vorgesehen.
In der Vorlage werden sehr viele Vorbehalte aufgeführt. Die Frage, ob diese Vorbehalte langfristig aufrechterhalten werden können, wurde in der Kommission wie folgt beantwortet: «Es gibt keine Klausel im Vertrag, die sagt, dass ein Staat periodisch überprüfen muss, ob er sie noch aufrechterhält.» In Artikel 43 Absatz 2 der Konvention steht aber etwas ganz anderes: «Eine Vertragspartei, die einen Vorbehalt nach Artikel 42 angebracht hat, nimmt diesen Vorbehalt ganz oder teilweise zurück, sobald die Umstände dies erlauben.» Gemäss Artikel 43 Absatz 3 erkundigt sich der Generalsekretär des Europarates in regelmässigen Abständen bei den Vertragsparteien nach den Aussichten für eine Rücknahme eines Vorbehalts.
Mit dem revidierten Strafrechtsartikel wird die Grundlage dafür geschaffen, Tätigkeiten im Bereich der Computersicherheit zu kriminalisieren. Mit dem neuen Rechtshilfeverfahren bei elektronischen Verkehrsdaten schaffen wir die Grundlage dafür, dass man auch fiskalische Auskünfte erlangen kann, die dann für Steuerverfahren missbraucht werden; denn nach Artikel 25 Absatz 4 des Übereinkommens darf die ersuchte Vertragspartei die Rechtshilfe nicht mit der Begründung verweigern, das Ersuchen betreffe eine fiskalische Straftat. Da nützen alle gegenteiligen Erklärungen der Verwaltung und des Bundesrates nichts.
Ich fasse zusammen: Das Übereinkommen des Europarates über die Cyberkriminalität ist veraltet, es schafft selbst gemäss Botschaft des Bundesrates keinen eigentlichen Mehrwert, es verwässert einmal mehr den Grundsatz der doppelten Strafbarkeit, und es stiftet zusätzlich Verwirrung in der internationalen justiziellen Zusammenarbeit in Strafsachen. Wir haben keine Abgrenzung zu Schengen, zu Interpol, zu bilateralen Polizeiabkommen, zu Europol, zu Eurojust usw. Das Übereinkommen unterstützt das Bestreben der EU, den automatischen Informationsaustausch in allen Belangen voranzutreiben.
Aufgrund all dieser Ausführungen bitte ich Sie, der Minderheit Heer zu folgen.

Le président (Germanier Jean-René, président): Le groupe socialiste soutient la proposition de renvoi de la minorité Sommaruga Carlo.

Sommaruga Simonetta, Bundesrätin: Die Europaratskonvention über die Cyberkriminalität ist das einzige internationale Übereinkommen, das sich mit Computerkriminalität und Netzwerkdelikten befasst. Sie ist vor sechs Jahren in Kraft getreten, und sie ist mittlerweile von dreissig Vertragsstaaten ratifiziert worden. Diese haben sich verpflichtet, ihre Gesetzgebung den Anforderungen der modernen Kommunikationstechnologie anzupassen. Auch wenn die Schweiz keinen grossen gesetzgeberischen Anpassungsbedarf hat, haben wir auch ein Interesse daran, dass möglichst viele Staaten diese Europaratskonvention über die Cyberkriminalität ratifizieren, weil Cyberkriminalität keine Landesgrenzen kennt.
Wo steht nun die Schweiz im Hinblick auf die Anforderungen der Konvention? Das Schweizer Computerstrafrecht und die Bestimmungen gegen Kinderpornografie genügen den Erfordernissen des Vertrags über weite Strecken. Es gibt aber in anderen Bereichen doch einen Anpassungsbedarf, z. B. beim sogenannten Hacking-Tatbestand, bei dem das unbefugte Eindringen in einen Computer unter Strafe gestellt wird. Hier wird eine Vorverlagerung der Strafbarkeit vorgeschlagen. Diese Ausweitung muss aber massvoll geschehen. Strafbar macht sich neu, wer Passwörter oder andere Daten zugänglich macht und weiss, dass diese für Hacking benutzt werden sollen. Im prozessualen Bereich genügt die schweizerische Strafprozessordnung den Anforderungen des Übereinkommens. Sie ist ja gerade erst am 1. Januar 2011 in Kraft getreten.
Eine zweite Anpassung der Gesetze ist bei der Rechtshilfe nötig. Die Schweizer Behörden sollen die Möglichkeit erhalten, elektronische Verkehrsdaten vor Abschluss eines Rechtshilfeverfahrens an ausländische Behörden weiterzugeben. Diese Möglichkeit wird jedoch auf ganz besondere Fälle eingeschränkt. Die Rechte der betroffenen Personen bleiben also angemessen geschützt, und von einer Verletzung der Grundrechte kann in keiner Art und Weise die Rede sein.
Ich möchte noch ein Wort zum Übereinkommen generell sagen: Die Erfahrungen aus der letzten Staatenkonferenz in

Paris haben gezeigt, dass die Staaten bei der Umsetzung des umfassenden und zuweilen – das stimmt – recht komplizierten Übereinkommens nach wie vor stark gefordert sind. Entsprechend haben sie von der Möglichkeit von Erklärungen und Vorbehalten Gebrauch gemacht. Wichtig ist, dass die Staaten den Kerngehalt der Konvention angemessen umsetzen und berücksichtigen. Dadurch werden die positiven Effekte des Vertrags in den kommenden Jahren weiter zunehmen. Dies sind Wirkungen, aus denen unser Land als Mitgliedstaat ebenfalls seinen Nutzen ziehen wird. Ein schneller und effizienter Austausch von Informationen liegt nämlich auch im schweizerischen Interesse.
Ich bitte Sie in diesem Sinne, dem einstimmigen Beschluss des Ständerates sowie dem Beschluss der Mehrheit Ihrer Kommission zuzustimmen und auf das Geschäft einzutreten.
Ich komme jetzt auch gleich noch zum Rückweisungsantrag: Schon bei der Ratifikation der Europaratskonvention war vorgesehen, dass Erklärungen oder Vorbehalte möglich sein sollen. Die Länder sollen nicht dazu verpflichtet werden, bewährte Regelungen im Bereich der Bekämpfung der Cyberkriminalität über Bord zu werfen. Der zwingende Kernbereich der umfangreichen Konvention ist aber nach wie vor beachtlich. Es geht darum, dass jeder Staat die Strafbarkeit und die Rechtshilfe in diesem Bereich garantieren kann. Werfen wir einen Blick über die Landesgrenzen hinaus, stellen wir fest, dass Vertragsstaaten wie Frankreich, Deutschland, Norwegen, Dänemark, Finnland, Portugal, Island und die Vereinigten Staaten eine Ratifikation mit zahlreichen Erklärungen und Vorbehalten vorgenommen haben. Keine Einschränkungen vorgenommen haben im westeuropäischen Umfeld ausschliesslich Italien und die Niederlande.
Ich möchte Sinn und Zweck der Vorbehalte aufzeigen, und zwar an einem konkreten Beispiel: Das Übereinkommen bestimmt, dass Staaten die Überwachung von Verkehrsdaten in Echtzeit vorsehen müssen. Sie können aber die betreffenden Straftaten mittels Vorbehalt angemessen einschränken, und der Bundesrat schlägt in diesem Zusammenhang vor, sich am geltenden Recht zu orientieren und eine solche Überwachung auf Verbrechen und Vergehen zu beschränken. Eine reine Übertretung würde eine solche Massnahme als unverhältnismässig erscheinen lassen.
Die jährlich stattfindende Konferenz der Vertragsstaaten, an welcher die Schweiz bereits teilnehmen konnte, hat zudem gezeigt, dass die abgegebenen Erklärungen und Vorbehalte der Staaten ohne Einschränkung akzeptiert werden und dass keine Versuche gestartet wurden, einen Rückzug zu bewirken. Der Mehrwert des Übereinkommens liegt in der Umsetzung seines Kerngehalts durch eine möglichst grosse Zahl von Staaten und nicht in einer wortwörtlichen Übernahme seines Inhalts.
Ich möchte mich noch kurz zum Vorwurf äussern, man würde mit dieser Konvention den Grundsatz der doppelten Strafbarkeit verwässern. Ich muss dem widersprechen. Das Übereinkommen des Europarates über die Cyberkriminalität ändert nichts für die Schweiz, was die doppelte Strafbarkeit betrifft. Das wollte ich doch noch festhalten.
Ich ersuche Sie, der Mehrheit Ihrer Kommission zu folgen, auf die Vorlage einzutreten und den Rückweisungsantrag abzulehnen. Damit kann die Schweiz noch in diesem Jahr Vertragsstaat werden.

Rickli Natalie Simone (V, ZH): Frau Bundesrätin, im Gegensatz zu meiner Partei tendiere ich zu Eintreten und Unterstützung dieses Übereinkommens. Ich habe eine Frage betreffend die umgehende Weitergabe von Verkehrsdaten: Wird die betroffene Person auch im Falle der späteren Einstellung des Verfahrens durch die Behörden darüber in Kenntnis gesetzt, dass Verkehrsdaten an ausländische Behörden übermittelt worden sind?

Sommaruga Simonetta, Bundesrätin: Ja, ich kann das bestätigen. Sobald es die Situation erlaubt, spätestens aber bevor die Strafuntersuchung abgeschlossen ist oder eingestellt wird, muss die betroffene Person über die erfolgte Übermittlung benachrichtigt werden. Die betroffene Person geniesst genau den gleichen Schutz, wie wenn das Strafverfahren in der Schweiz geführt worden wäre.

Schwander Pirmin (V, SZ): Frau Bundesrätin, wer entscheidet, ob ein Vorbehalt aufgehoben wird oder nicht: der Bundesrat oder das Parlament?

Sommaruga Simonetta, Bundesrätin: Ich gehe davon aus, dass das Parlament diesen Entscheid fällt. Aber ich habe vorher ausgeführt, dass zahlreiche Staaten Vorbehalte gemacht haben. Es ist nicht festzustellen, dass die Erklärungen und Vorbehalte infrage gestellt werden – weil andere Staaten das eben auch gemacht haben. Das gemeinsame Interesse besteht darin, dass möglichst viele Staaten den Kerngehalt dieser Konvention umsetzen. Von daher sollten Sie sich hier keine Sorgen machen und auch keine Befürchtungen haben. Es ist auch die Meinung des Bundesrates, diese Vorbehalte zu machen. Es gibt keinen Hinweis darauf – auch von den Vertragsstaaten nicht –, dass diese Vorbehalte aufgehoben werden sollten.

von Rotz Christoph (V, OW): Frau Bundesrätin, ich habe eine Frage in Bezug auf die Verkehrsdaten und darauf, wie Verkehrsdaten Personen zugeordnet werden können. Es ist ja klar – ich bitte Sie, das nochmals zu bestätigen –, dass die Verkehrsdaten keine Inhalte umfassen dürfen. Ist es auch so, dass die Verkehrsdaten, die an ausländische Behörden geliefert werden, faktisch anonymisiert sind, also nicht mit einer Person in Verbindung sind?

Sommaruga Simonetta, Bundesrätin: Ich kann Ihnen bestätigen, dass ausschliesslich Verkehrsdaten, also keine Inhalte, geliefert werden. Es findet in diesem Zusammenhang zwar keine Anonymisierung statt, doch ist eine solche auch nicht notwendig, weil die gelieferten Daten keine Rückschlüsse auf eine Person in der Schweiz zulassen. Ich gehe davon aus, dass es das ist, worüber Sie sich Sorgen machen. Es sind also keine Rückschlüsse auf eine Person in der Schweiz möglich.

Schmid-Federer Barbara (CEg, ZH), für die Kommission: Wir von der Kommissionsmehrheit haben heute früh in der Eintretensdebatte zum Eintreten gesprochen, wir haben uns aber noch nicht über die Rückweisung geäussert. Mit 16 zu 5 Stimmen bei 5 Enthaltungen empfiehlt Ihnen die Kommission, den Rückweisungsantrag abzulehnen. Im Jahr 2001 hat der Bundesrat das Übereinkommen des Europarates unterzeichnet und dann eben sehr lange gebraucht, um eine Botschaft vorzulegen. Es ist der Motion Glanzmann 07.3629 von 2007 zu danken, dass wir heute diese Botschaft haben.
Der erste wichtige Grund, warum die Rückweisung abzulehnen ist, ist eben, dass wir uns beeilen möchten. Der zweite Grund ist, dass die Minderheit Sommaruga Carlo mit ihrem Rückweisungsantrag alle Vorbehalte weghaben möchte. Wenn ich sage «alle», dann ist es halt so, dass nicht alle Vorbehalte gut und nicht alle schlecht sind. Tatsächlich hat man in der Vernehmlassung und haben auch wir von der Mehrheit gewisse Vorbehalte gefunden, die durchaus diskutabel sind, namentlich die Vermarktung von Pornografie im Internet, die die Schweiz nach wie vor für Sechzehn- und Siebzehnährige als Akteure zulassen will. Wir haben dann aber auf einen Einzelantrag verzichtet, weil der Bundesrat im Zusammenhang mit der Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung diese Sachfrage noch einmal vertieft prüfen will. Zudem kann man diesen Aspekt auf dem normalen Gesetzgebungsprozess dann anpassen.
Wie bereits gesagt, lehnt die Mehrheit den Rückweisungsantrag auch deshalb ab, weil er alle Vorbehalte ausräumen will. So wäre z. B. auch der Vorbehalt in Artikel 6 betroffen, wo es um die Herstellung von Tools geht. Hierzu hat die Schweiz einen Vorbehalt vorgesehen, weil damit nach Auffassung der IT-Industrie die Gefahr bestünde, dass die Entwicklung von spezifischen Programmen und Vorrichtungen behindert würde.

Zusammenfassend bitte ich Sie im Namen der Mehrheit von 16 zu 5 Stimmen bei 5 Enthaltungen, den Rückweisungsantrag abzulehnen, weil wir eine rasche Ratifizierung wünschen und weil es nicht im Sinne der Vorlage ist, alle Vorbehalte aus dem Weg zu räumen.

Lüscher Christian (RL, GE), pour la commission: Je dirai quelques mots d'abord sur la proposition de non-entrée en matière de la minorité Heer. Contrairement à ce qui vous a été dit, il n'y a absolument aucune remise en question des droits démocratiques tels qu'ils existent dans notre Confédération. Le Code de procédure pénale est tout à fait applicable pour tout ce qui concerne la procédure, et donc il n'y a absolument aucune crainte à avoir de ce côté-là. Il n'y a aucune remise en question du droit en vigueur. En réalité, il y a plutôt une mise à niveau du droit matériel dont nous devrions nous réjouir tous ici puisque nous avons tous le souci de lutter contre la cybercriminalité et que l'adhésion à cette convention, en l'occurrence l'approbation et la mise en oeuvre de cette convention, sont l'occasion de renforcer notre droit fédéral et les moyens de lutter contre la cybercriminalité.
En ce qui concerne la proposition défendue par la minorité Sommaruga Carlo, qui demande le renvoi de ce projet au Conseil fédéral pour que les réserves soient supprimées, je pense que c'est à tort que cette proposition est faite. D'ailleurs elle a été balayée par la Commission des affaires juridiques. Je pense que le Conseil fédéral a eu tout à fait raison de procéder à une vérification des dispositions de la convention pour être sûr qu'elles correspondent à la vision que nous avons du droit pénal. En ce qui concerne par exemple les collectes de données informatiques en temps réel, le Conseil fédéral a dit que ces dispositions – les articles 20 et suivants de la convention – ne s'appliqueraient qu'en cas de crimes et de délits. Donc, le Conseil fédéral a voulu préserver un principe important du droit suisse, qui est le respect de la sphère privée.
Il y a un autre exemple où le Conseil fédéral a fait une réserve – étant précisé que ces réserves sont expressément autorisées par la convention. Le Conseil fédéral a voulu faire une réserve s'agissant d'une disposition assez particulière, qui voulait que la diffusion sur Internet de pornographie infantile soit aussi punissable lorsqu'un adulte apparaît comme un mineur. Alors, évidemment, c'est une disposition extrêmement confuse. D'abord, un adulte qui apparaît pour un mineur n'est pas mineur puisqu'il est adulte; et quelles sont les circonstances dans lesquelles on devrait considérer qu'un majeur a voulu se faire passer pour un mineur? A juste titre, le Conseil fédéral a voulu que la convention soit comprise, applicable et ne laisse pas des zones d'ombre ou des confusions comme cela pourrait être le cas.
Il convient de préciser qu'en fonction de l'évolution du droit suisse, ces déclarations et réserves pourront être modifiées, voire retirées. Il est exact – et Monsieur Schwander l'a dit tout à l'heure – que l'article 43 alinéa 3 de la convention permet au secrétaire général du Conseil de l'Europe de demander à la Suisse si ces réserves peuvent effectivement être retirées ou modifiées. Personne ne l'a encore fait jusqu'à maintenant. Et, donc, il n'y a absolument aucun risque que cela soit fait.
J'aimerais aussi vous dire que le Conseil des Etats, qui a analysé ces réserves, a considéré, à l'unanimité, qu'elles étaient applicables et qu'il n'y a eu absolument aucune remise en question par le Conseil des Etats, qui a accepté les réserves telles qu'elles existent dans le message du Conseil fédéral.
Nous demandons donc, au nom de la majorité de la commission, de rejeter la proposition de renvoi de la minorité Sommaruga Carlo au Conseil fédéral.

Le président (Germanier Jean-René, président): Nous votons d'abord sur la proposition de non-entrée en matière de la minorité Heer.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 10.058/5066)
Für Eintreten ... 112 Stimmen
Dagegen ... 36 Stimmen

Le président (Germanier Jean-René, président): Nous votons maintenant sur la proposition de renvoi de la minorité Sommaruga Carlo.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 10.058/5067)
Für den Antrag der Minderheit ... 57 Stimmen
Dagegen ... 91 Stimmen

Bundesbeschluss über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität
Arrêté fédéral portant approbation et mise en oeuvre de la convention du Conseil de l'Europe sur la cybercriminalité

Detailberatung – Discussion par article

Titel und Ingress, Art. 1, 2 Einleitung
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Titre et préambule, art. 1, 2 introduction
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 2 Ziff. 1 Art. 102 Abs. 2
Antrag der Minderheit
(Sommaruga Carlo, Daguet, Jositsch, Leutenegger Oberholzer)
Handelt es sich dabei um eine Straftat nach den Artikeln 143, 143bis, 144bis, 147, 260ter, 260quinquies ...

Art. 2 ch. 1 art. 102 al. 2
Proposition de la minorité
(Sommaruga Carlo, Daguet, Jositsch, Leutenegger Oberholzer)
En cas d'infraction prévue aux articles 143, 143bis, 144bis, 147, 260ter, 260quinquies ...

Sommaruga Carlo (S, GE): Avec la minorité que je représente, je vous propose d'étendre la responsabilité pénale des personnes morales aux actes délictuels en matière de cybercriminalité.
En droit pénal suisse, le principe qu'une personne morale ne peut pas commettre d'infractions a prévalu pendant longtemps comme un dogme. Seules peuvent se voir reprocher des infractions et, le cas échéant, se faire condamner, des personnes physiques, selon ce principe.
Mais ce principe a été remis en cause à travers des conventions internationales sur la lutte contre le terrorisme, contre le crime organisé et contre la corruption, émanant notamment du Conseil de l'Europe, comme la convention qui est aujourd'hui en train d'être discutée.
En droit suisse, la responsabilité pénale pour des personnes morales est réglée à l'article 102 du Code pénal. Elle pose le principe de la subsidiarité de la responsabilité pénale des personnes morales: un crime ou un délit ne peut être imputé à une société que s'il ne peut être imputé à une personne physique. Toutefois, la personne morale peut être condamnée indépendamment de la personne physique dans le cas d'une procédure parallèle lorsqu'il s'agit d'un crime ou d'un délit relatif à la criminalité organisée, au financement du terrorisme, au blanchiment d'argent, à la corruption d'agents publics et en cas d'actes de concurrence déloyale. La dernière extension de la responsabilité pénale directe des personnes morales est intervenue en 2005 lors de l'approbation et de la mise en oeuvre de la Convention pénale du Conseil de l'Europe sur la corruption et de son protocole additionnel. Aujourd'hui, je vous invite à procéder de la même manière que l'on a procédé en 2005 en ce qui concerne les infractions figurant aux articles 143, 143bis et 144bis CP, relatives

à la cybercriminalité. Certes, la convention que nous discutons aujourd'hui n'oblige pas un Etat membre à procéder de la sorte. Toutefois, cet acte s'inscrit dans la logique d'harmonisation du droit pénal en matière de criminalité internationale et va aussi dans le sens du renforcement de la répression d'actes commis par des personnes morales.

En effet, il est juste dans notre société actuelle, où les personnes morales jouent un rôle économique primordial, de sanctionner les sociétés elles-mêmes, indépendamment de leurs dirigeants ou de leurs employés, pour des actes délictuels ou criminels qui résultent d'une organisation interne défaillante. Il n'y a aucune raison de traiter moins bien et de manière différente la cybercriminalité par rapport à la criminalité organisée, la corruption ou encore des actes de concurrence déloyale. Bien au contraire, dans le domaine de la cybercriminalité, il faut aussi responsabiliser l'entreprise en tant que telle pour qu'elle puisse finalement aussi répondre et avoir sur elle un effet de prévention.

L'objection à l'extension de la responsabilité pénale des entreprises, au-delà de l'ancien dogme émoussé selon lequel une personne morale ne peut commettre d'infraction, est que la Suisse dispose d'un dispositif légal civil et administratif suffisant qui pourrait combler l'absence de condamnation possible de la personne morale. Mais c'est oublier la nature spécifique de la norme et de la sanction pénale, que la majorité nous rappelle d'ailleurs sans cesse dans d'autres domaines du droit. Par ailleurs, la norme pénale prolonge la prescription, ce qui permet de mieux protéger les victimes d'attaques cybercriminelles, même devant la justice civile.

Je vous invite donc à soutenir la proposition de la minorité.

Jositsch Daniel (S, ZH): Beim Minderheitsantrag Sommaruga Carlo geht es um das Thema der strafrechtlichen Unternehmenshaftung. Bei der strafrechtlichen Unternehmenshaftung haben wir zwei Konzepte: Das eine ist, in Absatz 1, die subsidiäre und das andere, in Absatz 2, die originäre Unternehmenshaftung. Die subsidiäre Unternehmenshaftung kommt nur dann zum Tragen, wenn kein Individuum für ein bestimmtes Delikt verantwortlich gemacht werden kann. Die originäre Unternehmenshaftung hingegen ist die eigentliche Unternehmenshaftung, die unabhängig davon, ob ein Individuum zur Verantwortung gezogen werden kann, zum Tragen kommt.

Warum haben wir diese beiden Konzepte? Es handelt sich hier um eine gesetzgeberische Schlaumeierei. Absatz 1 ist nichts anderes als eine Placebo-Bestimmung, die überhaupt keine Wirkung entfaltet. Der Gesetzgeber, also wir, hat diese Bestimmung damals erlassen, weil man international den Eindruck erwecken wollte, man kämpfe gegen Fälle der Unternehmensstrafbarkeit. In Tat und Wahrheit hat man das aber nur in ganz wenigen Fällen gemacht, nämlich gemäss Absatz 2. Das können wir heute – leider – nicht ändern. Wir müssen uns damit abfinden, dass wir uns selbst an der Nase herumgeführt haben.

Allerdings geht es nun um die Frage, welche Ausnahmebestimmung oder welche Strafnormen nach Absatz 2 der originären Unternehmenshaftung unterliegen sollen, damit eben wirklich auch die Unternehmensstrafbarkeit erfasst wird. Hier gibt es verschiedene Delikte, die bereits in Absatz 2 erwähnt sind. Es sind ganz wenige: Korruption, Terrorismusfinanzierung, Geldwäscherei und noch ein paar wenige mehr.

Es stellt sich nun die Frage, ob wir die Delikte, die zur Cyberkriminalität gehören, hier auch miterfassen sollen. Der Minderheitsantrag schlägt Ihnen vor, dass diese Delikte zur Cyberkriminalität auch unter Absatz 2 miterfasst werden. Das hätte zur Folge, dass die Unternehmen, die mitbeteiligt sind, die aufgrund ihrer organisatorischen Mängel verantwortlich sind, dass solche Delikte verübt werden können – das ist die ganze Industrie, die da mitbeteiligt ist, die die entsprechenden Plätze im Internet zur Verfügung stellt, Provider usw. –, auch strafrechtlich miterfasst werden können. Das hat zur Folge, dass wir diese Normen überhaupt erst griffig machen, und das hat auch zur Folge, dass wir der Konvention überhaupt zu einer gewissen Schlagkraft verhelfen.

Deshalb bitte ich Sie im Namen der SP-Fraktion, dass Sie den Minderheitsantrag Sommaruga Carlo unterstützen.

Sommaruga Simonetta, Bundesrätin: Das geltende schweizerische Recht im Bereich der Strafbarkeit der Unternehmung entspricht den Anforderungen von Artikel 12 der Europaratskonvention. Unsere subsidiäre Verantwortlichkeit geht zum Teil noch weiter und stellt sicher, dass Straftaten, die im Rahmen einer Unternehmung begangen werden, auch dann nicht ungesühnt bleiben, wenn die Tat aufgrund der mangelhaften Organisation der Firma nicht einem Individuum zugeordnet werden kann. Das Übereinkommen lässt neben dem Strafrecht alternativ einen zivilrechtlichen und einen administrativen Lösungsansatz zu. Die Schweizer Rechtsordnung stellt solche zivilrechtlichen Instrumente zur Verfügung, damit Unternehmen, zu deren Gunsten ein leitender Angestellter Straftaten verübt hat, für den Schaden haftbar gemacht werden können. Zudem kennt unser Recht verschiedene Massnahmen im Bereich der verwaltungsrechtlichen Haftung. So können gegen Unternehmen, die einer Aufsicht unterstellt sind, entsprechende Sanktionen ausgesprochen werden, oder es können ihnen Bewilligungen entzogen werden.

Der Bundesrat hat es als unangemessen erachtet, im Zusammenhang mit der Umsetzung dieses Übereinkommens eine umfassende primäre Strafbarkeit der Unternehmung vorzuschlagen. Dieser Befund wurde im Rahmen der Vernehmlassung mehrheitlich begrüsst. Die von der Konvention ins Auge gefassten Tatbestände sind, anders als Tatbestände in den Bereichen Korruption, Geldwäscherei und organisierte Kriminalität, auch in praktischer Hinsicht keine Delikte, bei welchen es naheliegend ist, dass sie zugunsten oder innerhalb einer Unternehmung begangen werden. Eine Erweiterung des Deliktkatalogs mit den Straftaten gemäss Konvention wäre weitgehend deklaratorischer Natur und würde unweigerlich zur Frage führen, weshalb andere, ebenso relevante Straftatbestände des Schweizer Rechts keinen Eingang finden.

Ich ersuche Sie daher, von einer Ausweitung der Strafbarkeit der Unternehmung abzusehen und den Minderheitsantrag abzulehnen.

Schmid-Federer Barbara (CEg, ZH), für die Kommission: Wie Ihnen Herr Jositsch richtig erklärt hat, gibt es für Unternehmen eine primäre Haftung, die nur bei einer Ausnahme von Tatbeständen wie Korruption oder Geldwäscherei angewandt wird. Eine sekundäre Haftung für Unternehmen bezieht sich auf alle Verbrechen und Vergehen, jedoch muss ein Organisationsverschulden der Unternehmung vorliegen.

Was die Minderheit Sommaruga Carlo möchte, ist, den sogenannten Hacker-Artikel zur primären Haftung hinzufügen. Die Kommission hat nicht sehr lange darüber diskutiert. Sie lehnt diesen Antrag ab und bleibt beim geltenden Recht, und zwar schlicht und einfach, weil eine solche Ausweitung aus praktischer Sicht keinem Bedürfnis entspricht, weil die Konvention eine solche Ausweitung nicht explizit verlangt und weil das Übereinkommen es den Mitgliedstaaten überlässt, wie sie vorgehen wollen, und weil wir mit dem heutigen System zufrieden sind.

Lüscher Christian (RL, GE), pour la commission: Il est regrettable que le groupe socialiste saisisse l'occasion de la mise en oeuvre de cette convention pour manifester une fois de plus sa méfiance et son désamour envers ceux qui, dans notre pays, créent des emplois en fondant des entreprises ou des sociétés.

Comme cela a été dit, la responsabilité pénale primaire est celle des personnes physiques, puis subsidiairement celle des entreprises. C'est un principe qui est inscrit dans le droit pénal suisse et également dans la convention que nous vous proposons d'approuver et de mettre en oeuvre aujourd'hui puisque, à l'article 12 alinéa 3, la convention précise bien que selon les principes juridiques de la partie concernée, en l'occurrence ici la Suisse lorsqu'elle aura mis en oeuvre cette convention, la responsabilité d'une personne

morale pourra être pénale, civile ou administrative. Or, sans modifier la loi, nous avons déjà aujourd'hui les mécanismes juridiques qui permettent, lorsqu'une personne physique a été reconnue coupable, de poursuivre son employeur au civil, le cas échéant, et que celui-ci soit tenu de payer des dommages et intérêts.
La proposition de la minorité ne repose donc sur aucune logique parce que l'on ne voit pas pourquoi aujourd'hui on intégrerait dans la responsabilité primaire des entreprises les infractions qui concernent la cybercriminalité, à savoir celles punissables conformément aux articles 143 et suivants du Code pénal, et non pas d'autres infractions punies en vertu du Code pénal, qui seraient, le cas échéant, dans le même chapitre du Code pénal concernant les infractions contre le patrimoine. Cela n'a aucune logique et il est presque regrettable que vous polluiez finalement cette convention que nous adoptons aujourd'hui par des tentatives politiques maladroites de changer les principes du droit pénal en vigueur.
C'est la raison pour laquelle, à l'instar de la très grande majorité de la commission, je vous demande de rejeter la proposition de la minorité Sommaruga Carlo.

Le président (Germanier Jean-René, président): Le groupe libéral-radical rejette la proposition de la minorité.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 10.058/5068)
Für den Antrag der Minderheit ... 27 Stimmen
Dagegen ... 124 Stimmen

Art. 2 Ziff. 1 Art. 143bis
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Schmid-Federer, Amherd, Hochreutener, Ingold, Roux, von Graffenried)
Abs. 1
Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes Datenverarbeitungssystem eindringt, wird ...

Art. 2 ch. 1 art. 143bis
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Schmid-Federer, Amherd, Hochreutener, Ingold, Roux, von Graffenried)
Al. 1
Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui est ...

Le président (Germanier Jean-René, président): La proposition de la minorité Schmid-Federer est présentée par Madame Ingold.

Ingold Maja (CEg, ZH): Der Bundesrat verlangt, dass ein Hacker dann bestraft wird, wenn er in ein besonders gesichertes Datenverarbeitungssystem eindringt. Dies ist auch im geltenden Recht so geschrieben. Aber dieser Passus ist zu einer Zeit geschrieben worden, 1995, als der Gebrauch des Internets noch eine Ausnahme war. Die weltweite Verknüpfung der Computersysteme war damals noch kein Thema. Die mobile Telefonie für alle, der ständig mit dem Internet verbundene PC zu Hause und das nicht selten offene WLAN an jeder Strassenecke kamen viel später. Der Gebrauch des Internets ist heutzutage auch ohne technische Kenntnisse möglich. Viele Programme sind so programmiert, dass sie sich selber installieren können und die nötigen Parameter selber konfigurieren.
Mit der Version Bundesrat/Mehrheit operiert man mit technischen Vorrichtungen, welche längst der Vergangenheit angehören. Damit manövriert sich die Schweiz unnötig ins Abseits. Das Internet ist zu einem tragenden Infrastrukturbestandteil unserer Wirtschaft geworden, aber auch zu einem festen Bestandteil des Grundrechtes Informationsfreiheit. Das Internet wird bekanntlich auch von Jugendlichen benutzt. Aus all diesen Gründen muss bereits unbefugtes Eindringen in ein Datenverarbeitungssystem unter Strafe gestellt werden, was sich übrigens auch für die Wirtschaft als lohnend erweisen würde. Vergleicht man diesen Passus in der Fassung der Mehrheit mit dem Hausfriedensbruch generell, könnte man sagen, dass man die Fenster immer sichert. Das kann es ja nicht sein! Mit dem Einschub bezüglich der besonderen Sicherung arbeitet man ausschliesslich den Kriminellen in die Hände. Wir schaffen hier eine Lücke, die die Schweiz für Täter attraktiv macht.
Der Bundesrat argumentiert, in der Rechtsprechung habe man bisher kein Problem damit gehabt. Es wird aber häufig gar keine Strafanzeige eingereicht, daher hat man auch keine grosse Praxis. Das Anzeigeverhalten in diesem Bereich ist sehr zurückhaltend, da man einen Angriff gar nicht automatisch oder leicht erkennen kann. Überdies geht der Betroffene in der Regel davon aus, dass die Täter irgendwo aus dem Dunkeln heraus operieren und nur schwer gefasst werden können. Das kann aber kein Argument dafür sein, das unbefugte Eindringen in fremde Daten nur bei besonderer Sicherung zu verfolgen.
Daher bitte ich Sie, die Minderheit zu unterstützen.

Le président (Germanier Jean-René, président): Le groupe socialiste soutient la proposition de la majorité.

Sommaruga Simonetta, Bundesrätin: Die Konvention bestraft das unbefugte Herstellen, Abgeben, Verschaffen, Einführen oder Verbreiten von Daten oder Programmen, die zur Begehung einer Computerstraftat gebraucht werden. Das Schweizer Strafrecht kennt in diesem Bereich den sogenannten Hacking-Tatbestand, und hier stossen wir auf eine Lücke des Schweizer Rechts. Nicht strafbar macht sich in der Regel derjenige, der ein Passwort, einen Code oder ein Hacking-Programm mit der Absicht weiterverbreitet, dass dieses künftig für ein nicht genau bestimmtes Delikt gebraucht wird. Der Bundesrat schlägt nun vor, auch das vorsätzliche Verbreiten von solchen Programmen und Daten unter Strafe zu stellen. Es geht bei dieser Anpassung, welche vom Ständerat und der Mehrheit Ihrer Kommission unterstützt wird, also nicht darum, die Strafbarkeit für Sicherheitstests oder für die Ausbildung von IT-Spezialisten einzuführen. Der verantwortungsvolle Umgang mit Zugangscodes oder entsprechenden Programmen und Tools bleibt nach wie vor straffrei.
Lassen Sie mich jetzt noch ein Wort zum Antrag der Minderheit Ihrer Kommission sagen, mit dem der Verzicht auf das Kriterium der Sicherung verlangt wird. Die Rechtsprechung hat bisher keinen Hinweis darauf geliefert, dass das geltende Recht zu einer ungewollten Einschränkung der Strafbarkeit geführt hätte. An die Sicherung werden keine hohen Anforderungen gestellt. Es ist insbesondere nicht notwendig, dass ein Passwort oder ein Zugangscode besonders kompliziert gemacht werden. Strafbar macht sich auch, wer durch einen Trick oder durch Ausprobieren auf gesicherte Daten zugreift. Die besondere Sicherung – der französische Text spricht von «spécialement protégé» – ist in diesem Kontext wichtig und stellt sicher, dass der Täter eine für ihn erkennbare Schranke überwindet. Ansonsten ist die Illegalität des Abrufens von Daten über ein Netzwerk in aller Regel nicht klar ersichtlich. Private und Firmen speichern ihre Daten häufig nicht in einem örtlich genau definierten Medium z. B. an ihrem Sitz. Sie bedienen sich stattdessen eines Hosting-Providers oder betreiben sogenanntes Cloud Computing, bei dem Bruchstücke ihrer Daten nicht fix gespeichert sind.
Das Internet ist ein dezentral gesteuerter Raum. Die Entwicklungen der letzten Tage in Nordafrika haben dies eindrücklich gezeigt. Unter diesen Voraussetzungen ist es in der virtuellen Welt von grosser Bedeutung, dass das Verbot eines Zutritts klar erkennbar und definiert ist. Das lässt sich am besten mit einer Zugriffssicherung erreichen, welche für

jeden Benutzer klar erkennbar ist und nicht ohne Weiteres überwunden werden kann. Der Antrag der Minderheit ist aus diesen Gründen abzulehnen.
Ich ersuche Sie, dem Bundesrat, dem Ständerat sowie der Mehrheit Ihrer Kommission zuzustimmen.

Schmid-Federer Barbara (CEg, ZH), für die Kommission: Der Bundesrat legt fest, dass ein Hacker dann bestraft wird, wenn er in ein besonders gesichertes Datensystem eindringt. Dies ist auch im geltenden Recht so. Die Minderheit Schmid-Federer verlangt, es sei auf den Wortlaut «besonders gesichert» zu verzichten, weil dies mit der heutigen Technik – Beispiel WLAN – gar nicht mehr möglich sei und weil diese Bestimmung vor der Internetzeit geschrieben worden sei.
Die Mehrheit bittet Sie, beim Beschluss des Bundesrates zu bleiben. Sie argumentiert, in der Rechtsprechung sei bislang kein Hinweis gefunden worden, dass dieses Kriterium der besonderen Sicherung zu einer ungewollten Einschränkung der Strafbarkeit geführt habe. Dort, wo es zu einer Anzeige gekommen sei, sei auch bestraft worden. Gemäss Mehrheit ist es wichtig, dass ein Täter weiss, dass er in einen geschützten Raum eindringt. Nur so kann er wissen, dass er sich strafbar macht. Im Sinne der Mehrheit gilt ein Passwort oder ein Code als besonders gesichert. Es wird nicht verlangt, dass der Code besonders kompliziert ist. Die Mehrheit geht davon aus, dass ein Opfer sehr wohl etwas tun muss und tun kann, um nicht Opfer zu werden.
Aus all diesen Gründen empfiehlt Ihnen die Mehrheit – der Entscheid fiel mit 16 zu 6 Stimmen bei 4 Enthaltungen –, den Minderheitsantrag Schmid-Federer abzulehnen.

Lüscher Christian (RL, GE), pour la commission: J'aimerais tout d'abord rendre hommage à la rapporteure de langue allemande pour la loyauté qu'elle manifeste à l'égard de la commission en défendant la majorité face à sa propre minorité.
L'article 143bis tel qu'il vous est proposé aujourd'hui contient deux alinéas. L'alinéa 2 est l'alinéa nouveau qui a été rendu nécessaire pour se mettre à niveau avec la convention, en l'occurrence avec son article 6 puisqu'il s'agit de punir les actes commis avant le piratage lui-même. Cet alinéa 2 n'est pas contesté par la minorité.
Ce que le Conseil fédéral a fait en toilettant cet article 143bis, c'est de proposer une légère modification en ce sens que le droit en vigueur stipule, à ce qui est aujourd'hui le seul alinéa, que celui qui, sans dessein d'enrichissement, se sera introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Or, cette formulation a attiré un certain nombre de critiques de la doctrine, en particulier du «Basler Kommentar», puisque la condition du «sans dessein d'enrichissement» avait pour but que celui qui avait l'intention de s'enrichir ne soit pas puni alors que celui qui agissait sans dessein d'enrichissement illégitime, lui, soit touché par cette disposition. Le Conseil des Etats a suivi le Conseil fédéral lorsque celui-ci a supprimé la notion de «sans dessein d'enrichissement».
Ce que propose la minorité, en revanche, c'est de supprimer la notion d'un système informatique appartenant à autrui «et spécialement protégé contre tout accès». La minorité Schmid-Federer demande que quiconque s'introduit dans un système informatique soit poursuivi et puni au sens de l'article 143bis. Or cette approche nous semble inappropriée pour plusieurs raisons. D'abord, pour des raisons de preuves: il suffit que quelqu'un se balade sur Internet et entre dans un système non protégé pour qu'il soit, selon la minorité Schmid-Federer, poursuivable et punissable au sens de l'article 143bis. Or, ce que veut punir le Code pénal en général, c'est l'intention délictuelle et l'intention de pénétrer sans droit dans un système informatique. Or, si celui-ci n'est pas protégé du tout, et si n'importe qui peut y avoir accès, on ne pourra jamais déterminer s'il y avait ou non volonté de s'introduire sans droit dans un système informatique.
Il s'agit finalement d'appliquer le principe «lex pro vigilantibus», qui veut que ne soient punis que ceux qui agissent au détriment de quelqu'un qui a pris les précautions d'usage pour empêcher qu'une infraction soit commise. Prenons un exemple extrêmement simple: celui qui laisse son portemonnaie sur un banc public ne pourra pas déposer plainte pour vol contre celui qui, le cas échéant, se contenterait d'en prendre possession, ne serait-ce que momentanément, pour l'apporter aux objets trouvés.
Chacun doit prendre des précautions pour éviter que des tiers aient accès à ses données privées. C'est ce que prévoit l'article 143bis CP, à savoir qu'il n'y a pas lieu de punir ceux qui vont simplement se balader sur le Net. En revanche, celui qui perce un système de protection informatique sera évidemment puni, puisqu'il aura voulu s'introduire sans droit dans un système que le détenteur, le propriétaire avait voulu protéger.
C'est la raison pour laquelle, presque à regret, la majorité de la commission vous demande de ne pas suivre la minorité Schmid-Federer.

Abstimmung – Vote
(namentlich – nominatif; Beilage – Annexe 10.058/5069)
Für den Antrag der Mehrheit ... 105 Stimmen
Für den Antrag der Minderheit ... 41 Stimmen

Art. 2 Ziff. 2; Art. 3
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Art. 2 ch. 2; art. 3
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Gesamtabstimmung – Vote sur l'ensemble
(namentlich – nominatif; Beilage – Annexe 10.058/5070)
Für Annahme des Entwurfes ... 117 Stimmen
Dagegen ... 30 Stimmen

08.3790

Motion Aubert Josiane. Schutz des Kindes vor Misshandlung und sexuellem Missbrauch

Motion Aubert Josiane. Protection de l'enfant face à la maltraitance et aux abus sexuels

Einreichungsdatum 09.12.08
Date de dépôt 09.12.08
Nationalrat/Conseil national 03.06.09
Bericht RK-SR 07.09.10
Rapport CAJ-CE 07.09.10
Ständerat/Conseil des Etats 29.11.10
Bericht RK-NR 21.01.11
Rapport CAJ-CN 21.01.11
Nationalrat/Conseil national 02.03.11

Antrag der Kommission
Zustimmung zur Änderung
Proposition de la commission
Approuver la modification

Le président (Germanier Jean-René, président): Vous avez reçu un rapport écrit de la commission.

Angenommen – Adopté