Zentralsekretariat/Secrétariat central
Spitalgasse 34, 3011 Bern
Postfach/Case postale, 3001 Bern
PC 30-28039-3
Tel. 031/329 69 69/Fax. 031 329 69 70
www.spschweiz.ch/www.pssuisse.ch

Sozialdemokratische Partei der Schweiz

Parti Socialiste Suisse
Partito Socialista Svizzero

Bern, den 30. Juni 2009

Bundesamt für Justiz
Fachbereich Internationales Strafrecht
3003 Bern

Vernehmlassungsantwort zum Übereinkommen des Europarates über Computerkriminalität

Sehr geehrte Frau Bundesrätin

Wir danken für die Möglichkeit der Stellungnahme, die wir gerne wie folgt wahrnehmen:

I. Generelle Bemerkungen:

Die SP Schweiz begrüsst die Ratifizierung der Übereinkunft des Europarats zur Computerkriminalität ausdrücklich. Die Vereinheitlichung sowohl des materiellen Strafrechts wie auch der strafprozessualen Massnahmen ist der allein zielführende Ansatz vor dem Hintergrund von im und über das Internet begangenen Straftaten und auf internationaler Ebene agierenden Täterkreisen.

Die vorliegende Vernehmlassungsvorlage hinterlässt allerdings nicht den Eindruck, die Prüfung der Übereinstimmung des nationalen Rechts mit dem Übereinkommen des Europarats sei durchgehend mit der nötigen Sorgfalt vorgenommen und die Bedeutung der hinter der Übereinkunft stehenden Problematik der Cyberkriminalität im ganzen Umfang erfasst worden. Bildlich gesprochen wurde das Problem möglicher Gletscherspalten an einigen Orten mit dem Mittel sehr langer Skis gelöst. Insbesondere im Bereich Rechtshilfe wurde so weit über das Ziel hinausgeschossen: gesichert und ohne vorheriges Beschwerdeverfahren herausgegeben müssen nach dem Übereinkommen nur Randdaten von miteinander kommunizierenden Computersystemen, nicht jedoch Telephonranddaten gemäss BÜPF – die Übereinkunft beschlägt diesen Teil nicht.

II. Spezielle Bemerkungen:

Art. 3 des Übereinkommens

Widersprüchlich erscheint der Abschnitt auf S. 10 der Vernehmlassungsvorlage zum Informationsfluss innerhalb eines Computers: In ein und demselben Satz werden bezüglich Erlangbarkeit solcher Daten via z.B. elektromagnetische Abstrahlung oder Bluetooth (älterer Generation) sich widersprechende Aussagen gemacht: „Diese Daten sind zuweilen, technische Ausrüstung und Kenntnisse vorausgesetzt, relativ leicht abzufangen, gelten aber (…)

wegen des Umstands, dass der gezielt handelnde Täter erhebliche Vorkehrungen treffen muss, (…) als gegen einen unbefugten Umgang besonders gesichert". Zu dieser doch gewagten Behauptung wird keine Fundstelle angeführt. Wir regen an, den rechtlichen Sachverhalt in diesem Punkt noch einmal eingehend zu prüfen.

Art. 6 des Übereinkommens und Art. 143bis StGB

In der Konvention wird im Artikel 6 Ziffer 1 lit. a explizit Bezug genommen auf eine „Vorrichtung einschliesslich eines Computerprogramms". Dies bedeutet, es werden Soft- und Hardwarekomponenten unter dem Begriff zusammengefasst. Dies wird verdeutlicht in Artikel 1a des Übereinkommens, welcher Vorrichtung auch bzw. vor allem als Hardwarekomponente definiert.

In der neuen Fassung von Art. 143bis Abs. 2 StGB werden die Hardwarekomponenten allerdings nicht berücksichtigt. Die Aufzählung: "Passwörter, Programme oder andere Daten" schliesst Hardwarekomponenten mit der Zielsetzung der Begehung einer Straftat gemäss Art. 2 – 5 des Übereinkommens aus.

Zwar ist gemäss Art. 6 Abs. 3 des Übereinkommens ein entsprechender Vorbehalt möglich, wie er nun auch im Entwurf zum Bundesbeschluss aufgeführt ist. Es darf allerdings bezweifelt werden, dass es sich hierbei, soweit es das Ausklammern von Vorrichtungen betrifft, um eine weitsichtige Lösung handelt. Mit einer Ergänzung um das Wort "Vorrichtungen" würde Art. 143bis StGB den Handlungsspielraum der Behörden im Kampf gegen z.B. gegen Skimming-Devices, Spionage-Chips, Fake-Terminals etc. vergrössern.

Gleichzeitig ist darauf zu achten, dass die Arbeit von Systemadministratoren und Softwareentwicklern nicht unnötig behindert wird. In Art. 6 Abs. 2 der Konvention findet sich hierzu eine unmissverständliche Formulierung, die in der neuen Fassung von Art. 143bis Abs. 2 keinen adäquaten Niederschlag gefunden hat. Sofern keine Absicht besteht, eine Straftat zu begehen, soll Verkauf, Vertrieb oder sonstiges Verfügbarmachen auch nicht unter Strafe gestellt werden. Dies ist insbesondere wichtig in Hinblick auf Forschung und Lehre in der Informatik, sowie auch auf die Arbeit von Computer-Sicherheitsfimen notwendig; so ist es beispielsweise gängige Praxis, dass mit simulierten Angriffen auf installierten Computersystemen versucht wird, allfällige Schwachstellen zu finden. Es ist noch einmal zu prüfen, ob die Formulierung "verwendet werden sollen" präzis genug ist; das Verbreiten derartiger Werkzeuge sollte nur dann unter Strafe gestellt werden, wenn der subjektive Tatbestand darauf hinweist, dass ein Vorsatz zur Begehung einer strafbaren Handlung mit einem derartigen Werkzeug besteht und kein offensichtlicher Nutzen des Werkzeuges für nicht-strafbare Handlungen vorliegt.

Eine undifferenzierte Anwendung des Artikels in der vorliegenden Version würde eine enorme Rechtsunsicherheit schaffen und hätte möglicherweise auch einen volkswirtschaftlichen Schaden im Bereich der Computer-Sicherheit zur Folge.

Art. 12 Verantwortlichkeit juristischer Personen

Nicht überzeugen können auch die Ausführungen auf S. 18 der Vernehmlassungsvorlage, die belegen sollen, dass die lediglich subsidiäre Strafbarkeit von Unternehmen gemäss nationalem Recht den Anforderungen des Übereinkommens genügen würden. Der Abs. 1 von Art. 12 macht von seinem Wortlaut her klar, dass eine direkte Strafbarkeit gemeint ist

und nicht nur eine, die nur dann greift, wenn die Täterschaft nicht einer natürlichen Person zugeordnet werden kann. Die Erklärung, dass die natürliche Person auch dann noch belangt werden kann, wenn das Unternehmen bereits verurteilt wurde, hilft hier nicht weiter – entscheidend ist, dass im nationalen Recht im Bereich der zur Debatte stehenden Delikte das Unternehmen nicht mehr belangt werden kann, wenn eine natürliche Person als Täter identifiziert werden konnte.

Die SP Schweiz beantragt deshalb, dass das Prinzip der Subsidiarität in Art. 102 Abs. 1 StGB gestrichen wird.

Art. 30 umgehende Weitergabe gesicherter Verkehrsdaten

In der Vernehmlassungsvorlage wird auf S. 7 oben darauf hingewiesen, dass die Begriffsbestimmungen des Übereinkommens sich in praktischer Hinsicht nicht wesentlich von den in der Schweiz angewendeten Begriffen unterscheiden würden.

Ein Vergleich der Umschreibungen des Begriffs "*Verkehrsdaten*" im Übereinkommen und in der VÜPF zeigt jedoch das Gegenteil: Nach dem Übereinkommen sind "*Verkehrsdaten*" Daten, welche "*im Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems"* anfallen. Der Begriff gemäss VÜPF geht weit darüber hinaus und beinhaltet auch Daten, welche beim Post- und Fernmeldeverkehr anfallen.

Zur Vermeidung eines übermässigen Eingriffs in die Geheim- und Privatsphäre sind wir deshalb der Auffassung, dass Art. 11 IRSG um den folgenden Absatz 3 ergänzt werden sollte:

> Art. 11 Gesetzliche Ausdrücke
>
> [3] "Verkehrsdaten" im Sinne dieses Gesetzes sind alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht.

Wir bitten Sie, unsere Einwände und Anregungen bei der notwendigen Überarbeitung der Vorlage zu berücksichtigen. Wir möchten höflich anregen, hierbei auch den Beizug externer fachlicher Experten in Erwägung zu ziehen.

Mit freundlichen Grüssen
SOZIALDEMOKRATISCHE PARTEI DER SCHWEIZ

Christian Levrat
Präsident

Carsten Schmidt
Politischer Fachsekretär