

## **AUSZUG AUS DER CONVENTION ON CYBERCRIME IN DEUTSCHER ÜBERSETZUNG (ART. 1–6, 11 UND 13)<sup>1</sup>**

### **Kapitel I – Sprachgebrauch**

#### Artikel 1 – Begriffsbestimmungen

Für dieses Übereinkommen bedeutet

- a) „Computersystem“ jede Vorrichtung oder Gruppe verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren in Ausführung eines Programmes eine automatische bzw. automatisierte<sup>2</sup> Datenverarbeitung durchführt;
- b) „Computerdaten“ jede Darstellung von Tatsachen, Informationen oder Begriffen in einer zur Verarbeitung in einem Computer geeigneten Form einschliesslich eines Programmes, das geeignet ist, ein Computersystem zur Ausführung einer Funktion zu veranlassen.
- c) „Diensteanbieter“:
  - i) jede öffentliche oder private Organisation, die den Nutzern ihres Dienstes die Möglichkeit verschafft bzw. anbietet<sup>3</sup>, mittels eines Computersystems zu kommunizieren, und
  - ii) jede andere Organisation, die für diesen Kommunikationsdienst oder die Nutzer dieses Dienstes Computerdaten verarbeitet oder speichert.
- d) „Verbindungsdaten“ alle in Zusammenhang mit einer Kommunikation mittels eines Computersystems stehenden Computerdaten, die durch ein Computersystem generiert wurden, das Teil der Kommunikationskette bildete, und die den Ursprung, die Bestimmung, den Übertragungsweg, die Uhrzeit, das Datum, die Grösse, die Dauer oder die Art des zugrundeliegenden Dienstes anzeigen.

---

<sup>1</sup> Übersetzung des Verfassers auf der Grundlage der englischen und französischen Fassung der CCC.

<sup>2</sup> „Automatic processing of data“ bzw. „traitement automatisé de données“.

<sup>3</sup> „Provides“ bzw. „offre“.

## Kapitel II – Massnahmen, die auf nationaler Ebene zu treffen sind

### Abschnitt I – Materielles Strafrecht

#### Titel 1 – Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und –systemen

##### Artikel 2 – Unrechtmässiger Zugriff<sup>4</sup>

Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um den vorsätzlichen und unrechtmässigen Zugriff auf das Ganze oder einen Teil eines Computersystems nach ihrem innerstaatlichen Recht unter Strafe zu stellen. Eine Partei kann verlangen, dass die Straftat durch Verletzung von Sicherheitsmassnahmen, in der Absicht, Computerdaten zu erlangen, oder in einer anderen unredlichen bzw. deliktischen<sup>5</sup> Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen wird.

##### Artikel 3 – Unrechtmässiges Abfangen<sup>6</sup>

Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um das vorsätzliche und unrechtmässige, mit technischen Mitteln ausgeführte Abfangen nichtöffentlicher Computerdatenübertragungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschliesslich der elektromagnetischen Abstrahlungen von einem Computersystem, welches solche Computerdaten transportiert, nach ihrem innerstaatlichen Recht unter Strafe zu stellen. Eine Partei kann verlangen, dass die Straftat in einer unredlichen bzw. deliktischen<sup>7</sup> Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen wird.

##### Artikel 4 – Eingriff in die Datenintegrität<sup>8</sup>

<sup>1</sup>Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um das vorsätzliche und unrechtmässige Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten nach ihrem innerstaatlichen Recht unter Strafe zu stellen.

<sup>2</sup>Eine Partei kann sich das Recht vorbehalten zu verlangen, dass das in Abs. 1 beschriebene Verhalten einen grossen Schaden<sup>9</sup> zur Folge hat.

---

<sup>4</sup> „Access“ wird in der Informatik mit „Zugriff“ übersetzt (Remote- oder Fernzugriff, lokaler Zugriff).

<sup>5</sup> „Dishonest intent“ bzw. „intention délictueuse“.

<sup>6</sup> Die wörtliche Übersetzung von „interception“ lautet „Abfangen“ oder „Unterbrechen“; der Begriff wird daneben auch mit „Abhören“, „Überwachen“ oder „Sniffen“ ins Deutsche übertragen. Nachdem im Strafprozessrecht der Begriff „Überwachung“ für das Abfangen der Telekommunikation inklusive Internetübertragung üblich ist (vgl. Art. 179<sup>octies</sup> StGB; Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF], SR 780.1; s.a. Art. 21 CCC „Interception of content data“, Überwachung von Inhaltsdaten), wäre es sinnvoll, von „unrechtmässiger Überwachung“ zu sprechen. Dem steht jedoch entgegen, dass die bisher mit dem Begriff Überwachung assoziierte Übertragung von Telefongesprächen nach h.L. gerade nicht als *Daten*-Übertragung angesehen wird.

<sup>7</sup> „Dishonest intent“ bzw. „intention délictueuse“.

#### Artikel 5 – Eingriff in die Systemintegrität<sup>10</sup>

Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um die vorsätzliche und unrechtmässige, schwere Behinderung der Funktionsfähigkeit eines Computersystems durch das Eingeben, Übertragen, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten nach ihrem innerstaatlichen Recht unter Strafe zu stellen.

#### Artikel 6 – Missbrauch von Vorrichtungen<sup>11</sup>

<sup>1</sup>Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um nach ihrem innerstaatlichen Recht unter Strafe zu stellen, falls vorsätzlich und unrechtmässig begangen:

- a) das Herstellen, Verkaufen, Beschaffen zum Gebrauch, Einführen, Verbreiten oder sonstwie Zugänglichmachen:
- i) einer Vorrichtung, einschliesslich eines Computerprogramms, die hauptsächlich zum Zwecke der Begehung einer der nach den obenerwähnten Artikeln 2 bis 5 geschaffenen Straftaten entworfen oder angepasst wurde;
  - ii) eines Computerpasswortes, eines Zugriffscode oder ähnlicher Daten, durch welche auf das Ganze oder einen Teil eines Computersystems zugegriffen werden kann,

mit der Absicht, sie zum Zwecke der Begehung einer der Straftaten zu verwenden, auf welche die Artikel 2 bis 5 abzielen; und

- b) den Besitz eines oben in den lit. a.i) oder ii) genannten Mittels<sup>12</sup> mit der Absicht, es zum Zwecke der Begehung einer der Straftaten zu verwenden, auf welche die Artikel 2 bis 5 abzielen. Eine Partei kann nach dem innerstaatlichen Recht den Besitz einer bestimmten Anzahl dieser Mittel verlangen, um die strafrechtliche Verantwortlichkeit zu begründen.

<sup>2</sup>Dieser Artikel darf nicht so ausgelegt werden, als schreibe er eine strafrechtliche Verantwortlichkeit vor, wenn das in Absatz 1 dieses Artikels genannte Herstellen, Verkaufen, Beschaffen zum Gebrauch, Einführen, Verbreiten oder sonstwie Zugänglichmachen oder Besitzen<sup>13</sup> nicht zum Zwecke der Begehung einer nach den obenerwähnten Artikeln 2 bis 5 dieses Übereinkommens geschaffenen Straftat erfolgt, wie im Fall des genehmigten Tests oder des Schutzes eines Computersystems.

<sup>3</sup>Jede Partei kann sich das Recht vorbehalten, Absatz 1 dieses Artikels nicht anzuwenden, soweit der Vorbehalt nicht das Verkaufen, Verbreiten oder sonstwie Zugänglichmachen der in Absatz 1 lit. a.ii) dieses Artikels genannten Mittel betrifft.

...

---

<sup>8</sup> „Data interference“ bzw. „atteinte à l'intégrité des données“.

<sup>9</sup> „Serious harm“ bzw. „des dommages sérieux“ (grosse Schäden).

<sup>10</sup> „System interference“ bzw. „atteinte à l'intégrité du système“.

<sup>11</sup> „Misuse of devices“ bzw. „abus de dispositifs“.

<sup>12</sup> „Item“ bzw. „élément“.

<sup>13</sup> Fehlt in der französischen Fassung!

#### Art. 11 – Versuch und Helferschaft

<sup>1</sup>Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um die vorsätzliche Helferschaft zur Begehung einer der nach den Artikeln 2 bis 10 des vorliegenden Übereinkommens geschaffenen Straftaten, nach ihrem innerstaatlichen Recht unter Strafe zu stellen, falls sie mit dem Vorsatz, dass eine solche Straftat begangen werde, ausgeführt wird.

<sup>2</sup>Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um einen vorsätzlichen Versuch der Begehung einer der nach den Artikeln 3 bis 5, 7, 8 und 9 Abs. 1 lit. a und c des vorliegenden Übereinkommens geschaffenen Straftaten, nach ihrem innerstaatlichen Recht unter Strafe zu stellen.

<sup>3</sup>Jede Partei kann sich das Recht vorbehalten, Absatz 2 ganz oder teilweise nicht anzuwenden.

...

#### Art. 13 – Sanktionen und Massnahmen

<sup>1</sup>Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um sicherzustellen, dass die nach den Artikeln 2 bis 11 geschaffenen Straftaten mit wirksamen, verhältnismässigen und abschreckenden Sanktionen bedroht werden, welche Freiheitsstrafen einschliessen.

<sup>2</sup>Jede Partei stellt sicher, dass juristische Personen, die nach Artikel 12 verantwortlich gemacht werden, mit wirksamen, verhältnismässigen und abschreckenden strafrechtlichen oder nichtstrafrechtlichen Sanktionen oder Massnahmen, einschliesslich Geldsanktionen, bedroht werden.