VERNEHMLASSUNGSBERICHT

DER REGIERUNG

BETREFFEND

DIE ABÄNDERUNG DES STRAFGESETZBUCHES

(CYBER CRIME)

Ressort Justiz

Vernehmlassungsfrist: 30. Januar 2009

INHALTSVERZEICHNIS

Beilagen:

- Übereinkommen über Computerkriminalität vom 23. November 2001 – Cyber Crime Convention (CCC), ETS Nr. 185.
- Zusatzprotokoll vom 28. Januar 2003 zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, ETS Nr. 189.

ZUSAMMENFASSUNG

Anlass für die Vernehmlassungsvorlage ist das Übereinkommen vom 23. November 2001 über die Computerkriminalität (Cyber Crime Convention, CCC) einschliesslich des Zusatzprotokolls vom 28. Januar 2003. Es ist ein Übereinkommen des Europarates zur Bekämpfung der Kriminalität im Zusammenhang mit den neuen Informationstechnologien und strebt eine Harmonisierung der nationalen Gesetzgebungen in Bezug auf die zu ahndenden Vergehen, die Definition der Untersuchungs- und Strafverfolgungsverfahren sowie die Errichtung eines schnellen und effektiven Systems der internationalen Zusammenarbeit an. Das Übereinkommen ist das erste internationale Rechtsinstrument zur Bekämpfung der Computer- bzw. Internetkriminalität. Es ist zudem direkt relevant für die verbesserte Zusammenarbeit im Rahmen der Bekämpfung des Terrorismus. Das Zusatzprotokoll weitet den Geltungsbereich des Übereinkommens auf Straftaten rassistischer oder fremdenfeindlicher Art aus und stellt damit ein wichtiges internationales Instrument im Kampf gegen Rassismus dar.

Die Regierung hatte im Hinblick auf eine Unterzeichnung des Übereinkommens und des Zusatzprotokolls den innerstaatlichen Anpassungsbedarf bereits vor einiger Zeit überprüft und eine interne Vernehmlassung durchgeführt. Aufgrund anderer Prioritäten wurde die Unterzeichnung und weitere Umsetzung aber zurückgestellt. Mittlerweile wurde der innerstaatliche Anpassungsbedarf durch die Regierung einer erneuten eingehenden Prüfung unterzogen und in der Vernehmlassungsvorlage wird die entsprechende Gesetzesrevision vorgeschlagen, damit Liechtenstein dieses angesichts der rasanten Entwicklungen im IT-Bereich und der damit zusammenhängenden Missbrauchsmöglichkeiten bedeutende Übereinkommen samt Zusatzprotokoll unterzeichnen und anschliessend ratifizieren kann. Das Übereinkommen ist am 1. Juli 2004 in Kraft getreten und zählt 23 Vertragsparteien; das Zusatzprotokoll ist seit dem 1. März 2006 in Kraft und zählt 13 Vertragsparteien. Österreich hat, wie die Schweiz, das Übereinkommen und das Zusatzprotokoll bereits unterzeichnet, jedoch noch nicht ratifiziert, die notwendigen Anpassungen der Rechtslage allerdings bereits vorgenommen. Das österreichische Strafgesetzbuch ist die Rezeptionsgrundlage für das liechtensteinische Strafgesetzbuch. Deshalb, und zur Wegbereitung für die Umsetzung des Übereinkommens, ist im Sinne der Vermeidung eines weiteren Regelungsgefälles gegenüber der österreichischen Rezeptionsgrundlage eine Revision des liechten-

steinischen Strafgesetzbuches angezeigt. Den Bestimmungen des Zusatzprotokolls genügt die liechtensteinische Rechtslage bereits. Weitere Massnahmen zur vollständigen Umsetzung der Konvention sind im Ressort Justiz bereits in Vorbereitung, namentlich hinsichtlich Straftaten in Bezug auf Kinderpornographie sowie bezüglich der strafrechtlichen Verantwortlichkeit von juristischen Personen sowie verfahrensrechtliche Anpassungen (StPO). Diese Vorlagen müssen einem separaten Strafrechtspaket vorbehalten bleiben, da die relevanten Bestimmungen in Österreich derzeit teilweise überarbeitet werden. Nach Abschluss dieser Anpassungen sollen die nötigen Umsetzungsarbeiten in Liechtenstein in Angriff genommen werden.

Eine Revision des Strafgesetzbuches wurde bereits im Bericht und Antrag betreffend die Änderung des Strafgesetzbuches, der Strafprozessordnung, des Betäubungsmittelgesetzes und des Rechtshilfegesetzes (BuA Nr. 2/2007, S. 178, s. dort) thematisiert. Das Obergericht hatte über die damalige Vernehmlassungsvorlage hinaus vorgeschlagen, zur Umsetzung von Art. 5 CCC die §§ 126b und c sowie § 148a des österreichischen StGB zu rezipieren. Dieser durchaus sinnvolle Vorschlag müsse jedoch einer getrennten Vorlage vorbehalten bleiben. Diese „getrennte Vorlage" ist nun Gegenstand der Vernehmlassungsvorlage, wobei neben Art. 5 der Konvention zusätzlich die Art. 2, 4, 6 und 7 umgesetzt werden sollen.

Neu zu schaffen sind Bestimmungen betreffend den widerrechtlichen Zugriff auf ein Computersystem, zur Störung der Funktionsfähigkeit eines Computersystems, zum Missbrauch von Computerprogrammen oder Zugangsdaten sowie zur Datenfälschung. Ebenfalls neu einzufügen sind zwei Legaldefinitionen, einerseits die Legaldefinition von Computersystemen, andererseits die Legaldefinition des Begriffes Daten. Lediglich Anpassungsbedarf gibt es hinsichtlich des bereits bestehenden § 148a, dem Computerbetrug. Hier müsste die Unterdrückung von Daten neu in die Liste der Tathandlungen nach Abs. 1 aufgenommen werden.

Sowohl zur Anpassung der bereits bestehenden Bestimmung des § 148a als auch zur Schaffung der erwähnten Tatbestände dienen die korrespondierenden Normen des österreichischen Strafgesetzbuches.

ZUSTÄNDIGES RESSORT

Ressort Justiz

BETROFFENE AMTSSTELLEN

Staatsanwaltschaft
Landespolizei
Landgericht
Amt für Auswärtige Angelegenheiten

Vaduz, 4. November 2008

RA 2008/2995-0135

P

1. AUSGANGSLAGE

Computerkriminalität definiert sich als Straftat, die mit der Nutzung von Computertechnologien verbunden ist.

Die Begriffe „Computerkriminalität“, „Computerstraftaten“, „High-Tech-Kriminalität“ und „Cyberkriminalität“ sind insofern gleichbedeutend, als sie a) die Nutzung von Informations- und Kommunikationsnetzen ohne geographische Begrenzung und b) die Übertragung von nicht erfassbaren und kurzlebigen Daten bezeichnen.

Die Entwicklung im Bereich der Computerkriminalität ist rasant. Der Missbrauch des Internets, insbesondere durch die organisierte Kriminalität, ist bereits stark verbreitet und nimmt weiter kontinuierlich zu. Handlungsbedarf besteht zweifellos, da sich viele neue Phänomene aus dem Bereich der Informations- und Kommunikationskriminalität (Mediendelikte) nur noch schwerlich unter die bestehenden Strafvorschriften des nationalen Rechts subsumieren lassen. Eine unübersichtliche, unklare und teils widersprüchliche Rechtslage stellt Behörden und Internetanbieter beim Kampf gegen die Computerkriminalität oft vor Probleme.

Die jüngsten Entwicklungen zeigen deutlich, dass die Gefahren der Computerkriminalität stetig zunehmen. Das aktuellste Beispiel ist die Weiterentwicklung von „Bot“-Netzwerken. „Bots“ sind Programme, die sich unbemerkt auf den

Computer eines Opfers herunterladen und selbständig auf dem Gerät installieren. Die „gehackten“ Rechner können in der Folge per Fernzugriff gesteuert werden und für kriminelle Aktivitäten wie beispielsweise dem Versenden von „Spam“ missbraucht werden.

Der Europarat hat diese Ausgangslage zum Anlass genommen, ein Übereinkommen auszuarbeiten. Das Übereinkommen vom 23. November 2001 über die Computerkriminalität[1] ist die erste internationale Vereinbarung über mittels Internet oder sonstiger Computernetze begangene Straftaten. Es betrifft vor allem Verletzungen des Urheberrechts, Betrug per Computer, Kinderpornographie und Verstösse gegen die Sicherheit von elektronischen Netzen. Das Übereinkommen enthält auch eine Reihe von Ermächtigungen und Verfahrensvorschriften wie etwa zur Suche in Computernetzen und zum Abfangen von Nachrichten. Hauptzweck ist laut der Präambel die Verfolgung einer gemeinsamen Strafrechtspolitik zum Schutz der Gesellschaft vor Straftaten per Computer (sog. Cyber Crimes), und zwar insbesondere durch entsprechende gesetzliche Regelungen und die Förderung der internationalen Zusammenarbeit. Das Übereinkommen ist das Ergebnis vierjähriger Arbeiten von Europaratsexperten, wobei auch Japan, Kanada, die USA und andere Länder, die nicht Mitglied des Europarats sind, mitgewirkt haben. Ergänzend dazu gibt es ein Zusatzprotokoll[2], das die Veröffentlichung rassistischer oder fremdenfeindlicher Propaganda in Computernetzen unter Strafe stellt.

---

1 Übereinkommen über Computerkriminalität vom 23. November 2001 – Cyber Crime Convention (CCC), ETS Nr. 185.

2 Zusatzprotokoll vom 28. Januar 2003 zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, ETS Nr. 189.

Die Cyber Crime-Konvention wurde bisher von 45 Staaten unterzeichnet[3] und von 23 Staaten ratifiziert[4]. Es stellt eines der bedeutenden internationalen Strafrechtsübereinkommen dar. Dem Zusatzprotokoll gehören 13 Vertragsparteien an. Beide Rechtsinstrumente stehen auch Nichtmitgliedstaaten des Europarats zum Beitritt offen. So sind z.B. die USA bereits Vertragspartei des Übereinkommens. Liechtenstein hat bisher weder das Übereinkommen noch das Zusatzprotokoll unterzeichnet. Die Regierung hatte im Jahr 2005 auf Vorschlag des Amtes für Auswärtige Angelegenheiten eine interne Vernehmlassung im Hinblick auf die Unterzeichnung des Übereinkommens und des Zusatzprotokolls durchgeführt, an welcher das Ressort Justiz, das Amt für Kommunikation, die Landespolizei, der Datenschutzbeauftragte, die Staatsanwaltschaft und das Landgericht teilnahmen. Die Mehrheit der Stellungnehmenden befürworteten damals die Unterzeichnung und Umsetzung des Übereinkommens und des Zusatzprotokolls. Kritik wurde insbesondere im Hinblick auf das Tempo des Unterzeichnungs- und Ratifikationsvorgangs geäussert, mit Blick auf die damals noch geringe Zahl der Vertragsparteien. Das Ressort Justiz hielt in seiner Stellungnahme zusammengefasst fest, dass im Sinne der Vermeidung eines weiteren Regelungsgefälles zur österreichischen Rezeptionsgrundlage eine Revision des liechtensteinischen Strafgesetzbuches angebracht erscheine. Zum Zusatzprotokoll gelte es – in Übereinstimmung mit dem Amt für Auswärtige Angelegenheiten – festzuhalten, dass die Vorgaben des Zusatzprotokolls bereits durch geltendes Recht (vor allem durch § 283 StGB) erfüllt seien und somit kein Umsetzungsbedarf gegeben sei.

---

3 Z.B. Deutschland, Österreich, die Schweiz, Japan und Kanada.

4 Z.B. Vereinigte Staaten von Amerika, Norwegen, die Niederlande, die Ukraine, Italien, Frankreich, Dänemark und sämtliche Länder des osteuropäischen Raumes.

2. ANLASS / NOTWENDIGKEIT DER VORLAGE / BEGRÜNDUNG DER VORLAGE

Die Notwendigkeit der Vorlage besteht in dreierlei Hinsicht. Erstens ist sie unabdingbar für die Umsetzung der Cyber Crime-Konvention des Europarates (CCC), da vor einer Ratifizierung in einem ersten Schritt die Rechtslage entsprechend angepasst werden muss. Zweitens gilt es, ein zu grosses Regelungsgefälle gegenüber dem österreichischen Strafgesetzbuch zu vermeiden, da dieses die Rezeptionsgrundlage für das liechtensteinische Strafgesetzbuch darstellt und Österreich die gegenständlichen Anpassungen bereits vorgenommen hat. Zum Dritten ist Rechtssicherheit und Rechtsklarheit zu schaffen angesichts der Tatsache, dass sich viele der heutigen Straftaten nicht mehr unter die bestehenden gesetzlichen Regelungen subsumieren lassen, was den Gerichten die Hände bindet und schlimmstenfalls eine Verurteilung verunmöglicht, wo in anderen Ländern nach deren Recht einer Verurteilung nichts im Wege gestanden hätte.

Zur vollständigen Umsetzung der Konvention sind noch weitere gesetzgeberische Massnahmen notwendig, die im Ressort Justiz bereits in Vorbereitung sind, namentlich hinsichtlich Straftaten in Bezug auf Kinderpornographie (Art. 9 CCC, § 218a StGB) und der strafrechtlichen Verantwortlichkeit juristischer Personen (Art. 12 CCC) sowie verfahrensrechtliche Anpassungen (Art. 14-22 CCC; StPO). Da mit dieser Vorlage die Umsetzung des wesentlichen materiellrechtlichen Teils der Konvention realisiert werden kann, wird die Regierung nach dem Start der Vernehmlassung die Unterzeichnung der Konvention und des Zusatzprotokolls vornehmen.

3. SCHWERPUNKTE DER VORLAGE

Die neu zu schaffenden bzw. anzupassenden Straftatbestände betreffen allesamt den Bereich der Computerkriminalität.

Mit der Einführung einer Legaldefinition in § 74 Abs. 1 Ziff. 8 StGB soll Klarheit darüber geschaffen werden, was unter einem „Computersystem“ zu verstehen ist. Die Einführung dieser Legaldefinition ist unabdingbar, da der Begriff „Computersystem“ in mehreren der neuen Tatbestände aufscheint und eine fehlende Legaldefinition folglich zu Rechtsunsicherheiten führen würde.

Die neue Legaldefinition des Begriffes „Daten“ in § 74 Abs. 3 StGB legt fest, dass unter Daten sowohl personenbezogene als auch nicht personenbezogene Daten zu verstehen sind. Dieser Datenbegriff geht über denjenigen des Datenschutzgesetzes hinaus (dort sind nur die personenbezogenen Daten geregelt). Diese Weitläufigkeit des neuen Begriffes ist deshalb nötig, weil es beim vorliegenden Bereich in der Natur der Sache liegt, dass es sich häufig um Daten handelt, welche nicht einer bestimmten oder bestimmbaren Person zuzuordnen sind. Auch diese Legaldefinition ist unabdingbar, da der vorliegende Datenbegriff ebenfalls für mehrere der neuen Tatbestände relevant ist.

§ 118a StGB regelt den widerrechtlichen Zugriff auf ein Computersystem. Diese Bestimmung zielt auf die Bestrafung des so genannten „Hackings“.

§ 119a StGB stellt das missbräuchliche Abfangen von Daten unter Strafe und ist als Auffangtatbestand zu § 119 StGB (Verletzung des Kommunikationsgeheimnisses) zu sehen. § 119a StGB erstreckt den Anwendungsbereich den Vorgaben der CCC entsprechend über Nachrichten im Sinne des § 119 StGB hinaus auf die sonstigen Daten im Sinne des neu vorgeschlagenen § 74 Abs. 3 StGB.

Die Störung der Funktionsfähigkeit eines Computersystems wird neu durch § 126b StGB unter Strafe gestellt. Unter einer Störung der Funktionsfähigkeit eines Computersystems ist die vollständige oder nahezu vollständige Blockade bestimmter Dienste oder eines ganzen Rechners zu verstehen.

§ 126c regelt den Missbrauch von Computerprogrammen oder Zugangsdaten. Diese Bestimmung umfasst das Herstellen, Einführen, Vertreiben, Veräussern oder sonst Zugänglichmachen eines Computerprogrammes zur Verfolgung von einschlägigen Zwecken oder der Schaffung oder Adaptierung von entsprechenden Zugangsdaten.

Der Computerbetrug ist bereits in § 148a StGB normiert, muss jedoch zur Angleichung an das österreichische Strafgesetzbuch analog § 148a öStGB um die Tathandlung der Unterdrückung von Daten (Input-Manipulation) erweitert werden.

Neu wird die Datenfälschung in § 225a StGB geregelt. Diese Bestimmung bezweckt die Bestrafung der Fälschung von Computerdaten als Gegenstück zur herkömmlichen Urkundenfälschung. Als Begehungsformen sind sowohl die Herstellung falscher Daten als auch die Verfälschung echter Daten möglich.

4. ERLÄUTERUNGEN ZU DEN EINZELNEN ARTIKELN

Zu § 74

Eine Legaldefinition des Begriffes „Computersystem“ wie in § 74 Abs. 1 Ziff. 8 öStGB fehlt im liechtensteinischen Strafgesetzbuch und muss deshalb neu als § 74 Abs. 1 Ziff. 8 StGB eingefügt werden. Der Begriff des Computersystems umfasst sowohl einzelne als auch miteinander vernetzte oder auf andere Weise verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen. Er umfasst somit nicht nur das Internet oder Computersysteme, sondern auch einzelne Computergeräte. Die Definition entspricht im Wesentlichen Art. 1 lit. a CCC.

Der Begriff der „Daten“ im Sinn der mit dem österreichischen Strafrechtsänderungsgesetz 2002 eingeführten Legaldefinition des § 74 Abs. 2 öStGB (neu StGB § 74 Abs. 3), wonach unter Daten sowohl personenbezogene und nicht per-

sonenbezogene Daten als auch Programme zu verstehen sind, ist sehr weit gefasst. Unter personenbezogenen Daten sind Angaben zu verstehen, welche sich auf eine bestimmte oder bestimmbare Person beziehen. Nicht personenbezogene Daten sind Angaben von technischen Einrichtungen, Gegenständen etc., die sich nicht einer bestimmten oder bestimmbaren Person zuordnen lassen. Dieser neue Begriff geht somit über den im Datenschutzgesetz vorgesehenen Begriff hinaus, da das Datenschutzgesetz lediglich personenbezogene Daten regelt. Diese Weitläufigkeit des neuen Begriffes ist deshalb nötig, weil es beim vorliegenden Bereich in der Natur der Sache liegt, dass es sich häufig um Daten handelt, welche eben nicht einer bestimmten oder bestimmbaren Person zuzuordnen sind. Zudem findet das Datenschutzgesetz[5] keine Anwendung auf hängige Zivil-, Straf- und Rechtshilfeverfahren sowie Verwaltungsbeschwerdeverfahren. Die gegebenenfalls zu wahrenden Rechte in einem hängigen Strafverfahren sind durch die bestehenden prozessualen Rechte (Akteneinsichtsrecht etc.) gedeckt. Die neu zu schaffende Bestimmung des § 74 Abs. 3 StGB stellt deshalb sicher, dass sowohl personenbezogene als auch nicht personenbezogene Daten von den prozessualen Rechten erfasst werden. Eine Nichtaufnahme in den liechtensteinischen Rechtsbestand würde zudem Unklarheiten verursachen, da in den aufzunehmenden Bestimmungen, beispielsweise in § 225a StGB (Datenfälschung), wiederholt auf die Legaldefinition in § 74 StGB verwiesen wird.

Zu § 118a

Diese Bestimmung ist neu. Sie dient der Umsetzung von Art. 2 CCC und zielt auf die Bestrafung des so genannten „Hackings“ (unerlaubter Zugang) ab.

Die Tathandlung besteht im Verschaffen des Zuganges zu einem Computersystem, über das der Täter nicht oder nicht alleine verfügen darf oder zu einem Teil

---

5 Art. 2 Abs. 3 lit. c DSG.

eines solchen unter Verletzung spezifischer Sicherheitssysteme im Computersystem. Der Begriff des „Computersystems“ ist in § 74 Abs. 1 Ziff. 8 StGB definiert. Sicherheitsvorkehrungen sind nur dann als spezifisch anzusehen, wenn sie im Computersystem angebracht worden sind, um sicherzustellen, dass nur berechtigte Personen zugreifen bzw. unberechtigten Personen der Zugriff verweigert wird (Zugangscodes, Passwörter etc.). Nicht als spezifisch anzusehen ist eine nicht in direktem Zusammenhang stehende, ganz allgemeine Massnahme. Das blosse Absperren eines Raumes oder eine Alarmanlage beispielsweise sind nicht als spezifisch anzusehen. Die Tat muss unter Verletzung eines spezifischen Sicherheitssystems begangen werden. Eine Verletzung ist mehr als eine Überwindung des Sicherheitssystems. Die unbefugte Verwendung eines fremden Passwortes genügt daher nicht.

Subjektiv ist ein erweiterter Vorsatz erforderlich. Der Täter muss zunächst in der Absicht (§ 5 Abs. 2 StGB) handeln, sich oder einem anderen Unbefugten Kenntnis der Daten zu verschaffen. Darüber hinaus muss er die Absicht haben, durch eigene Benützung, Zugänglichmachung oder Veröffentlichung der Daten sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Unter Daten sind Daten im Sinne des § 74 Abs. 3 StGB zu verstehen. Dieser weite Anwendungsbereich wird durch die restriktiven Bedingungen auf der subjektiven Tatseite eingeschränkt.

Die strafbare Handlung ist ein Ermächtigungsdelikt (§ 2 Abs. 5 StPO).

Zu § 119a

Diese Bestimmung ist neu und dient der Umsetzung des Art. 3 CCC. § 119a StGB ist als Auffangtatbestand zu sehen und übernimmt die Tathandlungen des § 119 StGB, erstreckt den Anwendungsbereich aber den Vorgaben der Cyber Crime-Konvention entsprechend über Nachrichten im Sinne des § 119 StGB hinaus auf die sonstigen Daten im Sinne des neu vorgeschlagenen § 74 Abs. 3 StGB.

Die Tathandlung entspricht derjenigen des § 119 StGB, bezieht sich jedoch nicht nur auf Nachrichten, sondern auf alle Daten im Sinne des § 74 Abs. 3 StGB. Zudem wird damit das Auffangen der elektromagnetischen Abstrahlung eines Computersystems für Nachrichten als auch sonstige Daten abgedeckt.

Als strafbarkeitseinschränkender Ausgleich für den weiten äusseren Tatbestand ist – wie bei § 118a – auf der subjektiven Tatseite ein erweiterter Vorsatz erforderlich. Der Täter muss zunächst in der Absicht (§ 5 Abs. 2 StGB) handeln, sich oder einem Unbefugten Kenntnis von dem im Wege eines Computersystems übermittelten Daten zu verschaffen. Darüber hinaus muss er die Absicht haben, durch eigene Benützung, Zugänglichmachung oder Veröffentlichung der Daten sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen.

Die strafbare Handlung ist ein Ermächtigungsdelikt (§ 2 Abs. 5 StPO).

Zu § 126b

Diese Bestimmung ist neu und zur Umsetzung von Art. 5 CCC einzufügen, soweit die Tat nicht bereits durch § 126a StGB strafbar ist.

Die Tathandlung besteht im Eingeben oder Übermitteln von Daten. Der Erfolg muss in einer schweren Störung der Funktionsfähigkeit des Computersystems bestehen. Von dieser Bestimmung erfasst sind somit nur Angriffe, die einer so genannten „Denial-of-service-attack“ entsprechen, also Angriffe, die bestimmte Dienste oder auch einen gesamten Rechner blockieren, beispielsweise durch Herbeiführung einer Überlastungssituation. Schwer ist eine Störung dann, wenn das Computersystem völlig lahm gelegt wird oder bis zur Unbrauchbarkeit verlangsamt wird. Die Dauer der Störung spielt bei der Schwere ebenfalls eine Rolle.

Zu § 126c

Diese Bestimmung ist neu und dient der Umsetzung von Art. 6 CCC in Form eines Vorbereitungsdeliktes.

Die Tathandlung besteht im Herstellen, Einführen, Vertreiben, Veräussern oder sonst Zugänglichmachen eines Computerprogrammes, das zur Begehung einer der Straftatbestände nach §§ 118a, 119, 119a, 126a, 126b geschaffen oder adaptiert worden ist, oder einer vergleichbaren solchen Vorrichtung (Abs. 1 Ziff.1) oder eines Computerpasswortes, eines Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder eines Teiles ermöglichen. Der blosse Besitz der erwähnten Computerprogramme oder Zugangsdaten reicht nicht aus.

Auf der subjektiven Seite ist der erweiterte Vorsatz erforderlich, dass diese Computerprogramme bzw. Zugangsdaten zur Begehung eines der genannten Tatbestände gebraucht werden.

Abs. 2 sieht die Strafaufhebung wegen tätiger Reue bei Schadensvermeidung, sei es auch durch blosses Bemühen, in Form einer Generalklausel vor.

Zu § 148a

Der Computerbetrug ist bereits in § 148a StGB geregelt, muss jedoch zur Angleichung an das österreichische Strafgesetzbuch analog § 148a öStGB und zur vollständigen Umsetzung von Art. 8 CCC um die Tathandlung der Unterdrückung von Daten (Input-Manipulation) in Abs. 1 erweitert werden.

Den Strafbestimmungen gegen Betrug können die denkbaren Manipulationen an einer Datenverarbeitungsanlage nur unterstellt werden, wenn durch sie eine Person, die in den Verarbeitungsablauf eingeschaltet ist, getäuscht wird und diese den Schaden herbeiführt. In rationell geschalteten Anlagen fehlt es aber regelmässig am Einsatz solcher Personen. Lassen sich Manipulationen an Daten-

verarbeitungsanlagen also nicht leicht ausschalten, so kommt dem Strafrechtsschutz besondere Bedeutung zu.

Die Tathandlung besteht in der Beeinflussung des Ergebnisses eines Datenverarbeitungsvorganges. Dass diese Beeinflussung unberechtigt sein muss, ergibt sich aus dem Erfordernis eines auf unrechtmässige Bereicherung gerichteten Vorsatzes. Die Aufzählung der Möglichkeiten der Beeinflussung ist taxativ. Für den Begriff der Daten wird auf die neu zu schaffende Legaldefinition des StGB § 74 Abs. 3 verwiesen (öStGB § 74 Abs. 2). Die Tat erfordert auf der inneren Tatseite Vorsatz und Bereicherungsvorsatz.

Das Einsetzen nicht angemeldeter Mobiltelefone, die in unzulässiger Manipulation mit Ruf- und Seriennummern ordnungsgemäss zugelassener Geräte versehen wurden, ist nach § 148a zu beurteilen (JBl 1998, 738 mit Anm. *Bertel* und *Burgstaller*). Der österreichische OGH hält auch nach der Einführung des § 148a StGB daran fest, dass Geldbehebung aus Bankomaten unter missbräuchlicher Verwendung fremder Bankomatkarten oder –duplikate mit Gewahrsamsbruch erfolgt und daher als Diebstahl zu beurteilen ist. Betrug liegt nicht schon deshalb vor, weil ein Kontrollorgan täuschungsbedingt ein Eingreifen in den Geschehensablauf unterlässt, sondern nur, wenn nach Vorliegen des manipulierten Ergebnisses eine Person eingeschaltet wird, die nun die schädigende Vermögensverfügung trifft.

Zu § 225a

Diese Bestimmung ist neu und dient der Umsetzung von Art. 7 CCC. Sie bezweckt die Bestrafung der Fälschung von Computerdaten als Gegenstück zur herkömmlichen Urkundenfälschung.

Die Formulierung lehnt sich denn auch eng an diejenige des § 223 StGB (Urkundenfälschung) an. Die Tathandlung besteht im Herstellen falscher Daten oder in der Verfälschung echter Daten durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten. Bezüglich des Datenbegriffs ist wiederum auf den neu zu schaffenden § 74 Abs. 3 StGB zu verweisen. Inhaltlich sind unter der Herstellung falscher Daten parallel zu § 223 StGB Daten zu verstehen, die nicht von der Person stammen, die als Hersteller bzw. Aussteller angegeben ist. Die Verfälschung echter Daten hingegen setzt den Bestand von Daten voraus, die nachträglich durch Austausch des Ausstellers oder einen anderen gedanklichen Inhalt geändert werden. Beide Begehungsformen spielen vor allem im Bereich der elektronischen Urkunde sowie der elektronischen Signatur ein Rolle.

Auf der subjektiven Tatseite ist der erweiterte Vorsatz erforderlich, dass diese Daten im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden.

5. VERFASSUNGSMÄSSIGKEIT / RECHTLICHES

Die Vorlage wirft keine verfassungsrechtlichen Fragen auf. Es stehen ihr keine diesbezüglichen Bestimmungen entgegen.

6. REGIERUNGSVORLAGE

Gesetz

vom ….

über die Abänderung des Strafgesetzbuches

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

Das Strafgesetzbuch vom 24. Juni 1987, LGBl. 1988 Nr. 37, in der geltenden Fassung, wird wie folgt abgeändert:

§ 74 Abs. 1 Ziff. 8 und Abs. 3

8. Computersystem: sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen.

3) Im Sinne dieses Gesetzes sind Daten sowohl personenbezogene und nicht personenbezogene Daten als auch Programme.

§ 118a (neu)

Widerrechtlicher Zugriff auf ein Computersystem

1) Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem überwindet, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

3) Wer die Tat als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

§ 119a (neu)

Missbräuchliches Abfangen von Daten

1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elekt-

romagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

§ 126b (neu)

Störung der Funktionsfähigkeit eines Computersystems

1) Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

2) Wer durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer die Tat als Mitglied einer kriminellen Vereinigung begeht, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

§ 126c (neu)

Missbrauch von Computerprogrammen oder Zugangsdaten

1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Da-

tenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder

2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, mit dem Vorsatz herstellt, einführt, vertreibt, veräussert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Ziff. 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

§ 148a Abs. 1

1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmässig zu bereichern, einen anderen dadurch am Vermögen schädigt, dass er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

§ 225a (neu)

Datenfälschung

Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

II.

Inkrafttreten

Dieses Gesetz tritt am Tage der Kundmachung in Kraft.