Österreichischer
Rechtsanwaltskammertag
Der Präsident

Die österreichischen
Rechtsanwälte

An das
Bundesministeriums für Justiz, Abt IV 1
zHd. LStA Dr. Christian Manquet
Museumstrasse 7
1070 Wien

per E-Mail: team.s@bmj.gv.at

Wien, am 22. Dezember 2010

21/ 10/184

BMJ-S886.041/0001-IV 1/2010
Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates ("Cyberkriminalität")

Referent: MMag. Dr. Rupert Manhart, LL.M. (LSE), Rechtsanwalt in Vorarlberg

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag (ÖRAK) ist die gesetzlich eingerichtete Vertretung der Rechtsanwälte in Österreich und als solche zur Wahrung der Rechte und Angelegenheiten sowie zur Vertretung der österreichischen Rechtsanwälte auf nationaler, europäischer und internationaler Ebene berufen. Als solcher obliegen ihm besonders die Erstattung von Gesetzesvorschlägen und Stellungnahmen zu Gesetzesentwürfen sowie die Anzeige von Mängeln der Rechtspflege und Verwaltung bei der zuständigen Stelle und die Erstattung von Vorschlägen zur Verbesserung von Rechtspflege und Verwaltung.

Der ÖRAK bedankt sich für die Übermittlung des Vorschlags für eine **Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates** und nimmt hierzu wie folgt Stellung:

1. Der ÖRAK teilt grundsätzlich die Auffassung, dass Cyberkriminalität nicht an nationalen Grenzen haltmacht, sodass ein einheitliches Vorgehen der

europäischen Strafverfolgungsbehörden zu begrüßen ist. Eine Harmonisierung des materiellrechtlichen Strafrechtes auf europäischer Ebene ist jedoch weder ausreichend noch nützlich, um die Verfolgung der Cyberkriminalität zu verbessern, solange die Ermittlung und Verfolgung der Täter an der fehlenden grenzüberschreitenden Zusammenarbeit und der technischen Ausstattung und Ausbildung der Behörden scheitert. Ferner darf nicht vergessen werden, dass Cyberkriminalität nicht nur innereuropäische Grenzen überschreitet, sondern ein Kontinente übergreifendes internationales Phänomen ist, sodass Regelungen auf europäischer Ebene zu kurz greifen. Darüber hinaus ist eine Intensivierung der grenzüberschreitenden Strafverfolgung ohne gleichzeitige Verbesserung sowohl der Strafverteidigung als auch des Opferschutzes abzulehnen, sodass in diesen Bereichen flankierende Maßnahmen zu setzen sind.

2. Wie der Richtlinienentwurf selbst anführt, besteht im Bereich der Bekämpfung der Cyberkriminalität bereits ein enges Netz internationaler Regeln, insbesondere durch das Übereinkommen des Europarates über Computerkriminalität (das auch von nichteuropäischen Staaten wie den USA ratifiziert wurde – im Folgenden „Cybercrime-Konvention“) und den Rahmenbeschluss 2005/222/JI des Rates. Eine vollständige Evaluierung dieser beiden Rechtsakte liegt bislang nicht vor, da die Cybercrime-Konvention bislang erst von 30 Staaten (davon 15 Mitgliedstaaten) ratifiziert wurde und der angeführte Rahmenbeschluss noch nicht in allen Mitgliedstaaten vollständig umgesetzt ist. Vor Erlassung eines neuen Rechtsaktes sollte daher die vollständige Umsetzung bzw Ratifikation der bestehenden Rechtsakte vorangetrieben werden. Bis dahin kann nicht nachvollzogen werden, dass Handlungsbedarf auf europäischer Ebene zur Schließung von Strafbarkeitslücken besteht.

   Im Vergleich mit dem Rahmenbeschluss 2005/222/JI und der Cybercrime-Konvention des Europarates ist festzustellen, dass durch den Richtlinienentwurf Kriminalpolitik lediglich durch Erhöhung der Strafdrohungen und Beseitigung von – wohl begründeten – Ausnahmen von der Strafbarkeit gemacht werden soll, ohne die grundsätzlichen Probleme der Verbrechensbekämpfung im Bereich der Internetkriminalität anzugehen.

3. Art 83 AEUV erlaubt dem Europäischen Parlament und dem Rat die Erlassung von Mindestvorschriften zur Festlegung von Straftaten und Strafen in Bereichen „besonders schwerer Kriminalität“, die zugleich eine grenzüberschreitende Dimension aufweisen. Der ÖRAK bezweifelt, dass dieser kompetenzrechtlichen Grundlage mit der nur für Art 3, 4 und 5 RL-E vorgesehenen Möglichkeit, „leichte Fälle“ – was immer unter diesem unklaren Begriff zu verstehen ist – von der Umsetzung auszunehmen, entsprochen wird.

4. Der vorliegende Richtlinienentwurf lässt aufgrund mangelnder begrifflicher Klarheit Spielräume bei der Umsetzung, die nicht nur das Ziel einheitlicher Mindestbestimmungen in allen Mitgliedstaaten konterkarieren, sondern auch die erforderliche Bestimmtheit strafrechtlicher Regelungen vermissen lassen. In höchstem Maße ausfüllungsbedürftig ist, was unter einem „leichten Fall“ (Art 3, 4 und 5 RL-E) zu verstehen ist; strafrechtlich nicht erhellend sind die Erläuterungen, dass damit etwa „Handlungen junger Leute“ ausgenommen sein

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

sollen, die „ihre Kenntnisse […] unter Beweis stellen wollen“. Genauso wenig klar ist der Begriff des „Abfangens“ (Art 6 RL-E) von Datenübermittlungen. Und wann ist eine Vorrichtung „in erster Linie“ (Art 7 lit b RL-E) dafür ausgelegt oder hergerichtet, eine Straftat zu begehen?

5. Die vorgeschlagenen Strafen und Straftatbestände sind gemessen am Ziel der Bekämpfung der Cyberkriminalität und insbesondere im Vergleich zum österreichischen Strafrecht überschießend. Das StGB stellt bereits jetzt in Umsetzung der einschlägigen internationalen Rechtsakte die im Richtlinienentwurf genannten Straftaten im Wesentlichen geschlossen unter Strafe, sieht jedoch – dem Unrechtsgehalt der Taten entsprechend – zum Teil deutlich geringere Strafdrohungen vor. Zu schließende Strafbarkeitslücken bestehen nicht.

   Die in Art 3 RL-E (Rechtswidriger Zugang zu Informationssystemen) und Art 6 RL-E (Rechtswidriges Abfangen von Daten) vorgeschlagenen Delikte entsprechen im Wesentlichen § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) bzw § 119a StGB (Missbräuchliches Abfangen von Daten), die Österreich in Umsetzung der von Art 2 und 3 der Cybercrime-Konvention erlassen hat. Die österreichischen Strafbestimmungen sind jedoch nicht nur klarer gefasst, sondern sind auch – systematisch richtig – nur Ermächtigungsdelikte. Warum darüber hinaus der Richtlinienentwurf in Art 3 die noch in Art 2 Abs 2 des Rahmenbeschlusses 2005/222/JI vorgesehene Ausnahme von der Strafbarkeit für ungesicherten Informationssysteme beseitigt, ist nicht begründbar.

   Die gemäß Art 4 RL-E (Rechtswidriger Systemeingriff) und Art 5 RL-E (Rechtswidriger Eingriff in Daten) zu bestrafenden Handlungen unterliegen in Österreich den § 126a StGB (Datenbeschädigung) und § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems). „Groß angelegte Cyberattacken“ wie DDoS-Angriffe (Distributed Denial of Service), die auch unter Verwendung von Botnetzen ausgeführt werden, sind in Österreich nach diesen Bestimmungen je nach Schwere des Angriffes mit bis zu fünf Jahren Freiheitsstrafe bedroht. Die Verfolgung scheitert in der Praxis daher nicht an der fehlenden Strafbarkeit, sondern an der Rückverfolgbarkeit der Täter, die sich hinter weit verzweigten Netzwerken verstecken. Hier nützt es auch nichts, erschwerende Umstände (Art 10 RL-E) zu normieren, solange es nicht gelingen kann, die Täter zur Verantwortung zu ziehen.

   Art 7 RL-E (Tatwerkzeuge), der im Wesentlichen § 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten) bzw Art 6 der Cybercrime-Konvention entspricht, verlagert die Strafbarkeit weit ins Vorbereitungsstadium eines Angriffs auf ein Informationssystem und normiert eine Höchststrafdrohung von mindestens zwei Jahren Freiheitsstrafe (Art 9 Abs 1 RL-E). Gerade bei den in Art 7 RL-E umschriebenen Taten handelt es sich aber oft um „Handlungen von jungen Leuten“, die „ihre Kenntnisse […] unter Beweis stellen“ wollen; warum hier auch jeder „leichte Fall“ mit Freiheitsstrafe von zwei Jahren strafbar sein soll, ist nicht nachvollziehbar. Um ein legistisches Versehen dürfte es sich bei der Verwendung des Wortes „unbefugt“ in Art 7 RL-E handeln, denn ein

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

unbefugtes (im Sinne der Definition des Art 2 lit d RL-E) Herstellen usw ist wohl kaum denkbar.

Angesichts der bestehenden hohen internationalen Regelungsdichte, deren Effizienz nicht durch den Inhalt der Rechtsakte, sondern durch mangelhafte Umsetzung und Zusammenarbeit der Strafverfolgungsbehörden beschränkt wird, ist daher nach Ansicht des ÖRAK der vorliegende Richtlinienentwurf aus grundsätzlichen Überlegungen abzulehnen. Eine Neuregelung ist zurzeit nicht erforderlich; vielmehr sollte auf die lückenlose Umsetzung des Rahmenbeschlusses und die Ratifizierung der Cybercrime-Konvention durch sämtliche Mitgliedstaaten hingewirkt werden. Der Entwurf ist weder nützlich noch ausreichend, um die Verfolgung von Cyberkriminalität zu fördern und den jüngsten Bedrohungen durch groß angelegte Cyberangriffe zu begegnen. Eine kriminalpolitische Notwendigkeit zur Verschärfung der Strafdrohungen besteht nicht, wie auch keine Strafbarkeitslücken vorliegen. Darüber hinaus leidet der vorliegende Richtlinienentwurf an begrifflicher Unklarheit. Der ÖRAK empfiehlt daher, den vorliegenden Richtlinienentwurf abzulehnen.

Mit freundlichen Grüßen

Dr. Gerhard Benn-Ibler

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at