Positionen des BACDJ zum 69. Deutschen Juristentag
München, 18. bis 21. September 2012

Strafrecht

Anpassung des Straf(prozess)rechts an die Informationsgesellschaft

Die Entwicklung zur Informationsgesellschaft stellt neue Anforderungen an das Strafrecht und Strafprozessrecht einschließlich der strafrechtlichen Nebengebiete. Die erforderliche grundlegende Überarbeitung und Anpassung dieser Rechtsgebiete hat unter Berücksichtigung der Internationalität und Anonymität des Internets sowie der Loslösung der Daten von der Körperlichkeit und der spezifischen Vulnerabilität informationstechnischer Systeme zu erfolgen. Bei der Überarbeitung der Rechtsvorschriften ist insbesondere die stetig fortschreitende technische Entwicklung abzubilden. Bei aller Unterschiedlichkeit der Rechtssysteme sollte eine weitere Harmonisierung der einschlägigen Vorschriften auf internationaler Ebene in Angriff genommen werden, denn das „WordWide-Web“ macht nicht an den Grenzen einzelner Staaten halt.

Die Cybercrime-Konvention des Europarates ist der richtige Ansatz, der konsequent weiterentwickelt werden sollte. Insbesondere sollten weitere Staaten ermutigt werden, der Konvention beizutreten. In diesem Geiste ist auch der internationale politische Konsens zur Strafbarkeit von Cyberkriminalität voranzutreiben. Die durch die internetbedingte exterritoriale

B undes
A rbeitskreis
C hristlich
D emokratischer
J uristen

BACDJ
der CDU Deutschlands

Konrad-Adenauer-Haus
Klingelhöferstraße 8
10785 Berlin

Telefon: 030 22070-315
Telefax: 030 22070-319

E-Mail: bacdj@cdu.de

CDU

Anwendung des Strafrechts entstehenden Kompetenzkonflikte sind verstärkt in den Focus zu nehmen.

Eine interdisziplinär und international besetzte Sachverständigenkommission zur Weiterentwicklung des deutschen Straf(prozess)rechts könnte die notwendigen Vorschläge erarbeiten, die dann in den parlamentarischen Prozess eingeführt werden müssen. Dabei werden die folgenden Punkte einer besonderen Betrachtung zu unterziehen sein:

Im Rahmen der Fortentwicklung des materiellen Strafrechts ist eine Zusammenfügung und Systematisierung der einschlägigen Straftatbestände des Strafgesetzbuches erforderlich, die derzeit noch in unterschiedlichen Abschnitten geregelt sind. So befinden sich die Regelungen zum Ausspähen und Abfangen von Daten (§§ 202 a und b StGB) sowie der Vorbereitung hierzu (§ 202 c StGB) im 15. Abschnitt des StGB unter der Überschrift: „Verletzung des persönlichen Lebens- und Geheimbereiches“. Die Datenveränderung (§ 303 a StGB) und Computersabotage (§ 303 b StGB) ist sachfremd im 27. Abschnitt unter „Sachbeschädigung“ geregelt. Der Computerbetrug (§ 263 a StGB) ist im 22. Abschnitt geregelt. Vor dem Hintergrund einer Verbesserung der Übersichtlichkeit wäre ebenso eine Zusammenführung mit den Straftatbestimmungen des Datenschutz- und Urheberrechts im StGB vorzugswürdig. Der durch das Urheberrecht gewährte Schutz sollte nicht generell auf organisierte und geschäftsmäßig handelnde Straftäter begrenzt werden, da ansonsten die Durchschlagskraft des Urheberrechts leiden würde. Der Prozess der Systematisierung der

einschlägigen Straftatbestände sollte auch eine Anpassung der Strafrahmen und Begrifflichkeiten einschließen. Eine Eingrenzung der Strafbarkeit durch das Tatbestandsmerkmal der Nachteilszufügung (bei §§ 303 a und b StGB) wird abgelehnt. Änderungsbedarf besteht darüber hinaus im Sexualstrafrecht. Neben einer Vorverlagerung der Strafbarkeit beim Erwerb von kinder- und jugendpornografischen Schriften sollte das „Grooming“, also die sexuell motivierte Kontaktaufnahme von Pädophilen zu Kindern, konsequent unter Strafe gestellt werden.

Die Löschung illegaler Daten an ihrer Quelle ist einer Sperrung illegaler Internetseiten vorzuziehen. Zum Schutz des Urheberrechts und zur Schärfung des diesbezüglichen Rechtsbewusstseins sind Warnhinweismodelle ein wirkungsvoller Baustein.

Bei der Aufklärung der Cyberkriminalität sollten einerseits vorhandene Ermittlungsmöglichkeiten konsequenter ausgeschöpft werden, indem beispielsweise die digitale Forensik einen Schwerpunkt bei Aus- und Fortbildung von Polizeibeamten, Richtern und Staatsanwälten einnimmt. Auch die verstärkte Forschung auf diesem Gebiet und die Zusammenarbeit zwischen Sicherheitsbehörden und Wissenschaft ist förderlich, um Defizite abzubauen.

Darüber hinaus müssen im Zuge der erforderlichen Überarbeitung und Anpassung der Strafprozessordnung an die Informationsgesellschaft verfassungs- und europarechts-konforme gesetzliche Grundlagen für die Vorratsdaten-speicherung, die

Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung geschaffen werden. Erforderlich ist in diesem Zusammenhang auch die durch die Entscheidung des Bundesverfassungsgerichts v. 24.02.2012 (1 BvR 1299/05) notwendig gewordene Schaffung einer gesetzlichen Grundlage für die Auskunftserteilung über Passworte, PIN-Nummern und sogenannte dynamische IP-Adressen, da die bestehenden Regelungen über die Speicherung und Verwendung der Daten unter Einschränkungen nur noch bis 30.06.2013 anwendbar sind. Eigenständige Regelungen über die Herausgabepflicht für Daten, die insbesondere die erforderlichen Mitwirkungs-pflichten beim Ausdruck und der Entschlüsselung beinhalten, müssen geschaffen werden. Da die klassische (physische) Post mehr und mehr durch elektronische Post ersetzt wird und bei letzterer je nach Zugriffsstadium die Arbeit in der Praxis erschwerende unterschiedliche Rechtsgrundlagen für die Überwachung bestehen, ist eine Vereinheitlichung der Zugriffsmöglichkeiten auf die E-Mail-Kommunikation erforderlich.

In der Praxis der Strafverfolgung kommt der Öffentlichkeitsfahndung über soziale Netz-werke („Facebook-Fahndung“) eine immer größere Bedeutung zu. Um den Strafverfolgungsbehörden eine verlässliche Rechtsgrundlage hierfür zu geben, sollten die einschlägigen Vorschriften über die Öffentlichkeitsfahndung in der StPO (§§ 131 ff. StPO) überarbeitet werden. Entsprechend ist auch eine Anpassung der RiStBV erforderlich, wonach derzeit die Einbindung privater Internetanbieter in die Öffentlichkeitsfahndung gerade nicht erfolgen soll.

Die Kooperation der Strafverfolgungsbehörden auf internationaler Ebene zur Bekämpfung der Cyberkriminalität ist zu fördern und fortzuentwickeln, z. B. auch durch einen personellen Austausch.

Auf nationaler Ebene sollte die Einrichtung von Schwerpunktstaatsanwaltschaften und von Sonderzuständigkeiten bei den Gerichten vorangetrieben werden. Denn die Bekämpfung der Cyberkriminalität erfordert eine umfangreiche Spezialisierung, die in „Mischdezernaten“ nicht mehr geleistet werden kann. Sonderzuständigkeiten sind auch wegen der erforderlichen Zusammenarbeit auf internationaler Ebene erforderlich.

Die Überarbeitung des Informationsstrafrechts sollte von einer umfassenden empirisch-kriminologischen Studie zur Cyberkriminalität und deren Auswirkungen begleitet werden, um die bislang nur unzureichend erforschten Deliktsfelder zu erhellen und verlässliche Datengrundlagen – unter Einbeziehung des Dunkelfeldes – zu bekommen.