Rainer Franosch
Oberstaatsanwalt

Marburg, den 15. September 2015

Hessische Zentralstelle zur Bekämpfung der Internetkriminalität
(z. Zt. abgeordnet an das Hessische Ministerium der Justiz)

Betr.: Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages

Anhörung zu dem
a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD
Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten
BT-Drucksache 18/5088

b) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten
BT-Drucksache 18/5171

c) Antrag der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE
Auf Vorratsdatenspeicherung verzichten
BT-Drucksache 18/4971

Zur Vorbereitung der Anhörung gebe ich die nachfolgende Stellungnahme ab, die sich vor allem auf den Phänomenbereich Cybercrime bezieht.

1) Notwendigkeit der Vorratsdatenspeicherung (VDS) für die effektive Bekämpfung von Cybercrime (zu BT-Drucksache 18/4971)

a) Die Bedrohung

Als „Cybercrime“ (früher „Informations- und Kommunikationskriminalität“ oder auch verkürzend „Internetkriminalität“) bezeichnet man alle kriminellen Handlungen, die

- gegen elektronische Kommunikationsnetze und Informationssysteme (Cybercrime im engeren Sinn, englisch: „cyber-dependent crimes“, z.B. Datenveränderung, § 303a StGB, Ausspähen von Daten, § 202a StGB etc.) oder
- mittels derartiger Netze und Systeme verübt werden (Cybercrime im weiteren Sinn, englisch: „cyber-enabled crimes“, also Taten, bei denen das Internet als virtuelles Tatwerkzeug für die Begehung von Straftaten genutzt wird, z.B. Verbreitung von Kinderpornografie, Volksverhetzung, Verbreitung extremistischer

Propaganda, öffentliche Aufforderung zu Straftaten, betrügerisches Anbieten von Waren und Dienstleistungen oder Geldanlagen, verbotenes Glücksspiel, unlautere Werbung, Urheberrechtsverletzungen, Verkauf von Waffen, Betäubungsmitteln oder verbotenen Medikamenten)[1]

Auch wenn die meisten Internet-Straftaten Betrugsdelikte sind (Anteil in der PKS 2014: 74,2 Prozent[2]), darf die gesamtgesellschaftliche Bedrohungslage durch Cybercrime aus mehreren Gründen nicht unterschätzt werden.

Zunächst ist festzuhalten, dass jeder – nicht nur die Internetnutzer – Opfer von Cybercrime werden kann, sei es der einzelne Bürger, Unternehmen oder auch staatliche Stellen.
Mit der Zunahme der Bedeutung der IT als Bestandteil des Alltags der Bürger steigen die Manipulations- und Angriffsmöglichkeiten auf Seiten der Cyberkriminellen. Cyberkriminelle handeln global, nationale Grenzen spielen keine Rolle, wobei Handlungs-, Taterfolgs- und Aufenthaltsorte von Tätern und Opfern irrelevant sind.

Das Internet bringt alles und alle zusammen. Bucht ein Bürger in Frankfurt am Main eine Urlaubsreise über Internet, hat der am anderen Ende der Welt wartende Straftäter in Echtzeit potentiellen Zugriff auf den für die Buchung genutzten Computer. Aber auch diejenigen, die ihre Urlaubsreise nicht selbst über Internet buchen, können Opfer von Cybercrime werden, z.B. dadurch, dass die Täter sich Zugriff auf die persönlichen Daten durch einen Angriff auf die Server des Reisevermittlers verschaffen.

Das bedeutet kurz gefasst, dass durch das Internet erstmals in der Geschichte der Kriminalität Straftaten

- weltweit und
- unter Überwindung jeder räumlichen Distanz zwischen Täter und Opfer in Echtzeit

begangen werden können.

Der im Januar 2014 bekannt gewordene Diebstahl von 16 Millionen E-Mail-Adressen belegt beispielhaft die Schadensdimensionen im Phänomenbereich Cybercrime. Der Diebstahl digitaler Identitäten, also der Diebstahl von Daten, ist ein Massenphänomen.

Die digitale Identität ist die Summe aller Möglichkeiten und Rechte des einzelnen Nutzers sowie seiner Aktivitäten innerhalb der Gesamtstruktur des Internets. Konkret handelt es sich um alle Arten von Nutzer-Accounts, also zum Beispiel Zugangsdaten in den Bereichen Kommunikation (E-Mail- und Messengerdienste), E-Commerce (Onlinebanking, internetgestützte Vertriebsportale aller Art), berufsspezifische Informationen (z. B. Nutzung eines Homeoffice für den Zugriff auf firmeninterne technische Ressourcen) und E-Government (z.B. elektronische Steuererklärung oder elektronische Bußgeldakte).

---

[1] vgl BKA, Bundeslagebild Cybercrime 2013, S. 5; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF

[2] Es ist allgemein bekannt, dass die Dunkelfeldproblematik bei Cybercrime besonders ausgeprägt ist, vgl. z.B. http://www.heise.de/newsticker/meldung/Cybercrime-Das-Dunkelfeld-wird-groesser-2303524.html; BKA, Bundeslagebild Cybercrime 2013, S. 10 m.w.N.

Darüber hinaus sind auch alle anderen zahlungsrelevanten Informationen (insbesondere Kreditkartendaten einschließlich der Zahlungsadressen sowie weiterer Informationen) Bestandteil der digitalen Identität. Die Täter nutzen Schadprogramme, um Eingaben des Computernutzers auszuspähen sowie Anmeldedaten zu erlangen und Transaktionen durchführen zu können; sie gehen dabei häufig arbeitsteilig und unter Nutzung professioneller Strukturen vor. Anschließend werden die Daten entweder von den Tätern selbst eingesetzt oder aber an Dritte weiterveräußert, welche die Daten dann kriminell einsetzen.

Legt man die Ergebnisse einer Online-Umfage aus dem Jahr 2013 zugrunde, wurde schon rund ein Fünftel der Deutschen (21 Prozent) Opfer von Identitätsdiebstahl oder -missbrauch, weitere 27 Prozent können nicht ausschließen, dass ihre personenbezogenen Daten schon missbraucht wurden[3]. Diese Zahlen gehen weit über die polizeilich registrierten Fälle des Ausspähens/Abfangens von Daten hinaus und sind ein Beleg für das hohe Dunkelfeld im Bereich Cybercrime.

Aber das Internet bietet für die Täter noch weit mehr: Immer mehr verlagert sich der Handel mit illegalen Waren und Dienstleistungen in das Internet.
Unter Nutzung der Informationstechnologie und digitaler Währungen gebrauchen Cyberkriminelle das sogenannte „Darknet“, jenen Teil des Internets, der nicht über normale Suchmaschinen auffindbar ist und der als versteckter Dienst z.B. im TOR-Netzwerk die Anonymität der Nutzer durch Verschleierung der Verkehrsdaten wahrt oder ein „anonymes“ Hosting ermöglicht. Über solche Online-Plattformen werden hier beispielsweise der illegale Handel mit Drogen, Waffen und Kreditkartendaten betrieben oder illegale Dienstleistungen, wie z.B. die Durchführung von DDoS-Attacken, angeboten.

Diese arbeitsteilige Cyberunterwelt wird zu Recht als „Underground Economy“ bezeichnet. Täter kaufen und verkaufen illegale Waren und Dienstleistungen, finden sich zu international agierenden Banden zusammen, ohne sich ein einziges Mal im wahren Leben getroffen zu haben. Es existiert ein funktionierender globaler Markt, auf dem Angriffswerkzeuge, Erkenntnisse über Schwachstellen in Betriebssystemen oder Schadsoftware eingekauft oder als Dienstleistung in Auftrag gegeben werden können („Crime-as-a-Service“).

Die nahezu unbegrenzten Möglichkeiten von Cybercrime führen dazu, dass sich auch die organisierte Kriminalität zunehmend dieses Bereiches annimmt.[4]

Naturgemäß sind derartige, allgemeine Beschreibungen von Kriminalitätsphänomenen blass und wenig eindrücklich.

Daher nachfolgend einige Beispiele:

[3] Online-Umfrage der SCHUFA Holding AG und des Marktforschungsinstituts Innofact AG, http://www.presseportal.de/pm/25316/2556036
[4] Europol, Internet Organised Crime Threat Assessment (iOCTA) 2014, S. 9

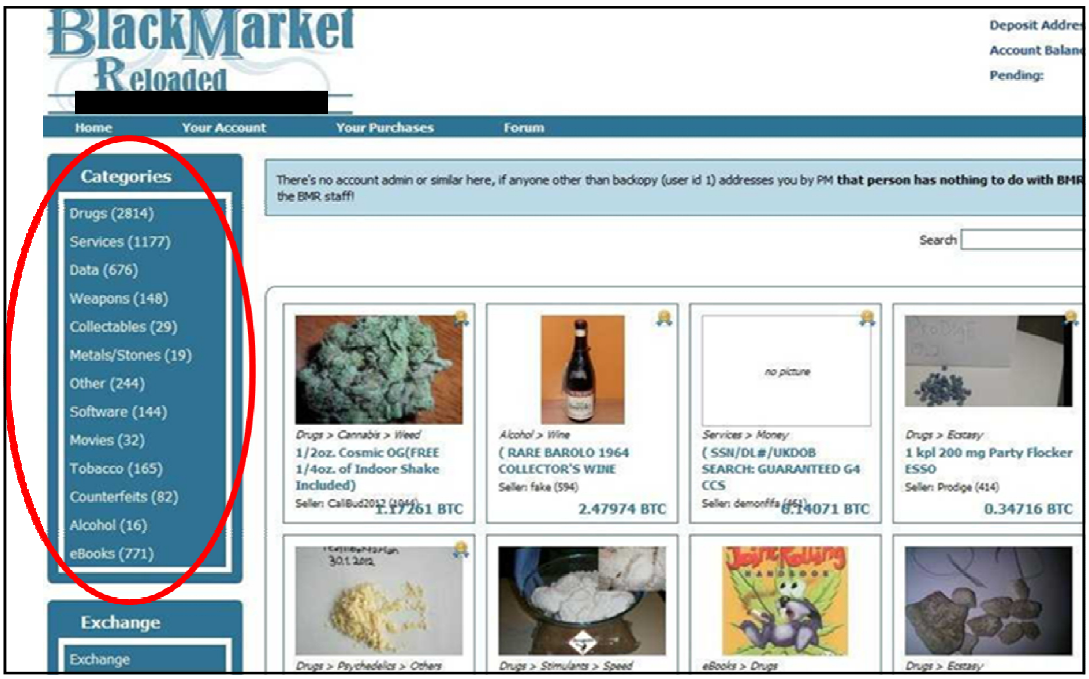

Abb. 1

Abbildung 1 zeigt die Startseite eines Marktplatzes im Darknet. Angeboten werden u.a:

- Drogen (Abb. 2 und 3)
- Dienstleistungen (illegaler Art)
- Daten (ausgespähte)
- Waffen (Abb. 4 und 5)
- Kinderpornographie
- gefälschte Dokumente und Falschgeld

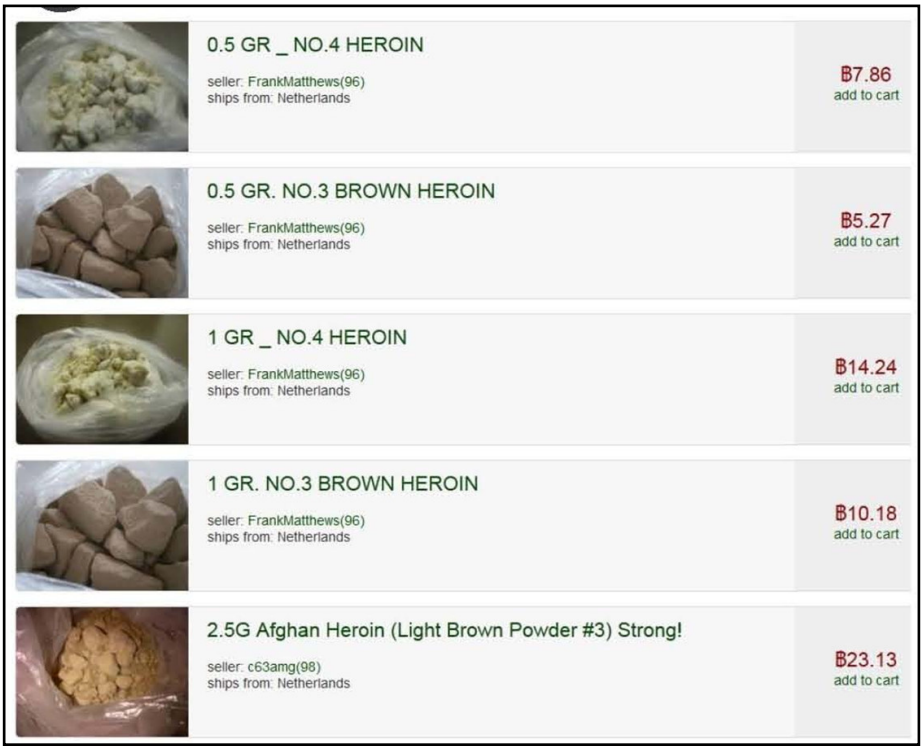

Abb. 2: Im Internet sind alle Drogen erhältlich, auch Heroin.

Abb. 3: Ware eines Online-Dealers von nur einem Tag (rd. 4,5 kg Cannabis und 0,5 kg Haschisch), beschlagnahmt in einer Packstation, adressiert an verschiedene Abnehmer aus ganz Deutschland.

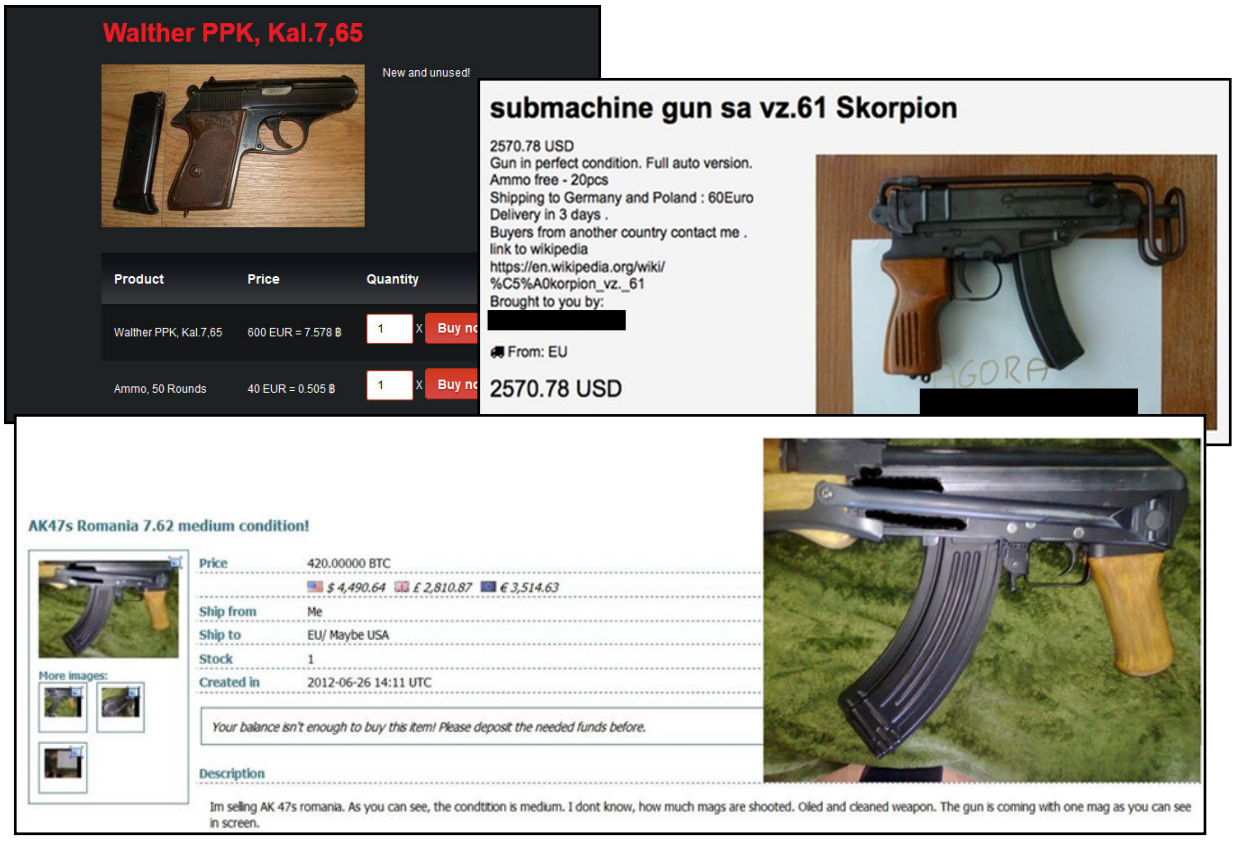

Abb. 4: Das Angebot an Waffen im Darknet ist unbegrenzt, einschließlich Kriegswaffen.

Abb. 5: Diese Pistole mit Schalldämpfer wurde in einem hessischen Ermittlungsverfahren bei einem Darknet-Verkäufer beschlagnahmt.

Neben Waren werden auch Dienstleistungen angeboten, darunter auch die Begehung von Tötungsdelikten gegen Entgelt:

Abb.6

Dass Auftragsmorde über das Internet verabredet werden, ist aus US-amerikanischen Ermittlungsverfahren bereits bekannt[5].

Auch in Hessen hat es bereits einen derartigen Fall gegeben:

Im Frühjahr 2014 kam der Angeschuldigte A via Internet über das „Darknet“ in Kontakt mit dem Mitangeschuldigten B. B. war im Forum http://germanyXXX.onion schon seit längerem auf der Suche nach Arbeit und bot gegen lukrative Bezahlung die Erledigung von Diensten aller Art an:

[5] z.B. http://www.bloomberg.com/news/articles/2014-12-09/us-says-silk-roads-ulbricht-solicited-six-murders-for-hire

„Fast egal was! Transporter, Mafia, Hitman“

Der Angeschuldigte A beauftragte B über Internet, gegen Entgelt für ihn den C zu töten, da dieser seit Mitte März 2014 der neue Lebensgefährte seines Ex-Freundes D war. Die Trennung von D hatte der von massiver Eifersucht sowie Missgunst geplagte A nicht verwunden. Für den geplanten Mord erhielt B eine Anzahlung in Höhe von 3.000,00 €, zusätzliche 10.000.- € waren als „Erfolgshonorar“ vereinbart worden. B suchte sodann das Opfer C auf und versuchte, ihm mit einem Messer mit 20 cm langer Klinge die Kehle durchzuschneiden. C konnte mit Hilfe von Zeugen den Angriff abwehren und überlebte mit erheblichen Schnittverletzungen im Hals-, Gesichts- und Schulterbereich sowie an den Händen.

Auszug aus einer E-Mail des Auftragsmörders B an den Auftraggeber A:

Du willst wissen wie Skrupellos ich bin, ich kann z.b. mit einem Grinsen im Gesicht jemandem ein Messer in den Hals stecken. Wie gesagt ich habe mit meinem Leben abgeschlossen, schon vor Jahren.

Und ich weise nochmals darauf hin das ich kein abgefuckter Gesetzesdiener bin, zu gern würde ich sie jagen und auslöschen.

Abb. 7

Ohne die Möglichkeit, anonym über das Darknet nach einem Auftragsmörder zu suchen, wäre es dem in kriminellen Dingen völlig unerfahrenen A nicht gelungen, die Verbindung zu einer tatgeneigten Person aufzunehmen.

- Kinderpornographie

Der sexuelle Missbrauch von Kindern wird durch das Internet ebenfalls massiv gefördert. Dies betrifft nicht nur die Kinderpornographie, die nahezu ausschließlich netzbasiert unentgeltlich im Tausch, aber auch entgeltlich über professionelle Webseiten vertrieben wird, sondern auch die internetgestützte Verabredung von Tätern zu Treffen, um gemeinsam Kinder zu missbrauchen. Auch der Missbrauch von Kindern durch Erwachsene vor der Webcam ist ein zunehmendes Phänomen.

Es ist festzustellen, dass sich im Internet organisierte pädokriminelle Strukturen neuer Qualität herausgebildet haben. In umfangreichen Ermittlungen in diesem Phänomenbereich seit 2009 konnte nicht nur festgestellt werden, dass es festgefügte, abgeschottete und hierarchisch aufgebaute geschlossene Benutzerkreise zum Austausch von Kinderpornographie gibt, sondern auch exklusive Bereiche, in denen der reale sexuelle Missbrauch von Kindern und die Weitergabe des so selbst produzierten Materials als Zugangsvoraussetzung dienen. Das Motto eines Bereiches in einem Pädophilen-Forum lautete:

„Don’t ask for membership if you haven’t got your own daughter to share”.

In dem Umfangsverfahren „Geisterwald“ konnten weltweit insgesamt über 160 Personen als Mitglieder solcher geschlossener Strukturen identifiziert werden. Rund 30% dieser Personen haben nicht lediglich Kinderpornographie konsumiert und weiterverbreitet, sondern selbst Kinder missbraucht. Das Verfahren war ein Erfolg, weil

zum Zeitpunkt des Beginns der Ermittlungen im Jahr 2009 die Regelung zur Vorratsdatenspeicherung noch in Kraft war.

Schließlich ist noch das sog. „Cybergrooming“ zu nennen, also die internetbasierte Kontaktaufnahme von pädophilen Erwachsenen zu Kindern, um diese zu sexuellen Handlungen entweder an sich selbst vor einer Webcam oder zu Realtreffen zum Zwecke des Missbrauch zu bringen. In einem hessischen Ermittlungsverfahren mit dem Einsatz nicht offen ermittelnder Polizeibeamter, die als vermeintliche Kinder auftraten, nahmen innerhalb von nur acht Tagen 395 Personen mit den als Kindern auftretenden Polizeibeamten Kontakt auf und wirkten im Sinne von § 176 Abs. 4 Nr. 3 StGB auf diese ein.

Im Zusammenhang mit sexueller Gewalt gegen Kinder dient das Internet indes nicht nur als Transportmedium für die inkriminierten Bilder und Filme. In einschlägigen Foren und Chatrooms finden Pädophile darüber hinaus Gleichgesinnte, mit denen sie sich austauschen können. Es ist zu beobachten, dass im Rahmen derartiger Kommunikationsgruppen eine Radikalisierung stattfindet. Teilnehmer, die noch Skrupel haben, Kinder zu missbrauchen, werden ermuntert, diese fallen zu lassen (siehe Bildunterschrift unter Abb. 8).
Die wechselseitige Stimulierung und Befeuerung der sexuellen Fantasien in Internetforen ist eine der Ursachen für die zunehmende Brutalisierung des durch Kindesmissbrauch entstehenden Bild- und Filmmaterials. Abbildungen des Missbrauchs von Säuglingen und Kleinkindern oder sadistischer Gewalthandlungen an Kindern waren noch vor 10 Jahren selten, heute findet man sie auf sehr vielen der sichergestellten Täterrechner (Abb. 8, 9):

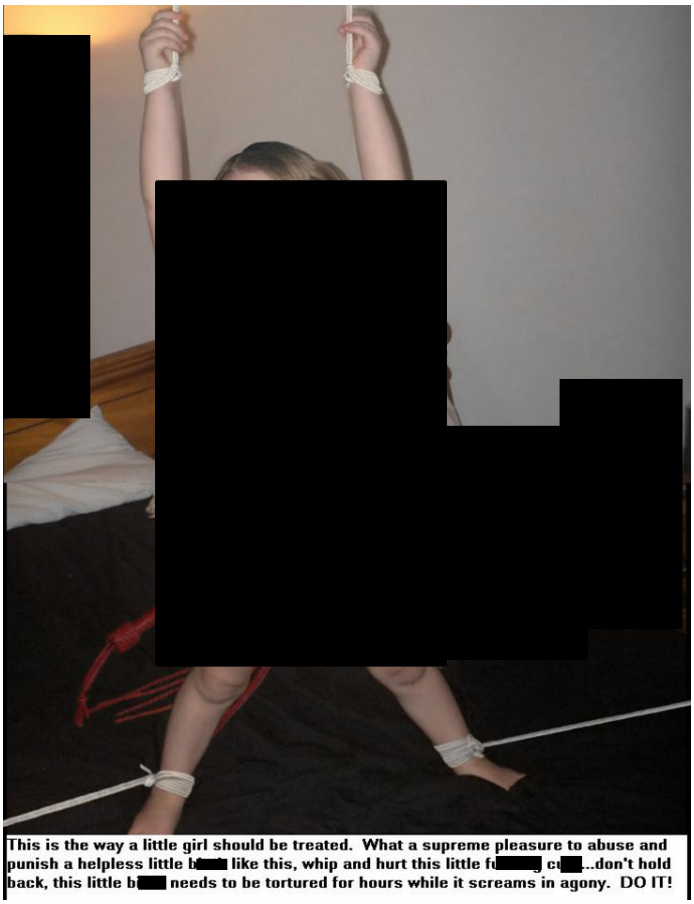

Abb. 8

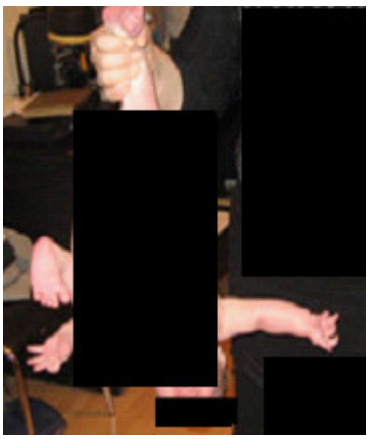

Abb. 9

- Terrorismus

Auch für den politisch oder religiös motivierten Terrorismus ist das Internet von unschätzbarer Bedeutung. Es dient wie kein anderes Medium der weltweiten Kommunikation und Planung von Anschlägen, aber vor allem auch der Rekrutierung des Nachwuchses. Die Verbreitung von Propaganda über das Internet ist ein wesentliches Mittel zur Nachwuchsgewinnung und zur Einschüchterung des Gegners.

Ferner machen sich Terroristen die Verwundbarkeit kritischer Infrastrukturen infolge ihrer Anbindung an das Internet zunutze. Dies belegt beispielsweise die Attacke auf den französischen Sender TV5. Bei dem Angriff auf TV5 hatten Cyber-Dschihadisten Anfang April den Fernsehsender lahmgelegt. Auch die Social-Media-Auftritte des Senders brachten sie unter ihre Kontrolle und verbreiteten Propaganda. Die Terroristen begründeten ihren Angriff mit der Beteiligung Frankreichs an Luftschlägen gegen den Islamischen Staat (IS) im Irak[6].

Erfolgreiche Cyber-Angriffe auf Unternehmen, Verwaltungen und Privatnutzer bedürfen jedoch keineswegs der nahezu unbegrenzten Ressourcen fremder Nachrichtendienste oder großer Terrornetzwerke. Dies spiegelt sich in der Masse der heutigen Cyber-Angriffe wider. Für erfolgreiche Cyberattacken braucht man derzeit vielfach nicht mehr als einen PC und einen Internetanschluss, da in der Underground Economy sog. Botnetze, also der Zugriff auf tausende infizierte Opferrechner, angekauft oder angemietet werden kann.

Zusammenfassend ist festzuhalten, dass Cybercrime rasant zunimmt, die Schwere der Taten eine erhebliche Steigerung erfährt und somit den einzelnen Bürger und die Gesellschaft nicht nur virtuell oder finanziell, sondern auch an Leib und Leben bedroht.

b) <u>Bedeutung der Vorratsdatenspeicherung für die Verfolgung von Cybercrime</u>

Bei Straftaten, die mittels Internet begangen werden, stellt die IP-Adresse des Täters regelmäßig den einzigen, immer aber den ersten, effizientesten und schnellsten Ermittlungsansatz dar.

Ohne die Zuordnung der IP-Adresse zu einem Anschlussinhaber laufen die Ermittlungen weitgehend ins Leere, weil keine anderen Spuren vorhanden sind.

Dabei dient die Zuordnung der IP-Adresse zu einem Anschlussinhaber in der überwiegenden Mehrzahl der Fälle von Cybercrime letztendlich nicht der Beweisführung in der Hauptverhandlung, wie z.B. die Standortdaten eines Mobiltelefons im gerichtlichen Verfahren die Anwesenheit eines Täter am Tatort beweisen können, sondern – viel elementarer – zunächst der Identifizierung des Anschlussinhabers und der Ermöglichung weiterer Ermittlungen wie z.B. Durchsuchungsmaßnahmen zur Feststellung des eigentlichen Täters.

[6] Inzwischen gibt es Medienberichte, die mutmaßen, dass der Angriff andere Urheber hatte.

Die Erhebung eines IP-Adressinhabers steht mithin grundsätzlich am Anfang der Ermittlungen. Solange eine IP-Adresse nicht zugeordnet werden kann, werden Verfahren entweder zunächst meist gegen Unbekannt geführt oder gar nicht erst eingeleitet.
Schlägt schon der erste Ermittlungsschritt - die Zuordnung einer dynamischen IP-Adresse zum Anschlussinhaber – fehl, müssen die Verfahren regelmäßig eingestellt werden.

Beispiele:

aa) Operation „Hünstein“
Dieses Verfahren ist ein klassisches Kinderpornographieverfahren von verhältnismäßig kleinem Umfang. Die Ermittlungen richteten sich zunächst gegen einen 30-jährigen Kinderpornographiekonsumenten aus Hessen wegen des Verdachts der Verbreitung und des Besitzes von kinderpornographischen Bildern und Videos. Nach der Durchsuchung wurde der Computer des Beschuldigten ausgewertet und dabei eine E-Mail-Datenbank mit über 200 Tauschkontakten aufgefunden. Die Bestandsdaten der Täter bei den E-Mail-Anbietern waren durchweg fiktiv. Aufgrund fehlender Vorratsdatenspeicherung konnten lediglich neun Täter ermittelt werden, da außer den IP-Adressen der letzten E-Mail-Nutzung keine weiteren Spuren vorhanden waren.

bb) Operation „Downfall“
Dieses internationale Ermittlungsverfahren richtete sich u.a. gegen die Nutzer des kinderpornographischen Internetboards „Hurt to the Core“. Die Seite war im Darknet gehostet, also vermeintlich anonym, und hatte zum Feststellungszeitpunkt 7.331 registrierte Mitglieder/Nutzer und 18.674 einzelne, allesamt noch abrufbare Postings zu 1.932 einzelnen Themen. Thematisch ausgerichtet war das Board vollständig auf das sexuelle Missbrauchen in Verbindung mit dem sexualisierten Verletzen, Foltern, Töten bis hin zum Verzehren von Menschen, hauptsächlich Kindern. Die Abbildungen 8 und 9 stammen aus diesem Board.
Es gab einen separaten Teil „Deutsch“, in dem zuletzt über 100 registrierte Mitglieder in deutscher Sprache kommunizieren und Dateien veröffentlichen konnten.

Es war den US-Ermittlungsbehörden gelungen, durch Ausnutzen einer Schwachstelle der Anonymisierungssoftware TOR (The Onion Router) die Verschleierung der IP-Adressen der Nutzer zu brechen, das Board zu überwachen und nahezu in Echtzeit Real-IP-Adressen an die internationalen Partner auszuleiten. Obwohl die Abfrage der IP-Adressen also zeitnah (binnen Stunden) erfolgte, konnten rund 20% der Täter nicht ermittelt werden.

cc) Operation „Blackshades“
Das Verfahren, in dem es um den Verdacht des Ausspähens von Daten und des Computerbetruges ging, richtete sich gegen die mutmaßlichen Verkäufer und Erwerber der Schadsoftware „Blackshades“.
Dieser Trojaner, der zum Preis von lediglich rund 80 Dollar erhältlich war, ermöglicht unter anderem, die Kontrolle über das infizierte Computersystem zu übernehmen, dieses aus der Ferne zu steuern und alle Daten, die darauf gespeichert sind, auszuspähen – ein ideales Tatmittel, um an sensible Unternehmensdaten zu gelangen, Computerbetrugstaten oder Erpressungen durchzuführen. Dazu stellte das Schadprogramm diverse Funktionen zur Verfügung, u.a. die Einrichtung eines sog. Keylog-

gers zum Mitschnitt und zur Ausleitung aller Tastatureingaben des Opfers, eine Funktion zur unbemerkten Steuerung der Webcam des Opfersystems, die Anfertigung von Screenshots (Momentaufnahmen) des aktuell sichtbaren Bereiches auf dem Bildschirm des Opfersystems, die Ausführung von DDoS-Angriffen, eine „Ransomware"-Funktion, die dazu dient, alle Dateien auf dem Opfersystem zu verschlüsseln und das Opfer gegen Geldzahlung zur Freigabe der Daten zu erpressen sowie die Möglichkeit zum gezielten Ausspähen digitaler Identitäten (sog. ID-Theft-Funktionalität.
Das Verfahren gegen die Programmierer und Verkäufer der Software hatte in den Vereinigten Staaten seinen Ursprung. Die US-Ermittlungsbehörden übermittelten die im Rahmen der dortigen Ermittlungen gewonnenen Daten über die weltweiten Abnehmer des Programms an ihre internationalen Partner, darunter Deutschland.
Da die Vertreiber der Schadsoftware nicht in Deutschland aufenthältig waren, richteten sich die hiesigen Ermittlungen ausschließlich gegen die deutschen Abnehmer. Die aus den USA übermittelten rund 400 Datensätze ermöglichten schließlich die Identifizierung von rund 150 Tatverdächtigen aus Deutschland. Haupthindernis für die Identifizierung war dabei die fehlende Vorratsdatenspeicherung. Der Datensatz eines Abnehmers enthielt neben Namen, Anschrift und E-Mailadresse auch die Bestell-IP-Adresse. Letztere war als Ermittlungsansatz in Deutschland unbrauchbar.

Diese Aufzählung von Rechtstatsachen ließe sich beliebig fortsetzen.

Fazit:
Ohne Vorratsdaten ist eine effektive Verfolgung von Cybercrime nicht möglich. Der Ermittlungsansatz „IP-Adresse" kann hier durch keinen alternativen Spurenansatz ersetzt werden. Daher kann auf die Vorratsdatenspeicherung nicht verzichtet werden.

Auch das BVerfG und der EuGH haben die VDS als geeignetes Ermittlungsinstrument angesehen.

Das BVerfG stellte in seiner Entscheidung vom 02.03.2010 fest:

> *„Unerheblich ist, ob die vom Gesetzgeber geschaffenen Regelungen in der Lage sind, lückenlos alle Telekommunikationsverbindungen zu rekonstruieren. Auch wenn eine solche Datenspeicherung nicht sicherstellen kann, dass alle Telekommunikationsverbindungen verlässlich bestimmten Anschlussnehmern zugeordnet werden können, und etwa Kriminelle die Speicherung durch die Nutzung von Hotspots, Internetcafés, ausländischen Internettelefondiensten oder unter falschen Namen angemeldeten Prepaid-Handys unterlaufen können, kann dies der Geeignetheit einer solchen Regelung nicht entgegenhalten werden. Diese erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird. […]*
> *Eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden beziehungsweise an die Nachrichtendienste darf der Gesetzgeber zur Erreichung seiner Ziele als geeignet ansehen. Es werden hierdurch Aufklärungsmöglichkeiten geschaffen, die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbe-*

reitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind. […]
Eine Speicherung der Telekommunikationsverkehrsdaten […] knüpft vielmehr in noch begrenzt bleibender Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt an und reagiert auf das spezifische Gefahrenpotential, das sich mit dieser verbindet. Die neuen Telekommunikationsmittel überwinden Zeit und Raum in einer mit anderen Kommunikationsformen unvergleichbaren Weise und grundsätzlich unter Ausschluss öffentlicher Wahrnehmung. Sie erleichtern damit zugleich die verdeckte Kommunikation und Aktion von Straftätern und ermöglichen es auch verstreuten Gruppen von wenigen Personen, sich zusammenzufinden und effektiv zusammenzuarbeiten. Durch die praktisch widerstandsfreie Kommunikation wird eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt. Manche Straftaten erfolgen unmittelbar mit Hilfe der neuen Technik. Eingebunden in ein Konglomerat von nurmehr technisch miteinander kommunizierenden Rechnern und Rechnernetzen entziehen sich solche Aktivitäten weithin der Beobachtung. Zugleich können sie - etwa durch Angriffe auf die Telekommunikation Dritter - auch neuartige Gefahren begründen. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung.“ (BVerfG NJW 2010, 833)

Der EuGH führte aus[7]:

„Nach der Rechtsprechung des Gerichtshofs stellt die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit eine dem Gemeinwohl dienende Zielsetzung der Union dar. Das Gleiche gilt für die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit.
Im Übrigen ist insoweit festzustellen, dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat. […]
Somit ist festzustellen, dass die durch die Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zu dem Zweck, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich machen zu können, eine dem Gemeinwohl dienende Zielsetzung darstellt.“

2) Bewertung einzelner Argumente gegen die Vorratsdatenspeicherung

a) <u>VDS und Aufklärungsquoten</u>
Es wird vorgebracht, dass sich der Wegfall der VDS 2010 nicht negativ auf die Aufklärungsquote in der PKS ausgewirkt habe. Diese belege, dass die VDS zur Bekämpfung von Cybercrime nicht nötig sei.

Zunächst ist nochmals darauf hinzuweisen, dass die PKS u.a. wegen der Dunkelfeldproblematik nur eine beschränkte Aussagekraft hat. Viele Betroffene einer Da-

[7] EuGH, Urteil vom 08.04.2014, C-293/12, Celex-Nr. 62012CJ0293, zit. nach Juris

tenausspähung z.B. bemerken zunächst nicht, dass sie Opfer einer Straftat geworden sind. Im Falle der 18 Millionen Datensätze mussten die Opfer über eine Homepage abfragen, ob sie betroffen sind. Nur wenige der Betroffenen haben anschließend Anzeige erstattet. Das bedeutet: eine enorme Menge von Cybercrime-Straftaten ohne statistische Erfassung.

Zudem werden Auslandstaten in der PKS nicht erfasst. Befindet sich das Opfer in Deutschland, handelt der Täter aber – wie es bei Cybercrime häufig der Fall ist – aus dem Ausland oder ist es unklar, ob der Täter aus dem Ausland handelte, fließen diese Fälle in die PKS nicht ein.

Auch werden Ermittlungsverfahren bei von vorneherein erkennbarer Aussichtslosigkeit mangels noch abfragbarer IP-Adressen von den Strafverfolgungsbehörden regelmäßig gar nicht erst eingeleitet und tauchen somit nicht als „ungeklärt“ in der Statistik auf. So wurden z.B. im Fallbeispiel der OP Hünstein (oben 1.b.aa) nur diejenigen Verfahren eingeleitet, bei denen noch Ermittlungsansätze bestanden. Das bedeutet, dass allein in dieser kleinen Operation 191 wegen fehlender Vorratsdatenspeicherung ungeklärter Fälle nicht in die PKS Eingang fanden.

Darüber hinaus muss man bedenken, dass in der Praxis der Erfassungsmarker „Tatmittel Internet“ durch die jeweiligen polizeilichen Datenerfasser – welche nicht immer mit dem Sachbearbeiter des Verfahrens identisch sein müssen – gesetzt wird, wenn das Internet im Verfahren in beliebiger Weise relevant wurde, also auch dann, wenn lediglich über das Internet kommuniziert wurde. Dies erklärt, warum beispielsweise in der Statistik für das Jahr 2010 auch 31 Fälle des „Diebstahls von Fahrrädern unter erschwerenden Umständen“ als Internetkriminalität erfasst wurden. Das heißt, in der PKS werden zahlreiche Fälle als Internetkriminalität erfasst, in denen Daten nicht der einzige Ermittlungsansatz sind.

Bedeutsam ist noch ein weiterer Umstand:
Bei der Beurteilung der Auswirkungen des Wegfalls der VDS auf die Aufklärungsquoten ist zu berücksichtigen, dass die VDS-Pflicht für den Bereich der Internet-Zugangsprovider zu keinem Zeitpunkt in dem gesetzlich vorgesehenen Umfang zum Tragen gekommen ist, weil die erste einstweilige Anordnung des BVerfG vom 11.03.2008 (NStZ 2008, 290) bereits vor Geltung der VDS für die Internetprovider ab dem 01.01.2009 die Verwendung der Daten eingeschränkt hatte. Nach dem genannten Beschluss des BVerfG war die Übermittlung der allein nach § 113a TKG auf Vorrat gespeicherten Verkehrsdaten an die Strafverfolgungsbehörden bis zur Entscheidung in der Hauptsache auf die Fälle des § 100g Abs. 1 S. 1 Nr. 1 StPO, also auf die Fälle der „Straftat von erheblicher Bedeutung“, beschränkt.
Das bedeutet: Für das Feld der Internetkriminalität hat sich die VDS nie in vollem Umfang positiv auswirken können. Dies bedingt zwangsläufig, dass ihr Wegfall auch nicht wesentlich negativ bei den Aufklärungsquoten zu Buche schlagen konnte.

Soweit als Beleg für die behauptete Unwirksamkeit der VDS die Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht aus dem Jahre 2011 herangezogen wird, ist darauf hinzuweisen, dass diese Studie erheblicher, auch wissenschaftlicher, Kritik ausgesetzt ist[8]. In der Ausgabe 11/2012 vom 12.03.2012 be-

[8] https://www.bka.de/nn_196810/sid_5351C45DBA5A6EE13D40CF99BC574DDF/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120330StellungnahmeMPIStudie.html?__n

richtete das Magazin „DER SPIEGEL“ über eine erste Version des Gutachtens wie folgt:

> *„[…] Es handelt sich dabei um die erste Fassung des Albrecht-Gutachtens. Leutheusser-Schnarrenberger hat sie bislang unter Verschluss gehalten. Das Papier kommt zu anderen Ergebnissen als die spätere Version.*
> *In der 200 Seiten umfassenden Ursprungsexpertise aus dem August 2010 ist Kritik an der Vorratsdatenspeicherung nicht zu finden. Im Gegenteil: Damals drängten Albrecht und seine Co-Autoren geradezu auf eine Neuregelung der Speicherpflicht: ‚In Anbetracht der vielfältigen Einschränkungen, die sich in Deutschland derzeit bei dem Zugriff auf Verkehrsdaten ergeben, erscheint der Handlungsbedarf dringend.‘ Auf dieses Instrument zu verzichten sei eine ‚politische Abwägung zu Lasten der Strafverfolgung‘.*
> *Das Freiburger Max-Planck-Institut hatte für die Originalstudie Interviews mit Experten aus der Praxis im In- und Ausland geführt, mit Staatsanwälten, Polizisten, Richtern. Diese berichteten von gravierenden Folgen, nachdem das Bundesverfassungsgericht die Speicherpflicht im März 2010 kassiert hatte. Die Suche nach IP-Adressen und Telefondaten von Verdächtigen scheitere nun regelmäßig. Viele Fälle vor allem bei der Kinderpornografie blieben ‚derzeit offensichtlich unaufklärbar‘, schrieben die Wissenschaftler.*
> *Doch als Kriminologe Albrecht diese Ergebnisse im Sommer 2010 dem Hause Leutheusser-Schnarrenberger präsentierte, fiel er glatt durch. Er habe sich in der Studie zu sehr auf die Wünsche der Ermittler konzentriert, vertraglich vereinbarte Leistungen seien nicht erbracht worden, hieß es aus dem Ministerium. Das Max-Planck-Institut musste nachbessern. Neben zusätzlichen Daten aus dem Jahr 2009, die in die Studie einflossen, sollte auf Wunsch des Hauses Leutheusser-Schnarrenberger ein neuer Schwerpunkt aufgenommen werden. Das Thema: ‚Ermittlungseffizienz und Aufklärungsquoten‘ - und dort werden jetzt jene Fakten betont, die dem Ministerium später als Argumente gegen die Vorratsdatenspeicherung dienen sollten.*
> *Das Freiburger Institut lieferte im vergangenen Juli die um 92 Seiten erweiterte Fassung mit deutlich modifizierten ‚Schlussfolgerungen‘. Frühere Bewertungen der Wissenschaftler standen im Konjunktiv oder wurden in der Neufassung den befragten Ermittlern zugeschrieben. Das Justizministerium war zufrieden. […]“* [9].

Das MPI hat den SPIEGEL-Bericht in einer Presseerklärung als „verkürzend“ und „fehlinterpretierend“ bezeichnet[10]. Eine Veröffentlichung der ersten Fassung des Gutachtens zum Zwecke der Überprüfung des Widerspruchs ist jedoch, soweit ersichtlich, nicht erfolgt.

---

nn=true; http://www.spiegel.de/spiegel/print/d-84339472.html;
www.sueddeutsche.de/digital/gutachten-zur-vorratsdatenspeicherung-ein-institut-zwei-meinungen-1.1307175

[9] http://www.spiegel.de/spiegel/print/d-84339472.html

[10] https://www.mpicc.de/shared/data/pdf/pm_02_12_vorratsdatenspeicherung.pdf

In der SPIEGEL-Ausgabe 12/2012 wurde über ein Gespräch mit dem Leiter des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht, Prof. Albrecht, wie folgt berichtet:

> *„[…] In der Debatte hätten Kritiker und Befürworter einer Wiedereinführung des umstrittenen Schnüffelinstruments die Ergebnisse seines Gutachtens ‚jeweils in ihrem Sinne interpretiert'. Die Vorratsdatenspeicherung sei keine Wunderwaffe, ‚aber sie bietet in bestimmten Fällen wichtige Ermittlungsansätze', so Albrecht. […]"*[11]

Eine mangelnde Sorgfalt bei der Erstellung der zweiten Fassung des MPI-Gutachtens dürfte sich jedenfalls dadurch belegen lassen, dass die oben dargestellte Rechtslage zur eingeschränkten Nutzung der vorratsgespeicherten Daten aufgrund der einstweiligen Anordnungen des BVerfG und damit die beschränkte Aussagekraft der Aufklärungsquoten in dem Gutachten nicht ausführlich diskutiert, sondern lediglich knapp abgehandelt wird. Damit vermitteln die Ergebnisse der Studie in der zweiten Fassung den Eindruck, die VDS hätte ihre Wirksamkeit bei der Bekämpfung von Cybercrime entfalten können, was aber nicht den Tatsachen entspricht. Auch erfährt die Aussagekraft von Aufklärungsquoten in der Studie insgesamt eine unangemessene Überbewertung (s.o., überproportionales Dunkelfeld).

Hinzu kommt, dass die in dem Gutachten getroffenen Aussagen zum Nutzen von Vorratsdaten für die Verfolgung von Kinderpornographie mehr als fragwürdig sind. Sie beruhen überwiegend auf Erkenntnissen einer Studie der Universität Hannover, für die lediglich 81 Verfahren ausgewertet wurden. Allein in der OP „Geisterwald" wurden über 160 Verfahren gegen Konsumenten von Kinderpornographie geführt und dabei rund 50 Kindesmissbraucher überführt. Die im MPI-Gutachten getroffene Feststellung, wonach nur eine verschwindend geringe Zahl an Konsumenten von Kinderpornographie tatsächlich auch Kinder sexuell missbrauchen würden, ist aus Sicht der Hessischen Zentralstelle zur Bekämpfung der Internetkriminalität, die sich dabei auf die Erfahrung von über 3.000 Ermittlungsverfahren berufen kann, unzutreffend[12].

b) <u>Einsatz von Anonymisierungsdiensten (z.B. TOR) oder Nutzung von Internetcafés</u>
Das Argument, dass die VDS durch die Benutzung von Anonymisierungsdiensten oder Internetcafés ausgehebelt werden könne und daher für zahlreiche Verfahren ohnehin ohne Bedeutung sei, greift zu kurz. Der Umstand, dass die meisten Wohnungseinbrecher Handschuhe tragen, hat bisher noch niemanden veranlasst, den Einsatz von Daktyloskopie als für die Strafverfolgung ungeeignet zu betrachten und deren Abschaffung zu fordern.
Allein die Tatsache, dass geschickt agierende Täter trotz Vorratsdatenspeicherung nicht zu ermitteln sein werden, spricht nicht gegen dieses Ermittlungsinstrument, denn dies gilt für viele andere Kriminalitätsfelder in gleicher Weise. Überdies hat eine Vielzahl von Verfahren gezeigt, dass in einigen Kriminalitätsfeldern – wie der Verbreitung von Kinderpornographie – Verschleierungsmaßnahmen nicht durchgehend vorgenommen werden. Dies liegt u.a. daran, dass z.B. Kinderpornographie als visuelle Masturbationsvorlage von den Tätern nicht im Internetcafé oder einer Telefonzelle konsumiert wird, sondern zu Hause. Zudem sind technische Verschleierungsmaß-

[11] http://www.spiegel.de/spiegel/print/d-84430173.html
[12] vgl. dazu und zu KiPo allgemein auch S. 22 ff. der Stellungnahme des BKA zum MPI-Gutachten (oben Fn. 8)

nahmen häufig umständlich einzurichten und verlangsamen den Datenverkehr, so dass viele Täter aus Bequemlichkeit keine solchen Maßnahmen ergreifen.

Schließlich zeigt das Beispiel der OP „Downfall“, dass es den Ermittlungsbehörden durchaus (wenn auch immer noch zu selten) gelingt, Anonymisierungsmaßnahmen der Täter zu brechen (s.o. 1.b.bb). Auf diese Weise erlangen die Behörden Real-IP-Adressen und benötigen die VDS.

Auch die Ermittlung eines vom Täter genutzten Internetcafés durch die VDS kann weiterhelfen, da sich daran weitere Maßnahmen - wie z. B. eine Observation - anschließen können.

c) Das Argument, durch Vermeidungsmaßnahmen der Täter könne der Erfolg sonstiger verdachtsabhängiger TKÜ-Maßnahmen im Internet vereitelt werden, ist nicht stichhaltig. Um eine verdachtsabhängige TKÜ-Maßnahme im Bereich von Internetermittlungen vornehmen zu können, sind regelmäßig Anknüpfungstatsachen erforderlich, die ohne vorratsgespeicherte Daten gar nicht erst erlangt werden können. Wie soll eine verdachtsabhängige TKÜ-Maßnahme gegen einen Täter eingeleitet werden, der wechselnde IP-Adressen verwendet, wenn man mangels Vorratsdatenspeicherung nicht ermitteln kann, an wen die IP-Adressen vergeben waren?

d) Kosten der Vorratsdatenspeicherung
Ebenso wird ins Feld geführt, die VDS sei für die TK-Unternehmen unverhältnismäßig teuer.
Es trifft zu, dass die VDS nicht unerhebliche Kosten verursacht. Andererseits ist die Anzahl der Insolvenzen von TK-Unternehmen in Ländern, die die VDS gesetzlich vorgeschrieben haben, nicht spürbar gestiegen.
Zudem darf nicht vergessen werden, dass die TK-Unternehmen seit dem Jahr 2009 für die Kosten der alten Regelung zur VDS dadurch entschädigt wurden, dass die Vergütung für Auskünfte im JVEG massiv erhöht wurde[13]. Seit dem 01.07.2009 erhielten die TK-Unternehmen z.B. für die Auskunft zu einer einzigen IP-Adresse 30,- Euro (geändert ab dem 01.08.2013, jetzt 30,-Euro pro zehn IP-Adressen in einem Abfragevorgang, immer noch ein sehr erheblicher Betrag). Als die VDS im März 2010 in Wegfall geriet, wurde das JVEG nicht geändert, so dass die TK-Unternehmen seit März 2010 für etwas entschädigt werden, das es nicht mehr gibt.

Schließlich sieht der Gesetzentwurf in § 113a TKG-E eine Entschädigung für die Umsetzung der VDS für solche Unternehmen vor, die eine unbillige Härte nachweisen können.

e) Die VDS sei ein unverhältnismäßiger Grundrechtseingriff und ermögliche die Erstellung von Bewegungsprofilen im Internet
Die Intensität des Eingriffs der Speicherung der Zuordnung einer IP-Adresse zu einem Anschlussinhaber wird überbewertet.
Es ist nicht möglich, durch eine verkehrsdatengestützte Bestandsdatenauskunft, also durch die Auskunft zu einer dynamisch vergebenen IP-Adresse, den Nutzer eines Computers oder Smartphones festzustellen. Festgestellt wird lediglich der Vertragspartner des TK-Unternehmens, der Anschlussinhaber. Es ist mithin auch nicht möglich, mithilfe von Vorratsdaten Kommunikationsvorgänge unmittelbar einer Person

[13] BT-Drs. 16/7103, siehe auch becklink 271926

zuzuordnen. Die Ermittlung eines Täters erfolgt in der Praxis mittels einer Durchsuchung und anschließender Rechnerauswertung, zumal sich häufig mehrere Personen einen Internetanschluss teilen. Am ehesten kann man die VDS im Internetbereich – etwas anderes gilt sicherlich für die Geodaten – mit der Funktion einer KFZ-Zulassungsstelle und die dynamische IP-Adresse mit einem KFZ-Kennzeichen vergleichen. Die Ermittlung des Halters eines KFZ lässt noch keinen endgültigen Schluss auf den Fahrer zu. Genauso ist es bei der VDS: Vertragspartner und Nutzer des Anschlusses zu Tatzeit sind oft verschieden. Mithin kann man aus vorratsgespeicherten Daten nicht die Kommunikationsgewohnheiten einer einzelnen Person zweifelsfrei belegen.

Die Behauptung, durch die Regelung über die VDS sei die Nutzung des Internets weithin nachvollziehbar („Bewegungsprofile“ im Internet), entspricht nicht den Tatsachen. Da im Rahmen der Vorratsdatenspeicherung keine Inhaltsdaten aufgezeichnet werden, können rückwirkend nur Verkehrsdaten erhoben werden, d.h. es können durch die Strafverfolgungsbehörden lediglich die näheren Umstände der Telekommunikation, nicht aber ihr Inhalt, ermittelt werden.
Für den Bereich der Internetnutzung werden die Provider verpflichtet, die Zuordnung einer dynamisch vergebenen IP-Adresse zu den Daten des Kunden zu speichern. Nur wenn den Strafverfolgungsbehörden der eigentliche Telekommunikationsvorgang bereits genau bekannt ist (Bsp.: Der Nutzer mit der IP-Adresse 88.196.249.49 hat am 10.11.2014 um 14:38 Uhr die Internetseite www.ebay.de aufgerufen und betrügerisch eine Ware verkauft), kann ermittelt werden, welcher Kunde Teilnehmer an dem betreffenden TK-Vorgang ist (Bsp.: Die IP-Adresse 88.196.249.49 wurde am 10.11.2014 um 14:38 Uhr durch den Kunden X genutzt).
Es ist jedoch bei geltender Verpflichtung zur Vorratsdatenspeicherung - selbst unter Heranziehung von Daten nach dem TMG – nicht möglich, die komplette Internetnutzung einer Person nachzuvollziehen, weil die Provider nicht speichern müssen, welche Internetseiten ein Kunde aufgerufen hatte (Bsp.: Die Anfrage „Welche Internetseiten hat der Kunde X zwischen dem 01.11. und dem 30.11.2014 besucht?“ kann der Provider auch zukünftig unter Geltung der Vorratsdatenspeicherung nicht beantworten).

f) Die VDS trage nicht zur Verhinderung von Straftaten bei.
Die Anschläge in Frankreich hätten bewiesen, dass trotz der dort vorhandenen VDS keine Straftaten verhindert werden können.
Diese Sichtweise verkennt, dass die VDS im Rahmen der Kriminalitätsbekämpfung nur ein Baustein ist. Zudem trägt die Auswertung der gespeicherten TK-Daten der Täter dazu bei, die Tat- und die Täterstrukturen aufzuklären und dadurch zukünftige Anschläge durch dieselbe Tätergruppierung zu verhindern.

Es wäre im Übrigen in Bezug auf die Aufklärung der NSU-Strukturen überaus hilfreich gewesen, auf Vorratsdaten zurückgreifen zu können. Unterstützerstrukturen hätte leichter ausgemacht werden können, wenn die TK-Verkehrsdaten rückwirkend für z.B. 6 Monate hätten erhoben werden können.

3) Zu einzelnen Regelungen des Gesetzentwurfes über die VDS

Die Vorratsdatenspeicherung ist, wie dargelegt, für eine effektive Strafverfolgung notwendig. Der Gesetzentwurf bedarf indes erheblicher Korrekturen, um für die Strafverfolgungspraxis von Nutzen zu sein.

a) Zu kurze Speicherfristen

Die in § 113b TKG-E bestimmten Speicherfristen von zehn (Verkehrsdaten) bzw. vier Wochen (Standortdaten) sind zu kurz. Für den Bereich Cybercrime gilt, dass IP-Adressen als Spuren für weiterführende Ermittlungen häufig das Ergebnis von Auswertungen von Servern und anderen Computern oder Smartphones sind. Diese Auswertungen nehmen erfahrungsgemäß eine gewisse Zeit in Anspruch und sind selten in zehn Wochen abgeschlossen.

Wie das in der breiten Öffentlichkeit bekannte Beispiel der OP „Selm“ zeigt, werden ermittlungsrelevante IP-Adressen nicht selten als Ergebnis ausländischer Ermittlungen nach Deutschland übersandt. Auch insoweit muss damit gerechnet werden, dass zehn Wochen Speicherfrist den Anforderungen der Praxis nicht genügen.

Ich vermag weder der Entscheidung des BVerfG, noch derjenigen des EuGH das Gebot derartig kurzer Speicherfristen zu entnehmen.

In dem BKA-Abschlussbericht „Stand der statistischen Datenerhebung im BKA zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu ‚Mindestspeicherfristen‘ “ finden sich folgende, empirisch begründete Aussagen[14]:

> *Darüber hinaus belegen die Angaben zur idealen Speicherdauer bezogen auf die zugrundeliegenden Sachverhalte die polizeifachliche Erforderlichkeit der Verkehrsdatenspeicherung für 6 Monate. Die Ergebnisse zeigen aber auch, dass die polizeiliche Reaktionszeit nur geringen Einfluss auf diesen polizeilich für erforderlich erachteten Mindestspeicherzeitraum hat. Zwischen dem Zeitpunkt der Kenntniserlangung des BKA über das Vorliegen ermittlungsrelevanter Verkehrsdaten und dem Moment der Stellung des Auskunftsersuchens lagen in der Regel (86 % der Fälle) maximal 7 Tage. Dies bedeutet im Umkehrschluss, dass nicht die polizeiliche Reaktionszeit, sondern das „Alter“ der Verkehrsdaten den erforderlichen Speicherzeitraum bestimmt. Das tatsächliche „Alter“ der relevanten Verkehrsdaten bei Auskunftsersuchenstellung muss daher zumeist annähernd 6 Monate betragen haben. Polizei bzw. Staatsanwaltschaft haben jedoch zumeist keinen Einfluss darauf, wie schnell sie durch Anzeige o. ä. überhaupt von dem Fall und somit dem Vorliegen möglicherweise ermittlungsrelevanter Verkehrsdaten erfahren.*
>
> *Nach wie vor wird eine hohe Bedeutung des „Ermittlungsansatzes Verkehrsdaten“ festgestellt, auch wenn diese deliktsabhängig nicht in allen*

---

14 http://www.bka.de/nn_234042/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120130StatistischeDatenerhebungMindestspeicherungsfristenAbschlussbericht.html

Fällen (so aber insbesondere in den Phänomenbereichen Kinderpornographie und IuK-Kriminalität) den einzigen Ermittlungsansatz bilden.

Aus meiner eigenen Erfahrung im Phänomenbereich Cybercrime (seit 1999) kann ich die Aussagen des BKA bestätigen.

b) Straftatenkatalog unvollständig

Der Straftatenkatalog des § 100g Abs. 2 StPO-E greift deutlich zu kurz. Es fehlen z.B. die im Cybercrimebereich besonders relevanten Straftaten der §§ 263, 263a StGB (s.o., 74,2 Prozent).

Es ist nicht verständlich und nicht geboten, dass durch den Gesetzentwurf der Zugriff auf Verkehrsdaten nunmehr höheren Schranken unterliegen soll als der Zugriff auf Inhaltsdaten. Dies führte zu dem absurden Ergebnis, dass bei einem Fall des gewerbsmäßigen Computerbetruges eine Inhaltsüberwachung der Telekommunikation möglich wäre, nicht aber ein Zugriff auf Vorratsdaten. Dies widerspricht der vom BVerfG in ständiger Rechtsprechung zugrunde gelegten Wertung, dass der Zugriff auf Verkehrsdaten weniger intensiv ist als der Zugriff auf Inhaltsdaten.

Aus Sicht der Strafverfolgungspraxis sollte der Katalog erweitert und derjenige des § 100a Abs. 2 StPO herangezogen werden. Verfassungsrechtliche oder europarechtliche Bedenken gegen die Anwendung dieses Straftatenkatalogs sind nicht ersichtlich.

c) Fehlende Abfragemöglichkeit für in der Vergangenheit liegende Standortdaten

Der Gesetzentwurf bleibt eine hinreichende Begründung dafür schuldig, aus welchem Grund der Zugriff auf in der Vergangenheit liegende Standortdaten zukünftig auf die Fälle von Katalogtaten nach § 100g Abs. 2 StPO-E eingeschränkt wird. Die zwingende Notwendigkeit hierfür ist weder dem Urteil des BVerfG zu entnehmen, noch folgt dies aus der Entscheidung des EuGH. Daher ist diese Einschränkung zu streichen, denn sie bedeutet eine Verschlechterung der Rechtslage gegenüber dem jetzigen Zustand.

d) Fehlende Erfassung der E-Mail-Verkehrsdaten

Obwohl das BVerfG dies in seiner Entscheidung als Anforderung für eine künftige Regelung der VDS nicht gefordert hat, werden Verkehrsdaten bei E-Mail-Providern zukünftig nicht zu speichern sein (§113b Abs. 5 TKG-E). Nach wie vor besitzt der E-Mail-Verkehr im Bereich Cybercrime indes eine erhebliche Bedeutung. Werden E-Mail-Verkehrsdaten von der VDS ausgenommen, schränkt dies die Aufklärungsmöglichkeiten für die Strafverfolgungsbehörden ohne sachlichen Grund erheblich ein.

E-Mai-Verkehrsdaten (Message-ID, Zeitstempel, IP-Adresse des Absenders) sind daher in den § 113b TKG-E aufzunehmen.

e) Richtervorbehalt ohne Eilanordnungskompetenz für die Staatsanwaltschaft

Auch dieser Unterschied zu Telekommunikationsinhaltsüberwachung ist sachlich und verfassungsrechtlich nicht geboten. Vorratsdaten sind in ihrer Sensibilität mit Inhaltsdaten nicht zu vergleichen, denn sie erlauben keinen unmittelbaren Rückschluss auf den konkret Kommunizierenden und bergen auch nicht die Gefahr von Kernbereichsrelevanz. Es ist mithin angezeigt, ebenso wie im § 100b StPO eine Eilanordnungskompetenz der Staatsanwaltschaft vorzusehen und § 101a Abs. 1 S. 2 StPO-E ersatzlos zu streichen.

f) Fehlende Speicherverpflichtung für Telemediendienste, die TK-Leistungen erbringen

Der Gesetzentwurf sieht in § 113a Abs. 1 TKG-E eine Pflicht zur Speicherung nur für die Erbringer von öffentlich zugänglichen Telekommunikationsdiensten, also für Telefon- und Internetzugangsdienste, vor. Vielfach werden heute aber Telekommunikationsdienste auch von Telemediendiensten erbracht. Telemediendienste sind gemäß § 1 Telemediengesetz (TMG) alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Beispiel: Facebook ist ein Telemediendienst). Die über Telemedien geführte Kommunikation besitzt eine erhebliche Bedeutung für die Strafverfolgungsbehörden.

Es sollten daher auch die Telemediendienste, die öffentlich zugängliche Telekommunikationsdienste erbringen, verpflichtet werden, folgende Daten zu speichern:

- die Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten, vgl. § 14 Abs. 1 TMG) und
- die Daten, die bei der Inanspruchnahme von über Telemedien öffentlich erreichbare Telekommunikationsdienste anfallen, soweit es sich nicht um Angaben über die vom Nutzer in Anspruch genommenen Telemedien handelt. (reduzierte Nutzungsdaten, vgl. § 15 Abs. 1 Nr. 1 und 2, aber nicht nach Nr. 3 TMG, also Merkmale zur Identifikation des Nutzers und Angaben über Beginn und Ende der jeweiligen Nutzung eines über Telemedien öffentlich erreichbare Telekommunikationsdienste, aber keine Inhaltsdaten).

g) Fehlende Regelung zur Umsetzung von Art. 16, 17 des Übereinkommens über Computerkriminalität

Die Grenzenlosigkeit des Internets verursacht eine steigende Notwendigkeit grenzüberschreitender Ermittlungen. Die damit verbundenen Probleme – erforderliche Strafverfolgungsmaßnahmen berühren die Hoheitsrechte anderer Staaten und bedingen Rechtshilfemaßnahmen – sind den Tätern wohlbekannt und werden gezielt ausgenutzt (siehe oben). Das Übereinkommen über Computerkriminalität (Convention on Cybercrime, ETS No.185, auch „Budapester Konvention gegen Datennetzkri-

minalität“ genannt) vom 23.11.2001 ist das weltweit erste multilaterale Übereinkommen über Datennetz- und Computerkriminalität. Die Vertragsstaaten haben sich zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen verpflichtet, bestimmte materielle Straftatbestände im Bereich der Computerkriminalität sowie bestimmte Befugnisse für Ermittlungsverfahren einzuführen. Deutschland hat die Cybercrime Convention (nachfolgend: CC) am 09.03.2009 ratifiziert und am 01.07.2009 in Kraft gesetzt. Das Vertragswerk enthält in Kapitel III (Art. 23 bis 35) Vorschriften zur internationalen Zusammenarbeit und Rechtshilfe, insbesondere, sofern Beweise in elektronischer Form erhoben werden sollen. Geregelt werden die Behandlung von Rechtshilfeersuchen bei Vorliegen von anwendbaren völkerrechtlichen Übereinkünften sowie solche ohne. Darüber hinaus sind Vorschriften enthalten zum grenzüberschreitenden Zugriff auf gespeicherte Daten ohne Rechtshilfeersuchen und zur Errichtung eines 24 (Stunden) /7 (Tage) Netzwerkes für eine schnelle wechselseitige Hilfeleistung.

Besonders hervorzuheben ist dabei die Möglichkeit einer beschleunigten zwischenstaatlichen Rechtshilfe zur umgehenden Sicherung von beweiserheblichen Computerdaten nach Art. 29 CC i.V.m. Art. 16 und 17 CC. Hierfür soll ein formloses Ersuchen an den ausländischen Vertragsstaat zur Vorabsicherung der beweisrelevanten Daten, das inhaltlich den Anforderungen des Art. 29 Abs. 2 CC entsprechen muss, genügen. Durch die Verpflichtung zur Sicherung der Daten, insbesondere gegen die automatische Löschung, begründet die Maßnahme im Unterschied zur klassischen Durchsuchung und Beschlagnahme, die nur mit einer Duldungspflicht einhergehen, eine aktive Mitwirkungspflicht der betroffenen Provider. Nach Eingang des Ersuchens hat der Vertragsstaat gem. Art. 29 Abs. 3 S. 1 CC geeignete Maßnahmen zur umgehenden Sicherung der Daten zu treffen, wobei die beiderseitige Strafbarkeit keine Voraussetzung für die Vornahme der Sicherung ist (Art. 29 Abs. 3 S. 2 CC). Durch diese vorläufige Maßnahme lässt sich damit eine Aufbewahrung der beweisrelevanten Daten erreichen, die viel schneller und effektiver als traditionelle Rechtshilfehandlungen ist. Art. 29 Abs. 7 CC sieht vor, dass die gesicherten Daten für mindestens 60 Tage aufbewahrt werden sollen, um der ersuchenden Vertragspartei ein förmliches Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff bzw. Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu ermöglichen.

Art. 35 CC verpflichtet die Vertragsparteien zur Einrichtung einer Kontaktstelle, die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um für eilige Ermittlungshandlungen oder für die Erhebung von Beweismaterial in elektronischer Form unverzüglich für Unterstützung zu sorgen. Diese Unterstützung umfasst unter anderem die jederzeitige transnationale Übermittlung der Vorabsicherungsersuchen nach Art. 29 CC. Die Aufgabe des Art. 35 CC übernimmt das auf polizeilicher Ebene eingerichtete G7 24/7 High Tech Crime Network (HTCN). Die deutschte Kontaktstelle ist das Bundeskriminalamt.

Derzeit kann Deutschland ausländischen Ersuchen gemäß Art. 29 nicht in der Weise nachkomme, wie es die Konvention eigentlich vorsieht. Die in Art. 17 i. V. m. Art. 16 Abs. 1 des Übereinkommens geforderte beschleunigte Sicherung von Verkehrsdaten ist bislang nicht ausdrücklich in nationales Recht umgesetzt worden. Zum Zweck der Umsetzung war zunächst erwogen worden, in § 100g StPO die zur Beauskunftung Verpflichteten auch zu verpflichten, die von ihnen erhobenen Verkehrsdaten aufgrund einer polizeilichen oder staatsanwaltschaftlichen Anordnung für die Dauer von einer Woche bereitzuhalten, wenn die Strafverfolgungsbehörden die Beantragung

einer gerichtlichen Anordnung zur Erhebung der Daten ankündigen. Man ging jedoch dann davon aus, dass die Umsetzung der Richtlinie 2006/24/ EG über die Vorratsspeicherung von Verkehrsdaten dies entbehrlich machen würde (BR-Drucksache 16/5846, S. 27). Durch den Wegfall der Vorratsdatenspeicherung besteht insoweit ein für die Strafverfolgungsbehörden spürbares Umsetzungsdefizit, das sich immer dann bemerkbar macht, wenn andere Vertragsstaaten entsprechende Ersuchen auf beschleunigte Vorabsicherung von Daten an die zuständige deutsche Kontaktstelle richten und diese oft nicht in erforderlicher Weise erledigt werden können. Mangels einer Verpflichtung der Provider (in der Praxis sind zumeist Hostserviceprovider, also Telemediendienste, betroffen), auf polizeiliche oder staatsanwaltschaftliche Anordnung beschleunigt Daten vor einer Löschung zu bewahren („Quick-Freeze"), kann hier derzeit regelmäßig nur der herkömmliche und deutlich langsamere Weg über §§ 94 Abs. 1 Nr. 1 i.V.m. 67 Abs. 1, Abs. 2 und 66 Abs. 1 Nr. 1, Abs. 2 Nr. 1 IRG beschritten werden.

In den GesetzE sollte die überfällige Regelung zur vollständigen Umsetzung des Übereinkommens aufgenommen werden. Das TKG und das TMD sind um Quick-Freeze Vorschriften zu ergänzen, wonach TK- und TM-Dienste verpflichtet werden, beweiserhebliche Daten für die Dauer von 60 Tagen (mit Verlängerungsmöglichkeit) zu sichern. Herauszugeben sind die Daten erst, wenn das ausländische Rechtshilfeersuchen eingetroffen und bewilligt ist.

4) Zur Datenhehlerei

Der Straftatbestand der Datenhehlerei schließt eine Schutzlücke, indem Daten im Kernstrafrecht nunmehr ähnlich wie Sachen geschützt werden. Die Einführung der Datenhehlerei ist trotz der Strafbarkeit nach § 44 BDSG notwendig, da sich der Schutz des BDSG nur auf personenbezogene Daten erstreckt, also nicht z.B. auf Unternehmensdaten, und dieser als absolutes Antragsdelikt für eine effektive Strafverfolgung im Bereich des Datenhandels untauglich ist.

Es ist allerdings zu kritisieren, dass der ursprüngliche Gesetzentwurf (BT-Drs. 17/14362) nicht unverändert übernommen wurde, sondern erhebliche Einschränkungen erfahren hat. So ist die Strafandrohung mit bis zu drei Jahren zu niedrig, d.h. Daten sind noch immer weniger geschützt als Sachen. Auch die Tatsache, dass die schweren Fälle nicht übernommen wurden, ist zu kritisieren.

Der ursprüngliche Gesetzentwurf der Datenhehlerei (BT-Drs. 17/14362) ist dem nunmehr vorgelegten vorzuziehen.

5) Zusammenfassung

Der Gesetzentwurf zur VDS vermag nicht zu überzeugen und bringt in einigen Bereich sogar eine Verschlechterung der Rechtslage für die Strafverfolgungsbehörden mit sich.
Vor allem die kurzen Speicherfristen und der zu sehr eingeschränkte Straftatenkatalog sind praxisuntauglich.

Sollte das Gesetz unverändert verabschiedet werden, wird es im Phänomenbereich Cybercrime weitgehend ohne Wirkung bleiben. Zudem besteht dann die Gefahr, dass die zahlenmäßig geringen Anwendungsfälle den nicht unerheblichen Grundrechtseingriff der Vorratsdatenspeicherung als solchen nicht mehr zu rechtfertigen vermögen und das Gesetz damit wegen fehlender Eignung zur Zweckerreichung insgesamt verfassungswidrig sein könnte.

Demgegenüber ist der Straftatbestand der Datenhehlerei eine notwendige Ergänzung des strafrechtlichen Schutzes für Daten. Allerdings ist der erste Gesetzentwurf zur Datenhehlerei aus der vergangenen Legislaturperiode praxisgerechter als der aktuelle.

gez.
Franosch
Oberstaatsanwalt