JUNIORPROFESSUR FÜR STRAFRECHT UND STRAFPROZESSRECHT
Jun.-Prof. Dr. Dominik Brodowski, LL.M. (UPenn)

RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Keine Staatsgrenzen mehr für Polizei und Staatsanwaltschaft?

Zur unmittelbaren Zusammenarbeit von Internetdiensteanbietern mit ausländischen Strafverfolgungsbehörden

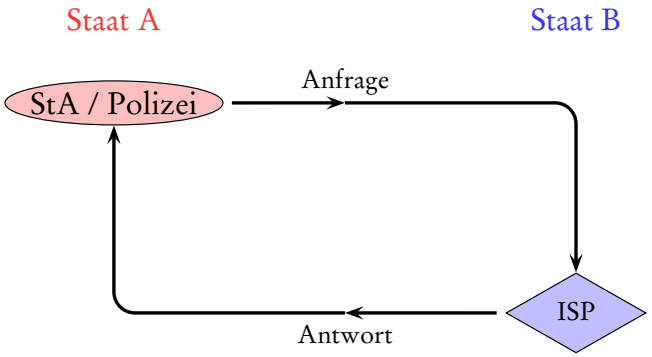
Jun.-Prof. Dr. Dominik Brodowski, LL.M. (UPenn)

12. Juni 2018

Jun.-Prof. Dr. Dominik Brodowski, LL.M. (UPenn)
T: +49 (0) 681 302–4950
dominik.brodowski@uni-saarland.de
Campus, C3 1, Raum 1.08
66123 Saarbrücken

Gastvorlesung ITM-WWU
12.06.2018

A. Problembeschreibung



B. Vorüberlegung: Inpflichtnahme von inländischen Dienste-anbietern durch inländische Strafverfolgungsbehörden

I. Eingriffsgrundlagen

Maßnahme	Rechtsgrundlage	Adressat
Zeuge	§§ 48 ff., 161a, 163 III StPO	Mitarbeiter
Beschlagnahme	§§ 94 ff. StPO	Gewahrsamsinhaber
Herausgabe	§ 95 StPO	Gewahrsamsinhaber
Auskunft	§§ 14 II, 15 V 3 TMG iVm § 95 StPO	Diensteanbieter (TMG)
TKÜ	§§ 100a, 100d f. StPO; § 110 TKG; TKÜV	Telekommunikations-dienstleister
Verkehrsdaten	§§ 100g, 101a StPO; §§ 113a ff. TKG	Telekommunikations-dienstleister
Bestandsdaten	§ 100j StPO; §§ 112 f. TKG	geschäftsmäßig tätige Telekommunikations-dienstleister

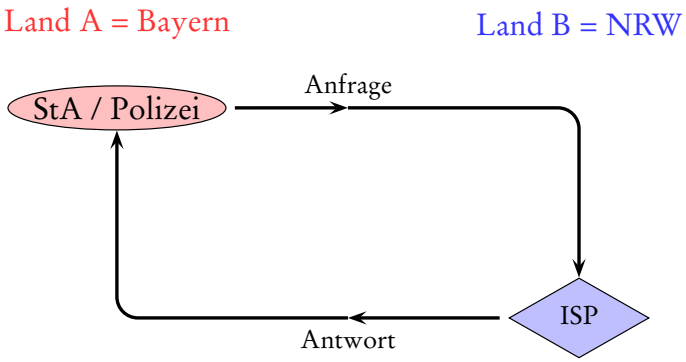
Aktuelle Rechtsprechung:

- BVerfG, Beschl. v. 06.07.2016 – 2 BvR 1454/13 = NJW 2016, 3508 (Überwachung DSL-Anschluss)
- BGH, Beschl. v. 26.01.2017 – StB 26/14, StB 28/14, Tz. 58, juris = BGHSt 62, 22 (Mitteilungspflicht an Nutzer bei Beschlagnahme eines E-Mail-Postfachs)
- OVG NRW, Urt. v. 26.02.2018 – 13 A 17/16 = K & R 2018, 348 (EuGH-Vorlage zum Begriff des TK-Dienstleisters)
- VG Köln, Beschl. v. 20.04.2018 – 9 K 7417/17 (Umsetzungsverpflichtung Vorratsdaten-speicherung)

II. Schutzmechanismen

- Anfangsverdacht (stets)
- qualifizierter Tatverdacht (insb. bei §§ 100a ff. StPO; im Einzelnen str.)
- Katalogtatsysteme (§§ 100a II, 100g II 2 StPO)
- Richtervorbehalt (§ 100a ff. StPO) und/oder jedenfalls nachträglicher Rechtsschutz (§§ 98 II, 101 VII 2 StPO)
- Benachrichtigungspflichten (§§ 35, 101 StPO)
- Kernbereichsschutz (insb. § 100d StPO)
- Verwendungsregelungen (§ 477 II 2 StPO)
- Verhältnismäßigkeit (stets)
- …

III. Länderübergreifende Anordnungen



§ 160 GVG Vollstreckungen … werden nach Vorschrift der Prozeßordnungen bewirkt ohne Rücksicht darauf, ob sie in dem Land, dem das Prozeßgericht angehört, oder in einem anderen deutschen Land vorzunehmen sind.

§ 143 I 1 GVG Die örtliche Zuständigkeit der Staatsanwaltschaft bestimmt sich nach der örtlichen Zuständigkeit des Gerichts, bei dem die Staatsanwaltschaft besteht. …

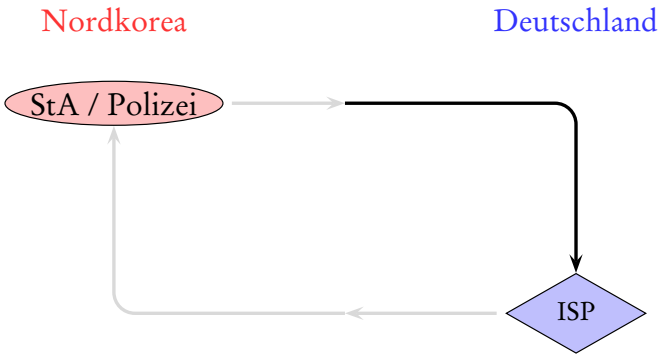
§ 7 II Nr. 1 POG NRW Die Polizeibehörden können durch ihre Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten auch außerhalb ihres Polizeibezirks tätig werden … zur Erforschung und Verfolgung von Straftaten und Ordnungswidrigkeiten ….

§ 7 III POG NRW Jede Polizeivollzugsbeamtin und jeder Polizeivollzugsbeamte darf Amtshandlungen im ganzen Land Nordrhein-Westfalen vornehmen, wenn dies … zur Erforschung und Verfolgung von Straftaten und Ordnungswidrigkeiten auf frischer Tat … erforderlich ist.

C. Transnationale Direktanfragen – Ausgangssituation

I. Grundlagen

1. Anfragen an deutsche Dienstleister



- individuelle Ebene (Dienstleister)
  - Handlungsverpflichtung?
  - Handlungsberechtigung?

§ 88 TKG (1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(3) … Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

Art. 49 DS-GVO (1) Falls weder ein Angemessenheitsbeschluss … vorliegt noch geeignete Garantien … bestehen, ist eine Übermittlung … personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig: …

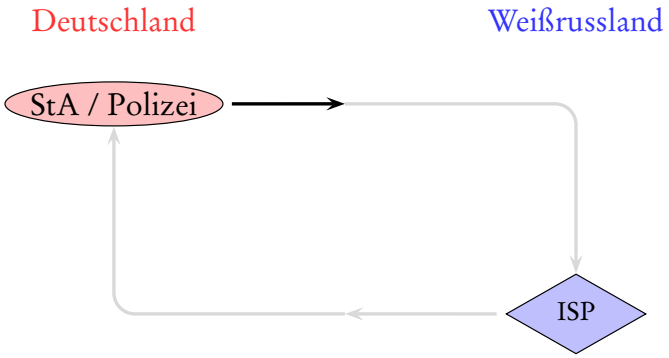
d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig, …

f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, …

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

- völkerrechtliche Ebene
- regulatorische Ebene

2. Anfragen von deutschen Strafverfolgungsbehörden



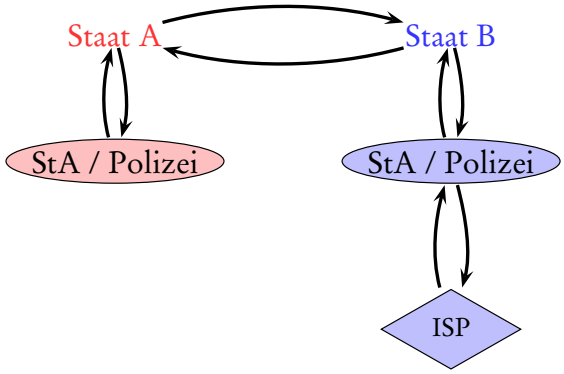
- innerstaatliche Befugnis: §§ 95, 100a, … StPO usw.
- datenschutzrechtliche Befugnis

> **§ 81 I Nr. 1 BDSG** Verantwortliche können … im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 78 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und 1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen …

- rechtshilferechtliche Befugnis

> **Nr. 121 RiVASt** (1) Die deutschen Behörden dürfen in strafrechtlichen Angelegenheiten mit Personen, die im Ausland wohnen … unmittelbar schriftlich oder fernmündlich nur dann in Verbindung treten, wenn nicht damit zu rechnen ist, dass der ausländische Staat dieses Verfahren als einen unzulässigen Eingriff in seine Hoheitsrechte beanstandet. Unbedenklich sind z. B. Eingangsbestätigungen, Zwischenbescheide, Terminabstimmungen, Benachrichtigungen von der Aufhebung eines Termins sowie Mitteilungen über die Einstellung eines Ermittlungsverfahrens an Beschuldigte, Antragstellerinnen und Antragsteller. …
>
> (4) Soweit keine völkerrechtlichen Übereinkünfte bestehen, sind Mitteilungen unzulässig
>
> a) in denen dem Empfänger für den Fall, dass er etwas tut oder unterlässt, Zwangsmaßnahmen oder sonstige Rechtsnachteile angedroht werden,
> b) durch deren Empfang Rechtswirkungen herbeigeführt, insbesondere Fristen in Lauf gesetzt werden, oder
> c) in denen der Empfänger zu einem Tun oder Unterlassen aufgefordert wird (z. B. eine Aufforderung zum Erscheinen vor einer Behörde).

II. Traditionelle »sonstige« Rechtshilfe



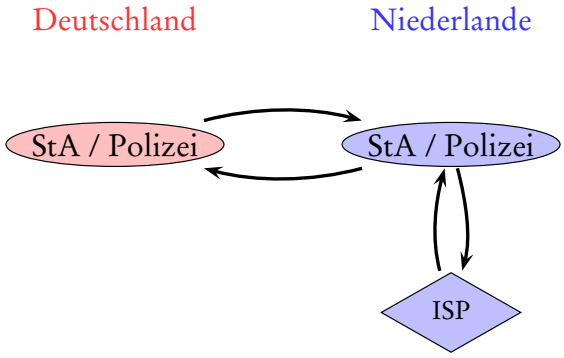
- Schutzmechanismen
- Aufwand
- Zeit – Problem bei Flüchtigkeit von Daten (»e-evidence«)
- Lokalisierung – Problem bei Volatilität von Daten (»e-evidence«)

§ 59 IRG (1) Auf Ersuchen einer zuständigen Stelle eines ausländischen Staates kann sonstige Rechtshilfe in einer strafrechtlichen Angelegenheit geleistet werden.

(2) Rechtshilfe im Sinne des Absatzes 1 ist jede Unterstützung, die für ein ausländisches Verfahren in einer strafrechtlichen Angelegenheit gewährt wird, unabhängig davon, ob das ausländische Verfahren von einem Gericht oder von einer Behörde betrieben wird und ob die Rechtshilfehandlung von einem Gericht oder von einer Behörde vorzunehmen ist.

(3) Die Rechtshilfe darf nur geleistet werden, wenn die Voraussetzungen vorliegen, unter denen deutsche Gerichte oder Behörden einander in entsprechenden Fällen Rechtshilfe leisten könnten.

III. Europäische Ermittlungsanordnung



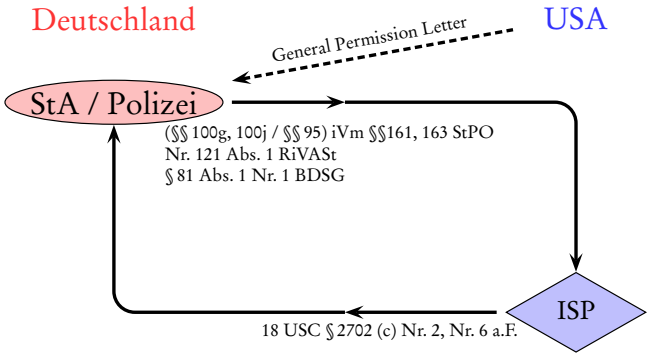
- Grundsatz der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen (Art. 82 AEUV)
- Europäische Ermittlungsanordnung / European Investigation Order
  - Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, AblEU 2014 L 130 v. 30.04.2014, S. 1–36
  - Umsetzung v.a. in §§ 91a ff. IRG
- grundsätzliche Verpflichtung zur Anerkennung – (enumerativer, str.) Katalog an Ablehnungsgründen
- strenge Fristen
- Verfahrensvereinfachung (Formblatt, unmittelbarer Kontakt)

IV. Direktanfragen an US-Provider – de lege abrogata

18 USC 2702 (c) a.F. A provider … may divulge a record or other information pertaining to a subscriber to … such service (not including the contents of communications …)— …

(2) with the lawful consent of the customer or subscriber; …

(6) to any person other than a governmental entity.



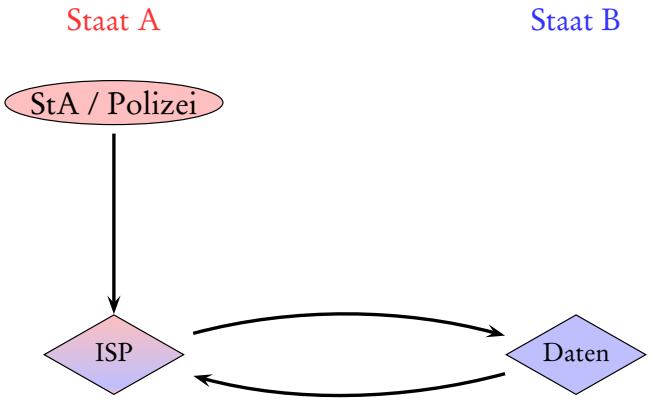
V. Umgehungsstrategien

1. Datenschutzanforderungen

Art. 44 DS-GVO Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden …

2. Domestikation

§ 5 II NetzDG Für Auskunftsersuchen einer inländischen Strafverfolgungsbehörde ist eine empfangsberechtigte Person im Inland zu benennen. Die empfangsberechtigte Person ist verpflichtet, auf Auskunftsersuchen nach Satz 1 48 Stunden nach Zugang zu antworten. Soweit das Auskunftsersuchen nicht mit einer das Ersuchen erschöpfenden Auskunft beantwortet wird, ist dies in der Antwort zu begründen.



D. Transnationale Direktanfragen – eine Zeitenwende

I. Direktanfragen an US-Provider – CLOUD Act

»DIVISION V — CLOUD ACT (Clarifying Lawful Overseas Use of Data Act)« des »Consolidated Appropriations Act, 2018« (H.R. 1625), in Kraft seit 23. März 2018:

18 USC 2702 (b) n.F. A provider … may divulge the contents of a communication …

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

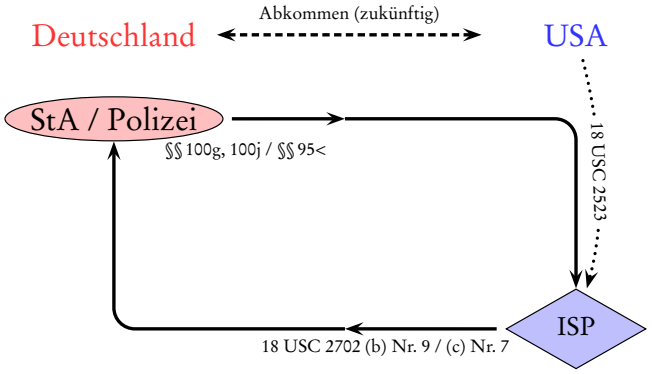
18 USC 2702 (c) n.F. A provider … may divulge a record or other information pertaining to a subscriber to … such service (not including the contents of communications …)— …

(7) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

Voraussetzungen (nach 18 USC 2523, Auswahl):

- »robust substantive and procedural protections for privacy and civil liberties«
- »adequate substantive and procedural laws on cybercrime and electronic evidence«

- »demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet«
- »the foreign government may not intentionally target a United States person or a person located in the United States«
- »shall be in compliance with the domestic law of that country« …»shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation«



II. Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen

- Vorschlag für eine **Verordnung** des Europäischen Parlaments und des Rates über **Europäische Herausgabeanordnungen** und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM(2018) 225 final v. 17.04.2018 (European Production Order / European Preservation Order)
- Anhänge zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM(2018) 225 final ANNEXES 1 to 3 v. 17.04.2018 (**Formblätter**)
- Vorschlag für eine **Richtlinie** des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die **Bestellung von Vertretern** zu Zwecken der Beweiserhebung in Strafverfahren, COM(2018) 226 final v. 17.04.2018

1. Anwendungsbereich

Persönlicher Anwendungsbereich (Adressaten)

Art. 2 Nr. 3 VO-E »Diensteanbieter« [ist] jede natürliche oder juristische Person, die eine oder mehrere der folgenden Kategorien von Dienstleistungen anbietet:

a) elektronische Kommunikationsdienste im Sinne des Artikels 2 Absatz 4 der [Richtlinie über den europäischen Kodex für die elektronische Kommunikation];

b) Dienste der Informationsgesellschaft im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates, bei denen die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist, einschließlich sozialer Netzwerke, Online-Marktplätze, die Transaktionen zwischen ihren Nutzern erleichtern, und anderen Anbietern von Hosting-Diensten;

c) Internetdomänennamen- und IP-Adressendienste wie IP-Adressenanbieter, Domänennamen-Register, Domänennamen-Registrierungsstellen und damit verbundene Datenschutz- und Proxy-Dienste;

Sachlicher Anwendungsbereich (e-evidence)

Art. 2 Nr. 6 VO-E »elektronische Beweismittel« [sind] Beweismittel, die zum Zeitpunkt [der …] Herausgabe- oder Sicherungsanordnung in elektronischer Form von einem Diensteanbieter oder in seinem Auftrag gespeichert werden und aus gespeicherten Teilnehmerdaten, Zugangsdaten, Transaktionsdaten und Inhaltsdaten bestehen

Art. 2 Nr. 7 bis Nr. 10 VO-E Differenzierung in Teilnehmerdaten (= Bestandsdaten), Zugangsdaten (= Zeitstempel, Benutzername, IP-Adresse u.ä.), Transaktionsdaten (= Meta- bzw. Verbindungsdaten i.Ü.), Inhaltsdaten

Art. 11 I VO-E Adressaten und … Diensteanbieter … sehen auf Aufforderung der Anordnungsbehörde davon ab, die Person, deren Daten angefordert werden, hiervon in Kenntnis zu setzen, um das betreffende Strafverfahren nicht zu behindern.

Art. 3 II 1 VO-E Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen dürfen nur für Strafverfahren während des Ermittlungs- und des Gerichtsverfahrens erlassen werden.

Art. 2 Nr. 1 VO-E »Europäische Herausgabeanordnung« [ist] eine verbindliche Entscheidung …, mit der ein Diensteanbieter … zur Herausgabe elektronischer Beweismittel verpflichtet wird;

Art. 2 Nr. 2 VO-E »Europäische Sicherungsanordnung« [ist] eine verbindliche Entscheidung …, mit der ein Diensteanbieter … im Hinblick auf ein späteres Ersuchen um Herausgabe zur Sicherung elektronischer Beweismittel verpflichtet wird;

Räumlicher Anwendungsbereich

Art. 3 I VO-E Diese Verordnung gilt für Diensteanbieter, die Dienstleistungen in der Union anbieten.

Erw.-Gr. 15 S. 2, Art. 1 I VO-E Die VO-E betrifft nicht innerstaatliche Konstellationen.

2. Verfahren und Ablehnungsgründe

(1.) Anordnung durch Strafverfolgungsbehörde des Anordnungsstaats

- Richtervorbehalt bei Herausgabeanordnung betreffend Transaktions- und Inhaltsdaten, im Übrigen Anordnung durch Staatsanwalt ausreichend (Art. 4 I bis III VO-E)
- Verhältnismäßigkeit; Rechtsgrundlage im innerstaatlichen Recht (Art. 5 II VO-E)
- Anfangsverdacht betreffend beliebiger Straftat (Art. 5 III, Art. 6 II VO-E); Ausnahme: Herausgabeanordnung betreffend Transaktions- und Inhaltsdaten (dann: Katalogtat, Art. 5 IV VO-E)
- ggf. Vorab-Konsultation vor Herausgabeanordnung, um Zeugnisverweigerungsrechte usw. zu wahren (Art. 5 VII VO-E)

(2.) Formblatt (EPOC / EPOC-PR) mit Minimalinformationen zu angewendeten Strafvorschriften, zu angeforderten Daten und zur Anordnungsbehörde (Art. 8 VO-E; Annex I, Annex II)

(3.) Ausführung durch den Diensteanbieter

- Fristen:
  EPOC-PR unverzügliche Sicherung der Daten für idR 60 Tage (Art. 10 I VO-E)
  EPOC Übermittlung binnen max. 10 Tagen, in Notfällen binnen max. 6 Stunden (Art. 9 I, II VO-E)
- Ablehnungsgründe (Art. 9 III bis V, Art. 10 IV bis VI, Art. 14, 15, 16 VO-E), betreffend EPOC im Einzelnen nur:
  unvollständiges oder fehlerhaftes Formblatt (Art. 14 IV (a) VO-E) Rückfrageverpflichtung (Art. 9 III VO-E)
  Unmöglichkeit (Art. 9 IV, Art. 14 IV (c), (d) VO-E)
  persönlicher Anwendungsbereich (Art. 14 IV (e) VO-E)
  fehlende Katalogtat (Art. 14 IV (c) VO-E) ⇒ Formblatt richtig ankreuzen!
  europäischer ordre public »ausschließlich aus den in dem EPOC enthaltenen Informationen geht hervor, dass das EPOC offenkundig gegen die Charta verstößt oder offensichtlich missbräuchlich ist« (Art. 14 IV (f) VO-E) ⇒ wegen mangelnder Informationen im EPOC bloßer Schein-Ablehnungsgrund
  »blocking statute« Befolgung einer Europäischen Herausgabeanordnung stünde im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats:
  – Grundrechte des Betroffenen (Art. 15 VO-E); Sonstiges (Art. 16 VO-E)
  – erfordert begründeten Einwand durch den Adressaten / Diensteanbieter
  – hält Anordnungsbehörde Anordnung aufrecht ⇒ Prüfung durch Gericht des Anordnungsstaats (ggf. mit Beteiligung von Behörden des Drittstaats)

(4.) ggf. Durchsetzung Vollstreckungsprozedur über Vollstreckungsbehörde im Vollstreckungsstaat (Art. 14 VO-E)

(5.) Rechtsschutz Möglichkeit zum nachträglichen Rechtsschutz im Anordnungsstaat (Art. 17 VO-E)

3. Kritik

Verdeckte Strafprozessrechtsharmonisierung und zweifelhafte kompetenzrechtliche Grundlage (Art. 82 I AEUV)

Mögl. Beeinträchtigung der internationalen Zusammenarbeit in Strafsachen, insbesondere bei unilateraler extraterritorialer Souveränitätsausübung

Zu weitreichender persönlicher Anwendungsbereich. Der VO-E und der begleitende RL-E erfasst nicht nur »große« TK-Dienstleister und Internetunternehmen, sondern – insb. bei extensiver Auslegung – auch im kleinen Kreis genutzte »Cloud-Server«. Mangelnde Differenzierung zwischen Diensteanbietern, Nutzungsarten und Speicherungsgründen.

Zu weitreichender sachlicher Anwendungsbereich. EPOC und EPOC-PR sind (jedenfalls auch) verdeckte Ermittlungsmaßnahmen ohne ausreichende, durch europäisches Recht zwingend vorgegebene Schutzmechanismen. Notwendigkeit des EPOC (bei Einführung des EPOC-PR und unter Berücksichtigung der EIO) zweifelhaft.

Zu weitreichender räumlicher Anwendungsbereich. EPOC und EPOC-PR erfassen auch Sachverhalte, die ausschließlich oder vorrangig den Vollstreckungsstaat betreffen.

Blindes Vertrauen in Anordnungsstaat. Nahezu vollständige Verlagerung des Rechtsschutzes (des Diensteanbieters, des Betroffenen, Dritter, …) in den Anordnungsstaat. Das erforderte tatsächlich ein sehr hohes Maß an gegenseitigem Vertrauen in den Grundrechtsschutz (einschl. Kernbereichsschutz), die Rechtsstaatlichkeit und die Sinnhaftigkeit der dort erlassenen Regelungen.

Marginalisierung des Rechtsschutzes im Vollstreckungsstaat. Kaum Möglichkeiten für Diensteanbieter, ihrerseits für Nutzer Grundrechtsschutz zu gewährleisten (»sole information contained in the EPOC«); kaum Anreiz für Diensteanbieter, Grundrechtsschutz zu gewährleisten (Ressourcen; Erw.-Gr. 46: Haftungsfreistellung). Privatisierung der Rechtshilfe mit reduzierter Kontrolldichte und marginaler (inner-)staatlicher Aufsicht.

Vorbild für Regelung in zweifelhaften Drittstaaten. Durch Erstreckung der eigenen »jurisdiction to prescribe« und der »jurisdiction to enforce« nimmt sich die EU Möglichkeiten, einen Datenabfluss an – auch zweifelhafte – Drittstaaten zu unterbinden.

⇒ **aus alledem resultierendes Missbrauchspotential** etwa für Wirtschaftsspionage, für exzessive Strafverfolgung, aber auch für politische Verfolgung.

⇒ **aus alledem teilweise Preisgabe staatlicher Souveränität.** Deutschland nimmt den Schutz der im Inland gespeicherten Daten – und damit mittelbar auch den Schutz derjenigen, die diese Daten speichern – vor ausländischer Souveränitätsausübung zurück.

E. Ausblick

- Bertele, Souveränität und Verfahrensrecht, Tübingen 1998
- Brodowski, NJW-aktuell ??/2018 (im Erscheinen)
- Burchard, Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen, ZIS 7+8/2018 (im Erscheinen)

ANHANG I

ZERTIFIKAT ÜBER EINE EUROPÄISCHE HERAUSGABEANORDNUNG (EPOC) ZUR

HERAUSGABE ELEKTRONISCHER BEWEISMITTEL

Gemäß der Verordnung (EU)...[1] muss der Adressat des Zertifikats über eine Europäische Herausgabeanordnung (EPOC) das EPOC ausführen und der unter Abschnitt G Ziffer i des EPOC genannten Behörde die angeforderten Daten übermitteln. Werden die Daten nicht herausgegeben, ist der Adressat nach Erhalt des EPOC verpflichtet, die angeforderten Daten zu sichern, es sei denn, er kann diese Daten nicht anhand der Angaben im EPOC identifizieren. Die Daten werden bis zur Herausgabe gesichert, oder bis die Anordnungsbehörde oder gegebenenfalls die Vollstreckungsbehörde mitteilt, dass die Sicherung und Herausgabe von Daten nicht mehr erforderlich ist.

Der Adressat trifft die erforderlichen Maßnahmen, um die Vertraulichkeit des EPOC sowie der herausgegebenen oder gesicherten Daten sicherzustellen.

ABSCHNITT A:

Anordnungsstaat: ……...

Hinweis: Nähere Informationen zur Anordnungsbehörde sind am Ende anzugeben (Abschnitte E und F).

Adressat:……..……..…

ABSCHNITT B: Fristen

Die angeforderten Daten sind binnen folgender Fristen herauszugeben (Zutreffendes bitte ankreuzen und ggf. erläutern):

□ spätestens binnen 10 Tagen

□ spätestens binnen 6 Stunden in einem Notfall aufgrund:

□ einer unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit einer Person. Begründung, falls erforderlich:

……

□ einer unmittelbaren Gefahr für eine kritische Infrastruktur im Sinne des Artikels 2 Buchstabe a der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

□ binnen einer anderen Frist (bitte angeben): ……..….. aus folgendem Grund:

□ unmittelbare Gefahr, dass die angeforderten Daten gelöscht werden
□ andere dringende Ermittlungsmaßnahmen
□ unmittelbar anstehendes Gerichtsverfahren
□ Verdächtiger oder Beschuldigter in Untersuchungshaft
□ sonstige Gründe: ……

[1] Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (*ABl. L...*).

ABSCHNITT C: Nutzerinformationen

Bitte beachten Sie, dass (sofern zutreffend, bitte ankreuzen):

□ der Adressat **die Person,** deren Daten mit dem EPOC angefordert werden, **hiervon nicht in Kenntnis setzen darf**.

ABSCHNITT D: Herauszugebende elektronische Beweismittel

i) Dieses EPOC betrifft (Zutreffendes bitte ankreuzen):

□ Teilnehmerdaten, die zumindest Folgendes umfassen:

□ Name, Anschrift, Geburtsdatum, Kontaktangaben (E-Mail-Adresse, Telefonnummer) und andere einschlägige Angaben zur Identität des Nutzers/Teilnehmers
□ Datum und Uhrzeit der ersten Registrierung/Anmeldung, Art der Registrierung/Anmeldung, Kopie des Vertrags, Methode der Identitätsüberprüfung zum Zeitpunkt der Registrierung/Anmeldung, Kopien der vom Teilnehmer vorgelegten Dokumente
□ Art des Dienstes, einschließlich Identifikator (Telefonnummer, IP-Adresse, SIM-Kartennummer, MAC-Adresse) und zugehörige(s) Gerät/Geräte
□ Angaben zum Profil (Nutzername, Profilbild)
□ Daten über die Validierung der Nutzung des Dienstes, z. B. eine vom Nutzer/Teilnehmer angegebene alternative E-Mail-Adresse
□ Debit- oder Kreditkarteninformationen (die vom Nutzer zu Abrechnungszwecken bereitgestellt wurden), einschließlich anderer Zahlungsmittel

□ PUK-Codes

□ Zugangsdaten, die zumindest Folgendes umfassen:

□ IP-Verbindungsdaten/-protokolle zu Identifizierungszwecken

□ Transaktionsdaten

□ Verkehrsdaten, die zumindest Folgendes umfassen:

a) für (Mobil-)Telefonie

□ ausgehende (A) und eingehende (B) Identifikatoren (Telefonnummer, IMSI, IMEI)
□ Verbindungszeit und -dauer
□ Anrufversuche
□ ID der Basisstation, einschließlich geografischer Koordinaten (X/Y-Koordinaten) zum Zeitpunkt des Verbindungsaufbaus und -endes
□ genutzter Träger-/Teledienst (z. B. UMTS, GPRS)

b) für Internet:

□ Routing-Informationen (Quell-IP-Adresse, Ziel-IP-Adresse(n), Port-Nummer(n), Browser, E-Mail-Header-Informationen, Message-ID)
□ ID der Basisstation, einschließlich geografischer Koordinaten (X/Y-Koordinaten) zum Zeitpunkt des Verbindungsaufbaus und -endes
□ Datenvolumen

c) für Hosting:

□ Protokolldateien
□ Tickets

□ Kaufhistorie

□ sonstige Transaktionsdaten, die zumindest Folgendes umfassen:

□ Historie über Prepaid-Aufladevorgänge
□ Kontaktliste

□ Inhaltsdaten, die zumindest Folgendes umfassen:

□ (Web-)Mailbox-Dump
□ Online-Storage-Dump (vom Nutzer generierte Daten)
□ Pagedump
□ Message log/Backup
□ Voicemail-Dump
□ Server-Inhalte
□ Geräte-Backup

ii) Die nachstehenden Informationen werden Ihnen zur Ausführung des EPOC zur Verfügung gestellt:

□ IP-Adresse:……
□ Telefonnummer:……
□ E-Mail-Adresse:……
□ IMEI-Nummer:……..
□ MAC-Adresse:……..
□ Person(en), deren Daten angefordert werden:……..……..
□ Name des Dienstes: ……...
□ Sonstiges: ……

iii) gegebenenfalls die Zeitspanne, für die die Herausgabe angefordert wird:

……..…….

iv) Bitte beachten Sie, dass (bitte ankreuzen und ausfüllen, sofern zutreffend):

□ die angeforderten Daten aufgrund eines früheren Ersuchens um Datensicherung folgender Behörde gespeichert wurden: ……...……
(Bitte die Behörde angeben und – sofern bekannt – das Datum der Übermittlung des Ersuchens sowie die Referenznummer). Diese Daten wurden übermittelt an:
……..……
(Bitte Diensteanbieter/Vertreter/Behörde angeben, an den/die das Ersuchen übermittelt wurde, sowie – falls bekannt – die vom Adressaten angegebene Referenznummer).

v) Art und rechtliche Würdigung der Straftat(en), die dem EPOC zugrunde liegen, und anwendbare Gesetzes-/Rechtsnorm:

……..……..……

Das vorliegende EPOC betrifft die Herausgabe von Transaktions- und/oder Inhaltsdaten im Zusammenhang mit (sofern zutreffend, bitte ankreuzen):

□ Straftat(en), die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden;

□ folgende Straftat(en), wenn diese ganz oder teilweise mittels eines Informationssystems begangen wurden:
□ Straftat(en) im Sinne der Artikel 3, 4 und 5 des Rahmenbeschlusses 2001/413/JI des Rates;

□ Straftat(en) im Sinne der Artikel 3 bis 7 der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates;

□ Straftat(en) im Sinne der Artikel 3 bis 8 der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates;

□ Straftat(en) im Sinne der Artikel 3 bis 12 und 14 der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates.

vi) Bitte beachten Sie, dass (sofern zutreffend, bitte ankreuzen):

□ die angeforderten Daten als Teil einer Infrastruktur gespeichert oder verarbeitet werden, die ein Diensteanbieter für ein Unternehmen oder eine Einrichtung, die keine natürliche Person ist, bereitstellt, und das vorliegende EPOC an den Diensteanbieter gerichtet ist, da auf das Unternehmen oder die Einrichtung abzielende Ermittlungsmaßnahmen nicht geeignet sind, insbesondere weil sie die Ermittlung beeinträchtigen könnten.

vii) Sonstige sachdienliche Informationen:

……..……..……

ABSCHNITT E: Angaben zur Behörde, die das EPOC ausgestellt hat

Art der Behörde, die das vorliegende EPOC ausgestellt hat (Zutreffendes bitte ankreuzen):

□ Richter, Gericht oder Ermittlungsrichter

□ Staatsanwalt (für Teilnehmer- und Zugangsdaten)

□ Staatsanwalt (für Transaktions- und Inhaltsdaten) → bitte auch Abschnitt F ausfüllen

□ andere vom Anordnungsstaat bezeichnete zuständige Behörde → bitte auch Abschnitt F ausfüllen

Angaben zur Anordnungsbehörde und/oder ihrem Vertreter zur Bescheinigung der inhaltlichen Richtigkeit des EPOC:

Name der Behörde:……..……

Name ihres Vertreters:……..……..

Funktion (Titel/Amtsbezeichnung):……..……

Dossier Nr.:……..……..