Prof. Dr. Stefan Braum

„Über den Wolken" – Grenzenlose Freiheit?*

Die Verformung des Europäischen Kriminaljustizsystems am Beispiel elektronischer Beweise

Résumé

La Commission européenne a présenté une proposition de règlement « relative aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale ». Il est destiné à répondre aux lacunes alléguées dans l'application de la loi lors de la collecte d'éléments de preuve à partir de données stockées dans le « cloud ». La proposition représente un changement de paradigme puisque le principe de territorialité est remplacé par le principe du marché. Elle implique un changement d'orientation du droit procédural pénal européen, qui passe de la reconnaissance mutuelle et de la coopération judiciaire à l'accès unilatéral de l'exécutif aux éléments de preuve. Cela porte atteinte aux principes de protection des données. Mais au-delà de ses conséquences immédiates, la proposition est avant tout un modèle à long terme pour déformer le système de justice pénale européen dans son ensemble. Elle fait partie d'un réseau européen d'enquête qui échappe largement à un contrôle judiciaire contraignant et efficace.

Abstract

The European Commission has presented a proposal for a Regulation on "European Production and Preservation orders for electronic evidence in criminal matters". It is intended to respond to alleged shortcomings in the enforcement of the law when gathering evidence from data stored in the cloud. The proposal represents a paradigm shift as the principle of territoriality is replaced by the principle of the marketplace. It implies a shift in the focus of European criminal procedural law from mutual recognition and judicial cooperation to unilateral executive access to evidence. This undermines data protection principles. Beyond its immediate consequences, however, the proposal is above all a long-term model for deforming the European criminal justice system as a whole. It is part of a European investigation network that largely eludes binding and effective judicial control.

„Ein Merkmal der digitalen Welt ist die Enthemmung und Maßlosigkeit ihrer Bewohner (...)".[1] Der Traum vom Naturzustand lebt – so scheint es. Der Naturzustand lässt sich als Raum der Freiheit aller begreifen, indes einer Freiheit die – das zeigt die Dis-

* *Prof. Dr. Stefan Braum*, Professur für Strafrecht, Université du Luxembourg.

1 Frankfurter Allgemeine Zeitung vom 26. März 2019, S. 1 (Bildtext).

KritV 2/2019, DOI: 10.5771/2193-7869-2019-2-93

kussion um Urheberrechte – so grenzenlos ist, dass sie sich um die gegenseitige Anerkennung von Rechten wenig schert. Vor allem aber ist der Naturzustand ein Raum der Mächtigen. Sowohl Staat und nicht zuletzt die wirtschaftlich geballte Macht privater Akteure sind zwingend bei der Durchsetzung ihrer Regeln. Die „Cloud" ist ein Zustand der Regellosigkeit – die Freiheit in den virtuellen Wolken erscheint grenzenlos, indes auch die rechtlich ungebundene politische und ökonomische Freiheit des Stärkeren.

Das europäische Kriminaljustizsystem steht vor der Herausforderung, die digitale Welt rechtlich zu konstituieren und die Maßlosigkeit seiner Bewohner – zu denen gerade auch staatliche Institutionen und globale Wirtschaftsakteure gehören – rechtlich einzuhegen. In nur naiver Form lässt sich das Internet als globaler Hort weltbürgerlicher Freiheit[2] denken. Vor allem ist es Gegenstand globaler Sozialkontrolle, die, weil ihr Gegenstand weit und allumfassend ist, ebenso tief und ubiquitär in Grundrechte einzugreifen vermag. Die Digitalisierung gibt sowohl staatlichen als auch privaten Akteuren nie dagewesene Möglichkeiten, soziale Kontrolle grenzenlos, universal und machtpolitisch funktional auszugestalten.[3] Wir werden Zeuge eines Prozesses der Konstituierung eines transnationalen Rechtsregimes, das den Zugriff auf Daten, deren Weitergabe und deren Schutz zum Gegenstand hat. Dabei erweisen sich digitale Herausforderungen nur als scheinbar neu. Bei deren Durchdringung durch das Recht kommt es schließlich auf die Frage an, wie es um die rechtliche Verfassung der Freiheit angesichts politischer und ökonomischer Macht steht.

Akteure politischer und gesellschaftlicher Macht versuchen ihr Verhältnis zu individueller Freiheit neu zu vermessen. Sie entfalten auf mehreren Ebenen Strategien, die mit dem Internet verknüpfte globale Konnektivität und den Austausch von Daten entweder ihrer Kontrolle zu unterwerfen, gegebenenfalls diese Kontrolle zu umgehen oder sie als machtpolitisches Instrument der Steuerung politischer Makroprobleme und ihrer Prozesse zu gebrauchen. Strategien finden sich auf der Ebene der Nationalstaaten, die etwa Inhalte des Internets filtern und blockieren und den Zugang zum World Wide Web regulieren, ihn begrenzen oder verweigern.[4] Über diesen Versuch der „Renationalisierung" der Internetregulierung hinaus, werden multilaterale Ansätze sichtbar, die entweder für gemeinsame Prinzipien der Internetregulierung – Schutz der Meinungsfreiheit, Transparenz, Datenschutz – streiten oder das genaue Gegenteil – Desinformation und Diskriminierung, Manipulation und ungehinderten Datenzugriff – bewirken wollen.[5]

Die Themen, an denen sich diese Neuvermessung versucht, sind zahlreich und sie sind einer dynamischen Rechtsentwicklung unterworfen. Dies betrifft den Schutz persönlicher Daten und deren ökonomischer oder auch – oft miβbräuchlicher – politischer Verwertung, dies umfasst das Urheberrecht oder den Umgang mit Rassismus und Hassreden im Netz. Dies betrifft nicht zuletzt auch das Kriminaljustizsystem: Die Konstituierung strafrechtlichen Zwangs im World Wide Web, insbesondere der strafprozesuale Zugriff auf persönliche Daten ist Seismograph der Freiheit im Angesicht

2 Vgl. Schmidt/Cohen, The New Digital Age, 2013, S. 13 ff.
3 Diskutiert bei Schmidt/Cohen unter dem Begriff „Police State 2.0", S. 75 ff.
4 Dazu Schmidt/Cohen, aaO., S. 83 ff.
5 AaO., S. 96 ff.

der Digitalisierung. So betrachtet, erweist sich auch der Zugriff auf elektronische Beweise nur vordergründig als neues Mittel europäischer Strategien im Umgang mit Kriminalität. Wer nur die Durchsetzung eines an einem gewissen Ort und zu einer gewissen Zeit geltenden politischen Katalogs an Regeln (auf neudeutsch „Law Enforcement“) in den Blick nimmt, verkennt die eigentliche Legitimationsfrage: Wie gelingt es im transnationalen Strafverfahrensrecht ein Rechtsregime zu etablieren, das die Grenzen politischer Macht gesetzmäßig und rechtsstaatlich hinreichend bestimmt? Geht man dieser Frage nach, mag der Entwurf der Verordnung zur Beibringung und Sicherung elektronischer Beweise[6] als Exempel dienen, in welchem Ausmaß die machtpolitisch gewollte Durchsetzung von Regeln mit konstituierter Freiheit kollidiert. In der Diskussion um elektronische Beweise in der Europäischen Union werden vor allem die Gefahren für die Freiheit sichtbar: Das Gesetzgebungsprojekt einer europäischen Beibringung elektronischer Beweise ist ein **Fehlschlag** einer freiheitlichen, gesetzmäßigen und rechtsstaatlichen Konstituierung transnationalen Strafrechts. Es ist

- Das Produkt einer fehlgeleiteten **Entgrenzung** politischer Souveränität (A);
- Beispiel der **Entformalisierung** europäischen Strafverfahrens und seiner gesetzgeberischen Legitimation (B);
- Beleg einer **Entleerung** des gerade nur mühsam begründeten europäischen Datenschutzes (C);
- Schließlich Instrument der **Verformung** des Strafrechts selbst in ein Instrument universeller sozialer Kontrolle (D).

Die einzige Alternative zu diesem Fehlschlag ist: das Gesetzgebungsprojekt muss zurückgezogen werden.

A. Entgrenzung

Die Konstituierung der Freiheit in Staat und Gesellschaft ist notwendig verbunden mit dem Begriff der Souveränität. Die politische Souveränität als Herrschaft der Staatsgewalt über ein bestimmtes Staatsvolk in einem bestimmten Staatsgebiet wandelte sich in eine normative durch Rechtsstaat und Grundrechte gebundene Souveränität. Angesichts von Globalisierung und Digitalisierung sehen sich diese Begriffe einer Transformation ausgesetzt, die sich in der Diskussion um elektronische Beweise widerspiegelt. Zum einen als Paradigmenwechsel vom Staatsgebiet zum Marktort (I), zum anderen als unilaterale Ausgestaltung politischer Macht in transnationalen Systemen (II).

6 Vgl. European Commission, Proposal for a Regulation of the European Parliament and the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final. (Im Folgenden VO-Entwurf).

I. Marktort und Territorialität – Virtuelle und analoge Spur des Kriminaljustizsystems?

Gemäß Artikel 1 VO-Entwurf sollen die Justizbehörden der Mitgliedstaaten die Möglichkeit erhalten, Internetdienstleister zu verpflichten, elektronische Beweise beizubringen oder zu sichern, unabhängig von deren Speicherort. In diesem Halbsatz liegt der entscheidende Ausgangspunkt des Paradigmenwechsels, der für ein transnationales europäisches Kriminaljustizsystem im Modus der Strafverfolgung prägend sein soll: der Zugriff der Ermittlungsbehörden kann unabhängig staatlicher Territorien erfolgen, er bezieht sich auf den Schwerpunkt wirtschaftlicher Aktivitäten eines Dienstleisters, er ersetzt den normativen Geltungsbereich staatlicher Souveränität durch die Faktizität ökonomischen Handelns, kurz die *Maxime des Marktortes* tritt an die Stelle des *Prinzips der Territorialität*.[7] Diese Schwerpunktverlagerung wird mit großer Selbstverständlichkeit eingeführt, so als sei sie die unbestreitbar notwendige Leitlinie bei der Ermittlung und Erhebung elektronischer Beweise.[8]

In den Motiven des Entwurfs sind die Grundrechte als Schranken grenzübergreifender Ermittlungen registriert, bleiben aber angesichts der Wucht kriminalpolitischen Wollens folgenlos. Geprägt ist der Zugriff durch Beschleunigung und durch Entgrenzung – beides Kennzeichnen der Digitalisierung, aber auch einer Sicherheitspolitik, die dieser folgt. Europäische Kriminalpolitik versucht im Wesentlichen auf zwei Aspekte zu reagieren: Zum einen auf die scheinbare *Entkopplung des Beweises von einem klar definierbaren Ort*.[9] Entgrenzung ist der Digitalisierung immanent: Daten finden sich auf Servern und zirkulieren zwischen Knotenpunkten des Internets, Dienstleistungen im Internet können von überall angeboten werden, Diensteanbieter verfügen nicht notwendigerweise über eine sachlich greifbare Infrastruktur, ihre Zugehörigkeit als juristische Person als Teil eines territorialen Geltungsbereichs ist verschieden von der Art und Weise der Dienstleistung. So finden sich für staatliche Strafverfolgungsbehörden Beweise nicht nur jenseits der eigenen Staatsgrenzen im Hoheitsbereich eines anderen Staates, sondern auch jenseits dieses zwischenstaatlichen Bereichs in einem virtuellen Raum, dort wo Daten gespeichert sind oder dort, wo der Dienstanbieter seinen Sitz hat. Zum anderen – eng mit dieser territorialen Entkopplung verbunden – soll es auf die *funktionale Effizienz eines beschleunigten Strafverfahrens ankommen*.[10] Die Maxime des Marktortes erlaubte den unmittelbaren Zugriff auf den elektronischen Beweis, ohne die Hürden zwischenstaatlicher Kooperation. Das so beschleunigte grenzübergreifende Strafverfahren soll auf die Beschleunigung reagieren, die mit Bedrohungsszenarien der digitalen Welt verbunden und insinuiert werden: das europäische Kriminaljustizystem rüstet sich für virtuelle Kämpfe um

7 Vgl. VO-Entwurf, Motive zu Kapitel 1, Artikel 1.
8 Mühelos erfolgt die Verlagerung von normativ gebundener Territorialität hin zu pragmatischen Erwägungen des Geschäfts- und Marktortes. In der englischen Fassung spiegelt der Topos „business considerations" diese Verlagerung eindrucksvoll wider (siehe ebenda).
9 VO-Entwurf, Motive I.
10 VO-Entwurf, ibidem.

Ordnung bis hin zum virtuellen Krieg.[11] Die Marktortmaxime findet ihre Rechtfertigung im *politischen Narrativ des bevorstehenden „Cyber-War".*[12]

Redundant erscheint es, wenn Artikel 1 neben der Maxime des Marktortes unterstreicht, dass die Verordnung die Kompetenzen nationaler Strafverfolgungsbehörden Internet-Dienstleister auf ihrem Territorium strafrechtlichem Zwang zu unterwerfen, ebenso unberührt lässt, wie die Grundrechte des Strafverfahrens (Art. 1 Abs. 2). Blickt man genauer hin, mag diese Redundanz und mag die betonte Selbstverständlichkeit des Grundrechtsschutzes nur vordergründig sein. Was sich hier bereits skizzenhaft andeutet, sind zwei Spuren europäischer Kriminaljustizsysteme: der europäische **Raum der Sicherheit** ist ein physischer und ein virtueller, kann ein analoger und ein digitaler Raum sein, wobei für den virtuellen Teil andere Regeln nach politischer Geltung drängen. So lässt sich das Verhältnis von Marktortprinzip und Territorialität, wie es Artikel 1 statuiert, auch umgekehrt lesen. Hier die Grundrechte, die physische Zwangswirkungen einhegen, dort ein transnationales Kriminaljustizsystem, das normative Grenzen seiner Funktionsbedingungen in der digitalen Welt der „Cloud" gerade neu vermisst.

II. Transformation der Souveränität

Grenzübergreifende Strafverfolgung war seit jeher ein Problem staatlicher Souveränität. In ihrer klassischen Konzeption knüpft sie daher an das Prinzip der beiderseitigen Strafbarkeit an: die Straftat, derentwegen verfolgt wurde, musste sich unter die Strafgesetze des jeweils anderen Staates subsumieren lassen.[13] Aus völkerrechtlichen Abgrenzungen, die sich im Respekt vor der physischen Zwangsgewalt des jeweils anderen Staates manifestieren, gewann dieser Ansatz seine legitimatorische Kraft. Später erst wird diese als unantastbare politische Handlungsmacht des Staates verstandene Souveränität ergänzt um dessen normative Bindungen. Die beiderseitige Strafbarkeit sichert das Prinzip der Strafgesetzlichkeit ab und gewährleistet mithin den Schutz bürgerlicher Freiheit auch bei grenzübergreifenden Fällen.[14] Strafgesetzlichkeit, bürgerliche Freiheit, beiderseitige Strafbarkeit und Territorialität sind in diesem Zusammenhang notwendig verknüpft,[15] was Auswirkungen auf die Bestimmung der sachlichen und örtlichen Zuständigkeit von Justizbehörden hat. Bei grenzübergreifenden Fällen ist der Staat zuständig, in dem die Tat begangen wurde oder in dem der Verdächtige seinen Wohnsitz hat. Bei komplexeren Straftaten wird zwischen Handlungs- und Erfolgsort unterschieden, kann sich die Zuständigkeit einer ausländischen Justizbehörde dann begründen, wenn auf ihrem Territorium der Schwerpunkt der Tatbege-

11 VO-Entwurf, ibidem, Absätze 2.1.1 und 2.3 des „Impact Assessment".
12 Kritisch Burchard, ZIS 2018, 190 ff. (S. 193 f.).
13 Vgl. etwa Franz von Liszt, Das Völkerrecht, 12. Auflage, 1925, S. 357.
14 Vgl. dazu Plachta, The Role of Double Criminality in international cooperation in penal matters, in: N. Jareborg (Hrsg.) Studies in International Criminal Law (1989), S. 84 ff. (S. 107 f.).
15 Vgl. zu diesem Zusammenhang auch D. Flore, Reconnaissance mutuelle, double incrimination et territorialité, in: La reconnaissance mutuelle des décisions judiciaires pénales dans l'Union Européenne (2001), S. 65 ff. (S. 69 f.).

hung lag. Das mag komplex sein, findet seine Legitimation aber in der prinzipiellen Einhegung und Begrenzung souveräner Staaten. Im Modus gegenseitiger Anerkennung wird das Prinzip beiderseitiger Strafbarkeit für einen Katalog an Straftaten durchbrochen, freilich – zu Recht oder zu Unrecht – insinuierend, dass europaweit ein gleiches Niveau an Grundrechtsschutz erreicht worden sei und mit der Prämisse, dass ein justizieller Rechtsakt im Kontext dieses Modus auf Grundlage einer reziproken Einbeziehung von Justizbehörden erfolgen muss. Daraus folgt – auch für den Modus gegenseitiger Anerkennung justizieller Entscheidungen – dass im Prinzip der Territorialität der Freiheitsschutz von Bürgern, die auf dem Territorium des durch die sie konstituierten Staates leben, notwendig enthalten ist.[16] Was aber in jedem Fall sichtbar bleibt, sind die Kriterien nach denen die zuständige Justizbehörde bestimmt wird. Die gesetzliche Bestimmtheit der sachlichen Zuständigkeit erweist sich im Raum der Freiheit, der Sicherheit und des Rechts als eine conditio sine qua non für die Lösung etwaiger Zuständigkeitskonflikte zwischen den Justizbehörden der Mitgliedstaaten.

Vergewissert man sich dieser Zusammenhänge lässt sich möglicherweise auch die Bedeutung ermessen, die das Umschalten vom Prinzip der Territorialität auf die Maxime des Marktortes bedeutet. Politisch gewollt lässt das Paradigma des Marktorts in der „Cloud" die *Legitimationserfordernisse freiheitlich gebundener Souveränität* am Boden des Rechts zurück.[17] Juristisch zwingend ist das nicht: Nationale Strafrechtssysteme stellen beim Zugriff auf – beispielsweise in einer Cloud gespeicherte – Daten auf den Standort des Servers ab, auf dem sich die Daten befinden (§ 110 StPO). International knüpft das Cybercrime-Übereinkommen ebenfalls an das Territorialitätsprinzip an (Art. 22 Abs. 1) und sieht im Fall konfligierender Zuständigkeiten Konsultationen zwischen den betroffenen Staaten vor, um die geeignete Jurisdiktion festzulegen (Art. 22, Abs. 5). Freilich mag diese am Tatortprinzip orientierte Ausgestaltung des Territorialitätsprinzips vor dem Hintergrund des Grundrechtsschutzes unbefriedigend wirken, weil angesichts der Ausdifferenzierung des Internets nicht nur die Strafverfolgung erschwert wird, sondern vor allem der Datenschutz nur noch transnational wirksam garantiert werden kann.[18] Aus der Absicht zum grenzüberschreitenden Rechtszwang („Law Enforcement") folgt gerade, dass man es nicht bei kontemplativer Betrachtung des Geschäftsverkehrs – „business considerations" – belassen darf.

So knüpft auch die Datenschutz-Grundverordnung in ihrem räumlichen Anwendungsbereich zum einen auf die Niederlassung des für die Daten Verantwortlichen oder des Auftragsverarbeiters an (Art. 3 Abs. 1 DSGVO), oder sie stellt zum anderen darauf ab, ob die Verarbeitung von Daten Unionsbürger betreffen (Art. 3 Abs. 2 DSGVO). Der räumliche Umfang des Grundrechtsschutzes wird zudem durch § 49 DSGVO abgesichert, der die Übermittlung von Daten an Drittstaaten nur in Ausnahmefällen erlaubt. Zum Zwecke eines EU-weiten kohärenten Datenschutzstandards nimmt die DSGVO Anleihen am klassischen Territorialitätsprinzip, gestaltet diese aber sachangemessen um. Sowohl im Niederlassungsort als auch in der Anknüpfung an den Aufenthaltsort von Unionsbürgern wird die Regel sichtbar, dass der Umfang

16 Vgl. dazu Cahin, La double incrimination dans le droit de l'extradition, R.G.D.I.P. 2013-3, S. 579 ff. (S. 597 ff.).

17 Kritisch dazu auch Burchhard, ZIS 2018, 249 ff. (S. 250).

18 Kritisch Fischer-Lescano/Teubner, S. 161 ff.

des Grundrechtsschutzes territorial verstanden wird. Es wäre widersprüchlich, diese Regel zu durchbrechen und die Erhebung elektronischer Beweise zu „entterritorialisieren“.[19] Dieser Widerspruch aber scheint bei der Erhebung elektronischer Beweise politisch gewollt, weil er bewußt Kontrapunkte zu einer Konzeption normativer Souveränität setzt.

Im Prozess der Konstituierung eines grenzübergreifenden Kriminaljustizsystems im Angesicht der „Cloud“ stehen sich machtverstärkende und machtbegrenzende Konzeptionen von Souveränität gegenüber. Auf der einen Seite liegt der Schwerpunkt auf der Ordnungskompetenz staatlicher Akteure, auf der anderen Seite geht es um die Neuorganisation eines an die bürgerliche Freiheit gekoppelten Begriffs von Souveränität. Angesichts des Multilateralismus im Netz[20] und der Transformationsprozesse von Souveränität hin zu staatlich entkoppelten Systemen, deren Normen und -kollisionen, lassen sich rechtstheoretische Erwägungen anstellen, Zuständigkeiten transnationaler Akteuren und deren justizielle Kontrolle neu zu justieren.[21] Markt und Dienstleistung werden eingerahmt durch Übereinkunft zwischen transnationalen Akteuren, wie Staaten, Staatenverbünden und NGOs. [22] Transnationale Gerichte schließlich sollen diese Übereinküfte justizförmiger Kontrolle unterwerfen.[23] Beides freilich in der Absicht, einen für das Internet möglicherweise sachgerechteren Rahmen des Grundrechts- und Freiheitsschutzes seiner Nutzer zu entwickeln.[24]

Für die Staaten erscheint dies indes wenig überzeugend. So wird der Übergang zwischen normativer territorial gebundener Souveränität und transstaatlicher prinzipiengebundener Regulierung durch die politische Tendenz konterkariert, den als Defizit politischer Handlungsfähigkeit empfundenen Verlust nationaler Souveränität durch einseitige Strategien der Rechtsdurchsetzung auszugleichen. Statt multilateraler Übereinkunft über den Zugang zu Daten, wird unilateral auf diese zugegriffen: die Regulierung in den USA – der Icloud-Act – liefert das Modell dieses unilateralen Zugriffs. Dieser fügt sich in den politischen Kontext der Erosion rechtsstaatlicher Prinzipien und der manifesten Krise einer multilateralen, sich an Demokratie und Bürgerrechte messenden Weltordnung.[25] Im scheinbar grenzenlosen Raum der Sicherheit liegt es nicht fern, ebenso grenzenlos auf jedwedes Beweismittel zugreifen zu können, wo immer es sich befindet. Dieser Zugriff wird als politischer Machtanspruch des staatli-

19 Zutreffend Burchard, ZIS 2018, 249 ff. (S. 251).
20 Vgl. Schmidt/Cohen, The New Digital Age, S. 96 ff.
21 Fischer-Lescano/Teubner, Regime-Kollisionen, S. 158 ff.
22 Vgl. etwa Berman, Vanderbilt Law Review, 2018, S. 11 ff. (S. 22 ff.); dazu auch Burchard, ZIS 2018, 249 ff. (S. 250).
23 Fischer-Lescano/Teubner, Regime-Kollisionen, S. 166 ff.
24 Vgl. auch Schmidt/Cohen, S. 98.
25 Kritisch Burchard, ZIS-online, 249 ff. (S. 253).

chen Souveräns ausgestaltet – ein Rückfall in ein normativ entgrenztes Modell staatlicher Macht. Die USA sind Vorreiter, Europa folgt.

B. Entformalisierung

I. Rechtsgrundlage – Vorrang politischer Zielbestimmung

Die Kommission stützt den Verordnungsvorschlag auf Art. 82 Abs. 1 AEUV, mithin auf den Grundsatz der gegenseitigen Anerkennung, wie er für die Zusammenarbeit zwischen Justizbehörden der Mitgliedstaaten einschlägig ist. Dabei wird unterstellt, der Artikel sei auch dann anwendbar, wenn sich die Justizbehörde eines ersuchenden Mitgliedstaates an irgendeine juristische Person in einem anderen Mitgliedstaat wendet, ohne dass es der Einbeziehung einer Justizbehörde des ersuchten Mitgliedstaates bedarf.[26] Vielmehr scheint es der Kommission zu genügen, dass diese Justizbehörde gegebenenfalls zur Vollstreckung des Ersuchens eingeschaltet werden kann, um die Kompetenz nach Art. 82 Abs. 1 AEUV zu begründen.[27] Dies steht weder mit dem Wortlaut noch mit dem Zweck des Artikels in Einklang.

Art. 82 Abs. 1 AEUV stellt ausdrücklich auf die Zusammenarbeit zwischen den Gerichten der Mitgliedstaaten ab, was nach einem *unmittelbaren Zusammenhang* zwischen der ersuchenden und der ersuchten Justizbehörde verlangt, ohne dass juristische Personen – schon gar nicht privaten Rechts – dazwischengeschaltet sind.[28] Dass eine nur indirekt, *nicht in allen Fällen verbindliche* Einbeziehung der Justizbehörde des ersuchten Mitgliedstaates ausreichte, lässt sich aus dem Wortlaut des Artikels nicht ableiten.[29] Art. 82 Abs. 1 lit. a AEUV erlaubt zwar Maßnahmen, Regeln festzulegen, die – scheinbar allgemein – der Durchsetzung gerichtlicher Entscheidungen in den Mitgliedstaaten der Europäischen Union dienen. Dies aber steht systematisch im Kontext des gesamten Absatzes 1, nämlich der reziproken justiziellen Zusammenarbeit.

Gegen einen einseitigen – unilateralen – Durchgriff durch eine Justizbehörde eines Mitgliedstaates gegenüber einer in einem anderen Mitgliedstaat ansässigen juristischen Person, sprechen auch Zweck und Entstehungsgeschichte der Ermächtigungsnorm. Beide hängen mit der Transformation von nationaler zu europäischer Souveränität eng zusammen und gewinnen daher besonderes normatives Gewicht. Die EU-Mitgliedstaaten übertragen einen Teil ihrer Souveränität an die Europäische Union, indem sie sich – gegenseitig und unter engen Voraussetzungen – den Entscheidungen eines anderen Mitgliedstaates unterwerfen. Nicht irgendeine Entscheidung rechtfertigt die Anerkennung des Strafrechts eines anderen Mitgliedstaates, sondern nur eine justiziell formell und materiell begründete. Die Übertragung solcher Kompetenzen ist daher ihrerseits am Bestimmtheitsgrundsatz zu messen und verbietet mithin die analo-

26 VO-Entwurf, Punkt 2, Legal basis.
27 Ibidem.
28 Vgl. Beschluss des Bundesrates, Drucksache 215/18, S. 4.
29 Vgl. dazu auch die "ECBA Opinion on European Commission Proposals for: (1) A Regulation on European Production and Preservation Orders for Electronic Evidence & (2) A Directive for Harmonized Rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings." (Punkt II.).

ge Anwendung auf nur ähnliche Fallkonstellationen, die Art. 82 AEUV selbst nicht unmittelbar erfasst.[30] Wie die Kommission selbst feststellt, ist die Einbeziehung der Justizbehörde des Landes, in dem der Adressat der Beweissammlung angesiedelt ist, nicht notwendig. Folglich liegt die zwingend erforderliche Unmittelbarkeit einer Rechtsbeziehung zwischen Justizbehörden, wie sie Art. 82 Abs. 1 AEUV voraussetzt, nicht vor. Vielmehr lässt sich die Wahl der Ermächtigungsgrundlage nur so erklären, dass der unilaterale Durchgriff der Justizbehörde eines Mitgliedstaates auf Private und deren Aktivitäten, wo immer diese sich in der EU verorten, mit Hilfe einer Verordnung mit unmittelbarer Rechtswirksamkeit geregelt werden sollte.[31] Der exekutivische Gedanke des vereinfachten Vollzugs justizieller Maßnahmen gewinnt in dieser Überlegung den Vorrang gegenüber einer mit dem Bestimmheitsgebot im Einklang stehenden Anwendung von Art. 82 Abs. 1 AEUV. Die dem Bestimmheitsgrundsatz geschuldete Form der Kompetenzgrundlage des Art. 82 wird abgeschliffen.[32]

II. Anwendungsbereich – Vorrang für politische Flexibilität

Liegt also im unmittelbaren Zugriff auf natürliche oder juristische Personen privaten Rechts schon eine Entformalisierung des Vertragsrechts, wird das Problem gesetzlicher Bestimmtheit im Sekundärrecht noch perpetuiert, betrachtet man sich den Anwendungsbereich der Verordnung:

Adressaten sind gemäß Art. 1 Abs. 1 VO-Entwurf solche Internet-Dienstleister, die ihre Online-Dienste in der Europäischen Union anbieten und die in einem Mitgliedstaat niedergelassen oder dort vertreten sind. Online-Dienste bietet gemäß Art. 2 Abs. 4 VO-Entwurf an, wer es juristischen oder natürlichen Personen ermöglicht, in einem oder mehreren Mitgliedstaaten online angebotene Dienstleistungen zu nutzen (lit. a) und dabei in einer wesentlichen Verbindung mit einem oder mehreren Mitgliedstaaten steht (lit. b). Bloßer Zugang zu einem Online-Auftritt, also einer Homepage, einer E-mail-Adresse oder zu anderen Kontaktdaten des Dienstleisters genügt demnach nicht. Wesentlich ist die Verbindung mit einem Mitgliedstaat jedenfalls dann, wenn der Dienstleister eine Niederlassung in der Europäischen Union hat, wobei es ausreicht, dass er tatsächlich für unbestimmte Zeit und von einem bestimmten – dauerhaften – Ort auf wirtschaftliches Handeln im Netz hin ausgerichtet ist (Art. 2 Abs. 5).Um diese Ausrichtung zu bestimmen, ist es – lediglich – erforderlich, eine bedeutende Anzahl von Nutzern in der EU aufzuweisen.[33]

30 Vgl. Beschluss des Bundesrates, Drucksache 215/18, S. 5 (lit b.).

31 VO-Entwurf, Punkt 2 Legal Basis, Unterabschnitt Choice of the Instrument.

32 Eine kriminalpolitische – aber gleichwohl berechtigte – Frage, wäre es, ob sich der weitreichende und unmittelbare Zugriff von Justizbehörden auf juristische Personen eines anderen Mitgliedstaates, die Voraussetzungen des Art. 82 AEUV einmal fingiert, derzeit auf das gegenseitige Vertrauen zwischen den Mitgliedstaaten – Kern der gegenseitigen Anerkennung – stützen kann. Angesichts rechtsstaatlicher Defizite von Mitgliedstaaten vor allem im Hinblick auf die richterliche Unabhängigkeit, die zum Teil durch die Einleitung eines Verfahrens nach Art. 7 EUV belegt sind, gilt es jedwede punitive Erweiterung des europäischen Sicherheitsraumes zurückzustellen. Dies gilt insbesondere für den grundrechtssensiblen Bereich des Strafverfahrensrechts.

33 Vgl. VO-Entwurf, Motive Artikel 3 Anwendungsbereich.

Der Kreis der Adressaten erfasst gemäß Art. 2 Abs. 3 VO die Dienste der Informationsgesellschaft, wie sie in Artikel 1 der EU-Richtlinie 2015/35 definiert sind. Freilich führt die Verweisung bei der Definition des Adressatenkreises nicht viel weiter. Dienste der Informationsgesellschaft sind danach solche, die „im Fernabsatz", „elektronisch" und auf „individuellen Abruf eines Empfängers" erbracht werden. Ein präzise bestimm- und eingrenzbarer Kreis der Normadressaten leitet sich daraus nicht unmittelbar ab. Vielmehr folgt dieser – gleichsam ex-negativo – aus einer im Anhang zur EU-Richtlinie 2015/35 beigefügten Liste von Diensten, die aus deren Anwendungsbereich herausfallen. Der elektronische Katalog eines Warenhauses, wird er in Anwesenheit eines Kunden konsultiert, unterfällt nicht dem Anwendungsbereich – wohl aber die Online-Suche im Rahmen des elektronischen Handels, die elektronische Buchung eine Flugtickets im Reisebüro in Anwesenheit eines Kunden, wird nicht erfasst – wohl aber die Online-Reservierung auf der Homepage einer Fluggesellschaft; die Geldausgabe am Automaten ist nicht Gegenstand der Richtlinie, wohl aber die im Web-Banking erfolgte Überweisung – die Liste ließe sich fortsetzen und sie ist lang. Sie erfasst Telekommunikations-Dienstleistungen im Netz, erstreckt sich auf Betreiber sozialer Netzwerke, auf Online-Handel und all seine Foren, auf Banken, Versicherungen, Verkehrs- und Transportunternehmen. Grundsätzlich erfasst sie alle Adressaten, mit denen wir alle im Internet täglich interagieren.[34]

Für eine strafprozessuale Maßnahme ist das bemerkenswert: Man muss sich dieser akzessorischen Verweisungstechnik des europäischen Gesetzgebers vergewissern, weil sie zum einen für den Bürger als Normadressaten als Form schwer zu erfassen ist und weil sie zum anderen – vor allem – durch die Form Inhalte fließend werden lässt. Den Adressatenkreis eines Rechtsaktes im Rahmen der Informationsgesellschaft möglichst offen zu lassen, mag angesichts des rasanten technologischen Wandels der Digitalisierung dem gesetzgeberischen Bedarf nach Flexibilität entsprechen. Wird dieser aber zum Bezugspunkt von Ermittlungskompetenzen in der digitalen Welt, gerät die politisch gewollte flexible Form zum formlosen politisch Gewollten. Die notwendige Regulierung der Informationstechnologie auf der einen Seite hat – in den Kontext des Kriminaljustizsystems gestellt – auf der anderen Seite das Legitimationsdefizit eines entformalisierten Zugriffs auf Bürgerrechte in seinem Rücken.

C. Entleerung

Gesetzesvollzug, Beschleunigung grenzüberschreitender Ermittlung, vermeintlich notwendige Anpassung des Strafverfahrensrechts an seine digitalen Herausforderungen bilden das kriminalpolitische Primat der Verordnung. Sie liegt auf der kriminalpolitischen Linie europäischer Institutionen, der Sicherheit den Vorrang vor Freiheitsrechten einzuräumen, die Exekutive gegenüber den anderen Akteuren des Kriminaljustizsystems zu stärken. In den Motiven der Verordnung ist zu registrieren, dass es an legitimatorischen Versuchen, Sicherheit und Freiheit ins Gleichgewicht zu setzen, nicht fehlt. Der unilaterale Zugriff auf elektronische Beweise soll die Anwendungseffizienz grenzübergreifender Ermittlungen zwar garantieren, aber auch Verfahrensrech-

34 Vgl. VO-Entwurf, Motive zu Artikel 2 Definitionen.

te und den Datenschutz nicht in Frage stellen.[35] Verwiesen wird auf die im Zuge der Roadmap-Gesetzgebung erreichten europäischen Verfahrensstandards ebenso wie auf einen Datenschutz-Aquis, wie er sich vor allem in der Datenschutz-Grundverordnung widerspiegelt.[36] Freilich erscheinen all diese Verweise strafjuristisch ungenau, zeigt sich der Grundrechtsschutz mehr als politische Deklaration denn als justizförmig wirksam. Der Zugriff auf elektronische Beweise ist ein Eingriff in den Schutzbereich des europäischen Grundrechts auf den Schutz persönlicher Daten (I), er unterliegt folglich Schranken, die an den Erfordernissen der Normenbestimmtheit, der Gesetzmäßigkeit der Beweiserhebung, der Zweckbindung und nicht zuletzt dem Prinzip der Verhältnismäßigkeit zu messen sind (II). Blickt man anhand dieser Kriterien genauer hin, entpuppt sich das in den Motiven des Verordnungsvorschlages behauptete Schutzniveau als sehr fragil. Im Angesicht seiner digitalen Herausforderungen wirkt die Konstituierung eines grenzübergreifenden Kriminaljustizsystems, das notwendig auf dem Respekt vor Rechtsprinzipien beruhen muss, inhaltlich leer.

I. Intensiver Eingriff

Reichweite und Tiefe des Eingriffs in das Recht auf den Schutz persönlicher Daten werden weder im Text noch in den Motiven der Verordnung mit der notwendigen juristischen Genauigkeit bestimmt. Schon der Anwendungsbereich und Adressatenkreis der Verordnung verdeutlichen indes, dass sich die Beweiserhebung nicht nur auf die Überwachung des Telekommunikationsverkehrs oder die Durchsuchung und Beschlagnahme von Personalcomputern erstreckt, sondern das Internet und seine Akteure selbst als vernetztes System erfasst. Die Daten, die gespeichert, gewonnen und verwertet werden sollen, beziehen nicht nur Zugangs- und Teilnehmerdaten ein,[37] sondern erstrecken sich auch auf Transaktions- und Inhaltsdaten,[38] wie sie im Rahmen der Nutzung informationstechnischer Systeme entstehen. Will die Verordnung so genannte Transaktionsdaten erfassen, geschieht dies explizit mit dem Verweis auf die Notwendigkeit, Verhaltensprofile von Internetnutzern im Rahmen eines Ermittlungsverfahrens zu gewinnen.[39] Daraus folgt, dass die Verordnung nicht nur – konkret-individuell – auf personenbezogene Daten zugreifen will, sondern vielmehr – abstrakt-generell – auf ein informationstechnisches System abzielt, um einen möglichst umfassenden Datenbestand zu sichern. Die Beibringung von Daten durch private Service-Provider ist mithin wesentlich weitreichender als etwa eine bloße Echtzeit-Überwachung von Telekommunikation, weil das Abrufen bestimmter Daten angesichts fortschreitender Digitalisierung der Lebenswelt umfassende Rückschlüsse auf das Leben einer Person bietet, bis hin zum Verhalten in der eigenen Wohnung, deren Geräte und

35 VO-Entwurf, Motive, „Context of the Proposal, Consistency with existing EU legal framework in the policy area and the Council of Europe Budapest Convention”.
36 Ibidem.
37 Art. 2 Abs. 7 Entwurf-VO; Art. 2 Abs. 8 Entwurf-VO; Art. 4 Abs. 1 Entwurf-VO.
38 Art. 2 Abs. 9 Entwurf-VO; Art. 2 Abs. 10 Entwurf-VO; Art. 4 Abs. 2 Entwurf-VO.
39 Erwägungsgrund 22, Entwurf-VO : « Transactional data (…) is generally pursued to obtain information about the contacts and whereabouts of the user and *may be served to establish a profile of an individual concerned.* ».

Einrichtungen durch informationstechnische Systeme gesteuert werden.[40] Solche Eingriffe aber wären – nach den Maßstäben des Bundesverfassungsgerichts – am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen, das über das Recht auf informationelle Selbstbestimmung noch hinausgeht, weil die Entwicklung informationstechnischer Systeme neue – und bislang unbekannte- Gefährdungen des allgemeinen Persönlichkeitsrechts mit sich führt.[41]

Zwar kennt das hier vorrangig einschlägige europäische Recht eine solche spezifische Interpretation der Art. 7 und 8 der EU-Grundrechtecharta (noch) nicht, der Europäische Gerichtshof geht aber gleichfalls von unterschiedlichen Graden der Eingriffsintensität in das Recht auf den Schutz personenbezogener Daten aus: Erweist sich ein Eingriff als besonders schwerwiegend, sind die Voraussetzungen, die den Eingriff sachlich rechtfertigen könnten, einer restriktiveren Auslegung zu unterziehen, verfügt der europäische Gesetzgeber nur über einen begrenzten Gestaltungsspielraum.[42] Schwerwiegend ist ein solcher Eingriff insbesondere dann, wenn der betroffene Teilnehmer oder der registrierte Nutzer nicht darüber informiert wird[43] oder wenn sich aus den erhobenen Daten weitgehende Rückschlüsse auf das Profil eines Rechtsadressaten ergeben können.[44] Beide Aspekte aber sollen für die Beibringung elektronischer Beweise charakteristisch sein. Zum einen macht sich der Verordnungs-Entwurf die Vertraulichkeit der Datenerhebung gerade zur wesentlichen Maxime, um den Ermittlungszweck nicht zu gefährden,[45] zum anderen ist es gerade dessen kriminalpolitisches Ziel, umfassende Datensätze zu gewinnen, um Personenprofile entwickeln zu können.[46] Folglich liegt – schon aufgrund dieser beiden Aspekte – ein besonders grundrechtsintensiver Eingriff in das Recht auf den Schutz persönlicher Daten vor, der strengen Maßstäben unterliegt; Maßstäben, denen der europäische Gesetzgeber in seinem Entwurf – bei weitem – nicht genügt:

II. Enge Grenzen

1. Normenbestimmtheit

Der Eingriff in das Recht auf den Schutz personenbezogener Daten verlangt nach klaren und präzisen Regeln im Hinblick auf Tragweite und Anwendung der Verordnung, insbesondere den wirksamen Schutz personenbezogener Daten vor Missbrauchsrisiken.[47] Wesentliche Entscheidungen über Eingriffe in europäische Grundrechte muss

40 Vgl. dazu S. Gless, StV 2018, 671 ff. (S. 672).
41 BVerfG (1 BvR 370/07, 1 BvR 596/07), Urteil vom 27. Februar 2008, 1. Leitsatz und Rz. 201 und 203.
42 EuGH (C-293/12 und C-594/12, Digital Rights Ireland U.A.), Rz. 37; EuGH (C-203/15 und C-698/15, Tele2 Sverige AB), Rz. 100).
43 EuGH (C-293/12 und C-594/12), Rz. 37; EuGH (C-203/15 und C-698/15), Rz. 100.
44 EuGH (C-203/15 und C-698/15), Rz. 99.
45 Art. 11 Entwurf-VO.
46 VO-Entwurf, Erwägungsgrund 23.
47 Vgl. EuGH Digital Rights Ireland (Fn. 42), Rz. 54.

der europäische Gesetzgeber selbst treffen, das europäische Gesetz muss steuernde und begrenzende Handlungsmaßstäbe vorfinden und justizförmig überprüfbar sein. Das Bestimmtheitsgebot setzt notwendig voraus, dass die Rechtslage für den Unionsbürger unzweifelhaft vorhersehbar und erkennbar ist.[48] Klarheit und Unzweideutigkeit der Rechtsgrundlage umfassen auch weitere normative Bedingungen eines Eingriffs in den Datenschutz, wie etwa dessen Zweckbindung und Verhältnismäßigkeit, sie betreffen aber ganz unmittelbar die Definition der Straftaten, zu deren Ermittlung die Erhebung und Verwertung elektronischer Beweise zulässig sein soll.

Art. 5 Abs. 1 des Entwurfs will bei allen Straftaten die Beibringung elektronischer Beweise erlauben, soweit es sich um Teilnehmer- oder Zugangsdaten handelt. Im Falle von Transaktions- und Inhaltsdaten schränkt Art. 5. Abs. 1 lit. a – lit.c den Anwendungsbereich auf bestimmte, akzessorisch definierte Straftaten ein. In den Motiven des Entwurfs kann man mit strafjuristischer Verblüffung feststellen, mit welchem Selbstverständnis und institutionellem Selbstbewusstsein der europäische Gesetzgeber dem allumfassenden Zugriff auf die europaweit gespeicherten Daten den Vorrang gegenüber der normativen Begrenzung dieses Zugriffs einräumt. Dies mag die Sorglosigkeit im Umgang mit dem Bestimmtheitsgebot begünstigen.

Zwei Aspekte belegen diese Sorglosigkeit: Sollen Teilnehmer- oder Zugangsdaten beigebracht oder gespeichert werden, gilt zum einen im Hinblick auf den Straftatbezug keine Begrenzung; alle Straftaten können eine Beibringung oder Speicherung auslösen – vom Diebstahl geringwertiger Sachen bis zum Hochverrat. Dabei ist der offensichtlich weite Anwendungsbereich nicht nur ein Problem der Verhältnismäßigkeit, sondern auch der Bestimmtheit. Zwar obliegt es der Strafgesetzgebung in den Mitgliedstaaten die jeweils gültigen Strafnormen mit der notwendigen Klarheit und Unzweideutigkeit in ihrem jeweils staatlichen Rechtskreis zu definieren. So hat der EuGH in *Advocaten voor de Wereld* kein Problem darin gesehen, dass der Grundsatz der beiderseitigen Strafbarkeit für einen Katalog von Straftaten, die der Rahmenbeschluss über den Europäischen Haftbefehl eher als Verhaltensweise denn als Straftatbestand beschrieb, keine Geltung mehr beanspruchen kann, weil das Bestimmtheitsgebot schon im ersuchenden Mitgliedstaat zu gewährleisten ist.[49] Auf die Vorhersehbarkeit der Normanwendung im ersuchten Mitgliedstaat kommt es demnach nicht an, weil das Prinzip der gegenseitigen Anerkennung selbst für einen Katalog von Straftaten – gedacht als europäische Verfahrensregel bei Wegfall der beiderseitigen Strafbarkeit – die Anerkennung des im jeweils anderen Mitgliedstaats herrschenden Bestimmtheitsniveaus schon mit sich führt.[50] Im Falle der Beibringungsanordnung aber wird im Wege einer strafprozessualen Maßnahme das materielle Strafrecht eines Mitgliedstaates in seiner Gesamtheit in einem oder mehreren anderen Mitgliedstaaten *unmittelbar* durchgesetzt und sind die Justizbehörden des ersuchten Mitgliedstaates gegebenenfalls nur *indirekt* eingebunden. Das Strafrecht eines anderen Mitgliedstaates kann jedoch in seiner Gesamtheit dann nicht für einen im ersuchenden Mitgliedstaat nicht ansässigen Bürger erkennbar und vorhersehbar sein, wenn es *im Wege strafpro-*

48 Ständige Rechtsprechung des EuGH, vgl. beispielhaft EuGH, Urteil vom 25. September 1984 (Rs. 117/83) (Könecke).

49 EuGH, Urteil vom 3. Mai 2007 (C-303/05).

50 EuGH, C-303/05, Rz. 53 f. Dazu Braum, wistra 2007, 401 ff. (S. 404).

zessualen Zwangs unmittelbare Geltung beansprucht. Dies gilt insbesondere dann, wenn die im ersuchenden Mitgliedstaat kriminalisierte Verhaltensnorm im ersuchten Mitgliedstaat straffrei ist. Die entsprechend notwendigen Grenzen aber formuliert der Entwurf nicht.[51]

Zum anderen scheint die Beibringung von Transaktions- und Inhaltsdaten hingegen zwar begrenzt, da sie nur für Straftaten Anwendung findet, die im Höchstmaß von mindestens drei Jahren Freiheitsstrafe bedroht (Art. 5 Abs. 1 lit. a VO-Entwurf) oder einer der in Art. 5 Abs. 1 lit b) und lit c) definierten Straftatbereiche zugehörig sind. Im Versuch aber Grenzen zu definieren, greift der europäische Gesetzgeber zur Technik der Akzessorietät. Der eigentliche Inhalt der Voraussetzungen nach Art. 5 Abs. 1 folgt aus dem Verweis auf weitere Rahmenbeschlüsse und Richtlinien. Das Bestimmtheitsgebot ist schon traditionell und durch nationale Strafgesetzgebung in einer Weise entleert, dass die Technik der Akzessorietät kaum auf wissenschaftlichen, schon gar nicht auf politischen Widerstand trifft.[52] Routiniert macht der europäische Gesetzgeber mithin von akzessorischer Gesetzgebungstechnik Gebrauch: Art. 5 lit. b nimmt daher Computerstraftaten in Bezug, deren Inhalt sich ihrerseits durch weitere Querverweise ergeben.[53] Ferner erstreckt sich die Norm sowohl auf Straftaten im Zusammenhang mit informationstechnischen Systemen[54] als auch auf solche, die den Terrorismus zum Gegenstand haben,[55] die ihrerseits wiederum auf Computerstraftaten und Straftaten im Zusammenhang mit Informationssystemen Bezug nehmen. Sorglos ist diese Routine der Akzessorietät, weil sie schon nicht mehr den Kern der Normen zu Kenntnis nimmt, auf die verwiesen wird: Die Beibringungsanordnung erstreckt sich nicht auf ausformulierte Straftatbestände, deren Tatbestandselemente der Auslegung zugänglich wären. Sie bezieht sich lediglich auf Mindestanforderungen des europäischen Gesetzgebers, die durch einen Gesetzgebungsakt umgesetzt und ausgestaltet werden müssen. Eine originäre Subsumtion eines Verhaltens unter einen Straftatbestand erlauben sie nicht. Dies mag solange kein Problem des europäischen Bestimmtheitsgebots sein, als die Formulierung von Mindestanforderungen als Gegenstand einer Richtlinie einen nationalen Strafgesetzgebungsakt voraussetzt und dieser dann dem Gesetzlichkeitsprinzip unterliegt. Die Beibringungsanordnung setzt als Verordnung jedoch die *unmittelbare Geltung der als Mindestanforderung ausgestalteten Umschreibung von Straftaten* voraus, die als solche in der Rechtsanwendung nicht subsumtionsfähig und folglich für Rechtsadressaten nicht erkennbar sein können.[56] Es läge dann ausschließlich im Ermessen des ersuchenden Mitgliedstaates, wie er die direkt aus der Verordnung folgenden Mindestanforderungen interpretiert, ohne sich prä-

51 Vgl. BR-Drucksache 215/18, S. 4 f. und S. 8.

52 Vgl. P.-A. Albrecht, Die vergessene Freiheit, 3. Auflage, S. 66 ff.

53 Rahmenbeschluss 2001/413 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, Art. 3, 4, 5. Dabei verweist Art. 4 des Rahmenbeschlusses (Straftaten bezogen auf spezielle Tatmittel) sowohl auf Art. 2 lit b des Rahmenbeschlusses (Straftaten bezogen auf Zahlungsinstrumente) als auch auf Artikel 3 (wiederum Computerstraftaten).

54 Richtlinie 2013/40 vom 12. August 2013 über Angriffe auf Informationssysteme (...), Art. 3 – 8.

55 Richtlinie 2017/541 vom 15. März 2017 zur Terrorismusbekämpfung (…). Art. 3 Abs. 1 lit i. verweist dabei auf Richtlinie 2013/40 und deren Artikel 9 Abs. 3 und Abs. 4.

56 BR-Drucksache 215/18, S. 9.

zise auf ein Strafgesetz beziehen zu müssen. So fehlt es an der Festigkeit von Tatbestandsvoraussetzungen, die den Rechtsanwender binden und die justiziell überprüfbar sind. Die sorglose Regulierungsroutine der Akzessorietät verkennt daher: Schon das Grunderfordernis der Strafgesetzlichkeit, nämlich die Formulierung eines Strafgesetzes selbst, das Gegenstand strafprozessualer Maßnahmen sein soll, wird durch den Entwurf der Verordnung nicht erfüllt.

2. Zweckbindungen des Datenschutzrechts

Die Zweckbindung des Datenschutzrechts ist mit dem Erfordernis einer klaren und unzweideutigen Rechtsgrundlage für Eingriffe in den Schutzbereich personenbezogener Daten eng verbunden. Dazu gehört, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.[57] Gemäß Art. 3 Nr. 2 des Entwurfs liegt der Zweck der Verordnung, in der Beibringung und Sicherung elektronischer Beweise im Rahmen eines ordentlichen Strafverfahrens, genauer: in Zusammenhang mit dem Ermittlungs- und Hauptverfahren. Seine Ausrichtung erscheint repressiv, der Zweck als zumindest legitim. Art. 5 Nr. 1 benennt die Voraussetzungen zur Umsetzung des Zwecks: Die Beibringung der Beweise muss zur Durchführung des Strafverfahrens erforderlich und verhältnismäßig (im engeren Sinne) sein und sie darf nur dann angeordnet werden, wenn eine ähnliche Maßnahme für dieselbe Straftat in einer vergleichbaren innerstaatlichen Situation zulässig wäre.

Das Strafverfahrensrecht setzt zur Legitimation jeglichen Eingriffs in bürgerliche Freiheitsrechte einen *Verdacht* voraus – je grundrechtsintensiver der Eingriff, desto strenger sind die Voraussetzungen, denen der Verdacht im Hinblick auf eine Straftat unterliegt. Im deutschen Strafverfahrensrecht findet sich im Anfangsverdacht des Legalitätsprinzips eine „Willkürschranke“ staatlicher Strafverfolgung.[58] Es liefert die praktische Übersetzung für das Prinzip der Strafgesetzlichkeit.[59] Das sei erwähnt, weil sich diese Grenze im Entwurf nicht findet, sie war schon nicht Gegenstand der Europäischen Ermittlungsanordnung.[60] Der Verzicht auf eine Verdachtsprüfung mag zwar fester Bestandteil des Auslieferungsverfahrens sein,[61] indes nur im Kontext fester und vorhersehbarer Kriterien beiderseitiger Strafbarkeit und Reziprozität normativer Standards. Europäisches Strafverfahrensrecht lässt nunmehr diese tradierten Grenzen hinter sich. An ihre Stelle treten Verhältnismäßigkeitserwägungen und eine hypothetische Prüfung. So kann eine Beibringungsanordnung schon dann erlassen werden, wenn sie für dieselbe Straftat in einer vergleichbaren Situation nach dem Recht des ersuchenden Mitgliedstaates erlassen werden könnte und sie für den Zweck der

57 EuGH, Rs. C-293/12 und C-594/12 (Digital Rights Ireland), Urteil vom 8. April 2014, Rz. 54; C-203/15 und C-698/15 (Tele2Sverige AB), Urteil vom 21. Dezember 2016, Rz. 102.
58 Siehe P.-A. Albrecht, Die vergessene Freiheit, aaO, S. 97 ff.
59 Ibidem, S. 97.
60 Richtlinie 2014/41 des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. L 130/1; Vgl. dazu Ahlbrecht, StV 2018, 601 ff und Böse, ZIS 4/2014, 152 ff. (S. 157).
61 Ibidem.

Durchführung eines Strafverfahrens erforderlich und angemessen wäre.[62] Hier treffen sich defizitäre Bestimmtheit und strafprozessuale Beweiserhebung, was die Eindeutigkeit der Zweckbindung in Frage stellt. Die Bindung an das Gesetz wird lose, da es nicht auf Präzision und Eindeutigkeit, sondern nur auf Ähnlichkeit und Vergleichbarkeit ankommen soll. Mangels strafgesetzlicher Genauigkeit obliegt es letztlich dem Ermessen der Strafverfolgungsorgane, zu entscheiden, ob die strafprozessuale Rechtslage ähnlich oder vergleichbar ist.[63] Das nur Ungefähre dieser Begründungsanforderung spiegelt den Verlust strafgesetzlich fester Formulierungen im Hinblick auf die in Bezug genommenen Straftaten wider. Eindeutig scheint letztlich nur das Problem, dass sich eine nur ungefähre Bindung an Regeln wirksamer (straf-)justizieller Kontrolle entzieht.

3. Verhältnismäßigkeit

Letztlich verdichtet sich die Frage nach der Legitimation des Eingriffs in das Recht auf den Schutz personenbezogener Daten in Verhältnismäßigkeitserwägungen. Die Merkmale der Geeignetheit, Erforderlichkeit und Angemessenheit der Beibringung und Feststellung elektronischer Beweise verarbeiten Erwägungen zur sachlichen Rechtfertigung dieser grenzübergreifenden strafprozessualen Maßnahme und deren Grenzen. Aufgrund fehlender Bestimmtheit und fragiler Zweckbindung erweist sich das Prinzip der Verhältnismässigkeit als ultimatives Auffangbecken, in dem Freiheitsrechte gegen exekutivische Effizienzerwägungen und Sicherheitsinteressen abgewogen werden. Für die Kriminalpolitik europäischer Institutionen geht diese Abwägung – oft einseitig – zugunsten der Sicherheit und zu Lasten bürgerlicher Freiheitsrechte aus. Justizieller Kontrolle – und wissenschaftlicher Kritik – kommt die Aufgabe zu, die Balance zwischen Freiheit und Sicherheit zurückzugewinnen. Das ist angesichts der Wucht einer „Law Enforcement"-Politik – und deren juristischer Apologien[64] – mühsam genug.

a) Geeignetheit – Vorrang unilateraler Beweiserhebung

Für den Gesetzgeber beurteilt sich die *Geeignetheit* der Maßnahme fast ausschließlich aus der Perspektive der mittels dieser Politik suggerierten Sachzwänge. Das Ziel ist der unmittelbare Zugriff auf elektronische Beweise und die vermeintlich damit verbundene Effizienzsteigerung grenzüberschreitender Ermittlungen. Dass es einen solchen im Hinblick auf die Begründung der Geeignetheit zu fordernden empirischen Kausalnachweis gibt, mag bereits bezweifelt werden. Entscheidend ist aber, dass schon die gewählte Form der Maßnahme – eine unmittelbar geltende Verordnung – die praktische Eignung im Strafverfahren in Frage stellt. Unmittelbar geltendes EU-

62 Art. 5 Nr. 1, 2. Absatz VO-Entwurf.

63 Kritisch dazu auch die Position des Deutschen Bundesrats, BR-Drucksache 215/18, S. 7 (Punkt f).

64 Vgl. etwa die fast durchweg affirmativen Beiträge zum VO-Entwurf in eucrim 2018, S. 212 – S. 225.

Recht wäre noch immer ein Fremdkörper im Strafverfahrensrecht, den die Praxis abstoßen würde, da er zum einen von tradierter strafprozessualer Terminologie entkoppelt (Verdachtsbegriff) und da er zum anderen angesichts strafprozessualer Handlungsalternativen im nationalen und europäischen Recht Anwendungsunsicherheiten generierte. Bereits die Form der Maßnahme wäre mithin nicht geeignet, um deren behauptete, sich scheinbar selbst tragende politische Zielbestimmung – „Law Enforcement" – zu implementieren.[65]

b) Erforderlichkeit – Vorrang für Vollzugsebene

Zudem wirft das Ineinandergreifen mit bereits existierenden Handlungsinstrumenten nationalen und europäischen Strafprozessrechts die Problematik der *Erforderlichkeit* der Maßnahme auf. Zurecht ließe sich fragen, warum es eines zusätzlichen Instruments bedarf, wenn es an evaluierten Erfahrungen mit der Implementation der Europäischen Ermittlungsanordnung noch fehlt.[66] In den Motiven des Entwurfs findet sich das Argument, dass die Europäische Ermittlungsanordnung elektronische Beweise nicht erfasse und zudem ein spezifisches Instrument vonnöten sei, dass die digitale Wirklichkeit des Kriminaljustizsystems abbilde.[67] Auch scheint es bei der Vorbereitung des Entwurfs nicht an einer empirischen Evaluation diverser Handlungsoptionen bei der Ausgestaltung der Maßnahme gefehlt zu haben.[68] Bemerkenswert ist jedoch, dass schon die Analyse kriminalpolitischen Bedarfs unter Einbeziehung juristischer Expertise zur politisch opportunen Affirmation dieses Bedarfs, a priori die *Vollzugsebene* – unmittelbare Beweisgewinnung – in den Blick nimmt, jedoch schon die *Anwendungsebene* im Funktionssystem des Strafverfahrens – wirksames, weil justizförmig abgesichertes Ermittlungsverfahren – weitgehend ignoriert. Dort aber hätte sich ergeben, dass sowohl das staatliche Strafprozessrecht als auch die gerade erst erfolgte Umsetzung der Ermittlungsanordnung zumindest ein gleichwirksames, milderes Mittel darstellt und der unilaterale Zugriff auf personenbezogene Daten einen Begründungsbedarf mit sich führt, dem der europäische Gesetzgeber nicht gerecht wird.[69]

c) Angemessenheit – Vorrang für Sicherheit

Schließlich würde die Legitimation des Entwurfs die Angemessenheit der Maßnahme voraussetzen. Überwiegt das geschützte Interesse – wirksames „Law Enforcement" im europäischen Strafverfahrensrecht – das beeinträchtigte Recht auf den Schutz personenbezogener Daten und andere Garantien eines fairen Strafverfahrens? Dies setzt voraus, dass die Grenzen dieser Beeinträchtigung rechtssicher definiert werden und je nach Schwere des Eingriffs wirksame prozedurale Garantien gelten, die die Rechte

65 So zutreffend Beschluss des Bundesrats Drucksache 215/18, Abs. 6 (S. 3).
66 ECBA, Opinion (vgl. Fn 29), S. 3 f.
67 VO-Entwurf, Motive, S. 6 f. (Verhältnismäßigkeit).
68 VO-Entwurf, Motive, S. 7 ff.
69 ECBA, Opinion (oben Fn 29), S. 3.

der Betroffenen absichern.[70] Dazu zählt, dass die Vertraulichkeit persönlicher Daten nur dann aufgehoben werden kann, wenn es der Ermittlung schwerer Kriminalität dient. [71] Dazu gehört, dass es Verfahren gibt, die den behördlichen Zugriff auf die Daten klar regeln.[72] Dazu gehört vor allem, dass der Zugang zu gespeicherten Daten dem Richtervorbehalt unterliegt, von einer unabhängigen Behörde kontrolliert wird und die betroffenen Daten innerhalb der Europäischen Union gespeichert werden.[73] Wie notwendig diese Grenzen sind, und wie streng sie interpretiert werden, hängt auch von der Intensität des Eingriffs ab, mit dem der Schutz eines übergeordneten Interesses behauptet wird. Intensität und Tiefe des Eingriffs folgen zum einen aus dem Umfang der Daten – und deren Typus – die im Anwendungsbereich der Verordnung liegen sollen.

aa) Datenprofile

Die Verordnung gestattet den Zugriff auf *Zugangsdaten*, zumindest auf diejenigen, die zum Zeitpunkt der Beibringungsanordnung schon gespeichert sind. Dies umfasst den Beginn und das Ende der Nutzung eines Internet-Services, Datum und Zeitpunkt der Nutzung sowie den Zeitpunkt des logins und des logouts, einschließlich der Metadaten, die bei jeglicher Internet-Kommunikation anfallen.[74] Ferner sind *Teilnehmerdaten* erfasst, die umfassend die Identität des Teilnehmers, des Kunden, die Daten von Gesprächen und deren Dauer zum Gegenstand haben. Ausgenommen sind Passwörter und andere Schlüssel zur Authentifizierung. Der Entwurf führt darüber hinaus einen Datentypus ein, der in der Datenschutz-Grundverordnung nicht als solcher explizit erwähnt sind – die *„Transaktionsdaten"*. Enthalten sind darin „Daten über die Erbringung einer von einem Diensteanbieter angebotenen Dienstleistung, die Kontext-oder Zusatzinformationen über eine solche Dienstleistung liefern und von einem Informationssystem des Diensteanbieters generiert oder verarbeitet werden".[75] Beispielhaft werden Sende-und Empfangsdaten einer Nachricht oder einer anderen Art von Interaktion, Daten über den Standort des Geräts, Datum, Uhrzeit, Dauer, Größe, Route, Format, Daten über das verwendete Protokoll und die Art der Kompression genannt.[76] Metadaten werden auch hier als möglicher Bezugspunkt des Datenzugriffs mitgeführt. Und schließlich Inhaltsdaten, also solche gespeicherten Daten in digitalem Format wie Texte, Stimmen, Videos und Bilder, soweit sie von Teilnehmer, Zugangs- und Transaktionsdaten verschieden sind.

Im Unterschied zur – für ungültig erklärten – Richtlinie zur Vorratsdatenspeicherung ist der Zugriff auf elektronische Daten weder anlasslos noch erstreckt er sich auf einen zu allgemeinen Zweck – Gewährleistung der inneren Sicherheit. Gleichwohl erinnert die Sicherung der im Moment der Anordnung gespeicherten Daten an das „Quick-Freeze-Modell", das schon als Alternative zur Vorratsdatenspeicherung disku-

70 Siehe etwa Bundesverfassungsgericht (aaO. Fn 41), Rz. 257.
71 EuGH C-203/15 und EuGH C-698/15, Rz. 102.
72 EuGH, aaO., Rz. 118.
73 EuGH, aaO., Rz. 120 u. 125.
74 Art. 2 Abs. 8 Entwurf-VO.
75 Art. 2 Abs. 9 Entwurf-VO.
76 aaO.

tiert wurde. Nun scheint sich ein Strafverfolgungsansatz zu entfalten, der eine demnächst modifizierte Vorratsdatenspeicherung mit der Erhebung von bereits bei Privaten gespeicherten Daten vereinen könnte. Mag auch die letztere in repressiver Absicht in ein laufendes Strafverfahren integriert sein, erweist sich der Umfang der Daten, die durch Private beigebracht oder gesichert werden müssen, als sehr erheblich. So beharrt der Verordnungsgeber darauf, dass alle vier Datenkategorien vonnöten seien, will man einen umfassenden Zugriff der Ermittlungsbehörden gewährleisten.[77] Es genüge nicht lediglich Zugangs- und Teilnehmerdaten in den Fokus zu nehmen. Der eigentliche Mehrwert bei der Beweisgewinnung erfolgt für den Verordnungsgeber gerade aus der möglichen Nutzung von Transaktions- und Inhaltsdaten.[78] Es ist juristisch beunruhigend zu sehen, mit welcher exekutivischen Gewissheit, Informationen über Kontakte und Aufenthaltsorte eines Benutzers gesammelt werden sollen, mit dem Ziel, das Profil eines Bürgers für die Akteure des Kriminaljustizsystems sichtbar werden zu lassen. Gerade aus der Verknüpfung der vier Datenkategorien lassen sich umfassende Rückschlüsse über das Privatleben eines Nutzers ziehen. Nichts bleibt verborgen und alles scheint möglich: mit Hilfe von Algorithmen werden private Vorlieben, berufliche Verbindungen, familiäre Situation, gesundheitliche Defizite und gar das Verhalten in der eigenen Wohnung bei Ermittlungsbedarf transparent. Da alles möglich scheint, erscheint es in der digitalisierten Welt des Kriminaljustizystems auch folgerichtig, dass es eine prozedurale Wahrheit um jeden Preis geben müsse.[79] Das ist eine beklemmende Perspektive.[80]

bb) Geheimes Verfahren

Hinzu kommt: die Erhebung elektronischer Beweise wird durch die Maxime der Vertraulichkeit gesichert. Gemeint ist indes nicht die Vertraulichkeit personenbezogener Daten, sondern die des staatlichen Ermittlungsverfahrens. Der von der Datenerhebung Betroffene soll solange nicht über die Datenerhebung informiert werden als es der Zweck des Ermittlungsverfahrens erfordert.[81] Dieses Modell heimlicher Ermittlung – unter Einbeziehung von Privaten – perpetuiert die Intensität des ohnehin umfänglichen Eingriffs. Das Recht auf Belehrung, das Recht zu schweigen, Beweisverbote insgesamt laufen leer, wenn in einer frühen Phase des Verfahrens die Beweiserhebung notwendig auf Geheimhaltung angelegt ist.[82] Daraus folgend müsste die Verordnung zumindest Verfahrensregeln etablieren, die den Eingriff besonders restriktiven Erfordernissen unterwirft.[83]

77 VO-Entwurf, Erwägungsgrund 23.
78 aaO.
79 Erneut abgesichert durch affirmative (mit Drittmitteln gestützte) Wissenschaft, die der Politik des „Law Enforcement" keine normativen Grenzen setzt, sondern (rechts-)technische Möglichkeiten erst aufzeigt. Beispielhaft M.A. Biasiotti, A Proposed Electronic Evidence Exchange across the European Union, Digital Evidence and Electronic Signature Law Review 14 (2017).
80 Ähnlich Burchard, ZIS-online 2018, 249 ff. (S. 264 ff).
81 Art. 11 Abs. 1 und Abs. 2 Entwurf-VO.
82 Vgl. dazu P.-A. Albrecht, Kriminologie, 3. Auflage, S. 154 ff.
83 Vgl. zum Beispiel EuGH Rs. C-293/12 und C-594/12 (Digital Rights Ireland), Rn. 48.

cc) Fragile Verfahrensrechte

Selbstsicher trägt der Verordnungsgeber vor, dass diese Intensität des Grundrechtseingriffs prozedural aufgefangen werde, was sich in differenzierten Strafverfolgungsvoraussetzungen widerspiegele.[84] Daran ist zunächst eimal richtig, dass für Transaktions- und Inhaltsdaten wegen deren – offenkundig – besonders sensiblen Charakters der Richtervorbehalt gilt**,** wohingegen der Zugriff auf Zugangs- und Teilnehmerdaten bereits nach staatsanwaltschaftlicher Genehmigung von Seiten des ersuchenden Mitgliedstaates erfolgen darf.[85] Diese prozeduralen Voraussetzungen aber erweisen sich bei näherem Hinsehen als fragil. Vier Aspekte unterstreichen diese Fragilität:

- Erodierte Gesetzesbindung

Zum einen – wir haben es gesehen – wird das Bestimmtheitsgebot unterminiert, weil die Straftaten, die in Bezug genommen werden, zu vage, zu breit und zu unklar definiert werden und weil es – vor allem – dem exekutivischen, kaum überprüfbaren Ermittlungsermessen eines Mitgliedstaates anheim gestellt ist vom Anfangsverdacht einer Straftat auszugehen.[86] Es kommt hinzu, dass bei der Erhebung von Transaktions- und Inhaltsdaten die Schranken der Zweckbindung sowie des Bestimmtheitsgebots ihrerseits ihre Grenzen an der Effizienz des Rechtsinstruments finden sollen. Legitimationsbedingungen des Grundrechtseingriffs stehen unter dem *Vorbehalt der Effizienz exekutivischer Sicherheitspolitik*: Im Falle von Internet gestützten Straftaten oder solchen Straftaten, bei denen ein terroristischer Kontext hergestellt wird, könnten sämtliche Datenkategorien unabhängig von der Schwere der Straftat erhoben werden.[87] Im politischen Bestreben die digitale Welt kriminalisierend vollständig zu durchdringen, gelten Begrenzungen der Strafverfolgung nicht. Der Maβstab ist lediglich die drohende Gefahr, selbst bei minderschweren Straftaten.[88] Erscheint es kriminalpolitisch opportun, wird die Bindung der Exekutive an präzise, verbindliche und begrenzende Zwecken des Eingriffs gelockert.

- Erodierte Beweisverbote

Zum anderen obliegt es gleichfalls dem exekutivischen Ermittlungsermessen des ersuchenden Mitgliedstaates, ob die Beibringung oder Sicherung eines Beweises einem absoluten oder relativen Beweisverbot in einem anderen Mitgliedstaat unterliegt. Gemäss Art. 5 Nr. 7 des Entwurfs definiert der ersuchende Mitgliedstaat die Reichweite eines absoluten oder relativen Beweisverbotes und determiniert so die Beweisverwertung im Verfahren. Zwar sieht der Verordnungsvorschlag vor, dass Beweisverbote im ausführenden Mitgliedstaat berücksichtigt werden sollen.[89] Deren Gewährleistung obliegt aber nur der justiziellen Kontrolle im ersuchenden Mitgliedstaat. Lediglich dort kann auch der Betroffene Rechtsschutz gegen den Zugriff auf seine Daten nachsuchen.[90] Dies ist zugleich praxisfern und realitätsfremd. Es schwächt die Rechtspositi-

84 VO-Entwurf, Erwägungsgrund 23.
85 VO-Entwurf, Artikel 4 Nr. 1 und Nr. 2.
86 Vgl. oben C II 2.
87 VO-Entwurf, Erwägungsgrund 31.
88 VO-Entwurf, Erwägungsgrund 32.
89 Art. 18 VO-Entwurf.
90 Art. 17 VO-Entwurf.

on des Betroffenen, wenn er seine Rechte in einer für ihn fremden Rechtsordnung verteidigen soll.[91] Es schwächt zudem die normative Professionalität unabhängiger Justiz im ersuchenden Mitgliedstaat, da eine rechtsvergleichende Strafprozessdogmatik, die den eigenen und den externen strafprozessualen Regelungsbereich integriert weder methodisch noch normativ und schon gar nicht grenzübergreifend hinreichend substantiiert ist.[92] Dabei belegt gerade die Dogmatik der Beweisverbote die immer noch signifikanten Unterschiede zwischen den nationalen Kriminaljustizsystemen im Hinblick sowohl auf Beweisthemen als auch auf die Methoden der Beweiserhebung und vor allem im Hinblick auf den normativen Zusammenhang zwischen unzulässiger Beweiserhebung und dem Verbot der Beweisverwertung.[93] Der behauptete Rechtsschutz bleibt somit deklaratorisch, ein Anschein von Rechtsschutz der sich formal und inhaltlich praktischer Wirksamkeit entzieht.

- Informalisierung

Justizförmige, rechtssichere und für den Bürger vorhersehbare Kontrolle erscheinen nicht zuletzt auch deswegen fragil, weil das Verfahren der Beibringung elektronischer Beweise – politisch gewollt – informeller Natur ist. Sein Kern besteht darin, die *eigentlich öffentliche Aufgabe des Grundrechtsschutzes zu privatisieren*. Gemäß Art. 7 des Entwurfs ist ein durch den Internet-Dienstleister bestimmter Vertreter zugleich auch der Empfänger der Anordnung. Die Anordnung selbst muss eine Reihe von Informationen enthalten, unter anderem die Person, deren Daten erhoben werden sollen sowie deren Kategorie und der Erhebungszeitraum. Sie enthält nach dem Entwurf jedoch nicht die ungleich wichtigeren Gründe, die auf die Erforderlichkeit und Angemessenheit der Maßnahme schließen lassen.[94] Private dürften daher mit der Kontrolle der in Frage stehenden Rechte der Unionsbürger zum einen überfordert sein,[95] zum anderen werden sie angesichts strenger Fristen bei der Sicherung der Daten a priori in eine exekutivische Drucksituation versetzt, die eine sorgfältige Prüfung faktisch unmöglich macht. Schon zehn Tage nach Zugang der Anordnung sind die Daten an die Behörde des ersuchenden Mitgliedstaates zu übermitteln, bei Gefahr im Verzug gar bereits nach sechs Stunden.[96] In der Vollstreckungsphilosophie des Entwurfs genießt die Beschleunigung des Verfahrens den Vorrang vor dem Schutz individueller Verfahrensrechte. Dies wird noch dadurch unterstrichen, dass für den privaten Dienstleister ein Versagungsgrund der Anordnung nur dann gegeben sein soll, wenn diese offen-

91 ECBA, Opinion, (Punkt 2 „Limited right of appeal by individual concerned").
92 Ebenfalls kritisch Deutscher Bundesrat, BR-Drucksache 215/18, S. 6 (Punkt 7 e). Vgl. auch Ahlbrecht StV 2018, 601 ff. (S. 608).
93 Gerade in jüngster Zeit ist das eindrucksvoll belegt im Fall des Whistleblowers *Rui Pinto* (Football-Leaks). Nach Auffassung der portugiesischen Justiz seien die Daten in dessen Besitz illegal erlangt und mithin unverwertbar, währenddessen Frankreich, Belgien oder die Niederlande die Daten verwerten können, auch dann, wenn sie mittels einer Straftat erlangt sind. Ausführlich und en détail entfaltet ist die Problematik der Beweisverbote im Raum der Freiheit, der Sicherheit und des Rechts bei M. Marty, La légalité de la preuve dans l'espace pénal européen, Diss.iur, Université du Luxembourg, 2014 (Date de soutenance : 1.04.2014).
94 Art. 8 Nr. 3 VO-Entwurf.
95 BR-Drucksache 215/18, S. 5 (Punkt 7 c).
96 Art. 9 Nr. 1 und Nr. 2 VO-Entwurf.

sichtlich die EU-Grundrechtecharta verletzt oder offensichtlich rechtsmissbräuchlich ist.[97] Dem ersuchenden Mitgliedstaat steht mithin kein gleichgewichtiges Pendant gegenüber, das die Weite des Grundrechtseingriffs mittels restriktiver Verfahrenskontrolle kompensieren könnte.

Erst im weiteren Vollstreckungsverfahren kann die Justizbehörde des ersuchten Mitgliedstaates eingeschaltet werden, wenn auch nur hilfsweise, falls der private Dienstleister der Beibringungsanordnung nicht oder nicht rechtzeitig entspricht.[98] In diesem Fall kann auch die Kontrolle nationaler Beweisverbote Geltung beanspruchen – wenn auch nur eingeschränkt.[99] Denn selbst für diesen Fall entfaltet sich der Primat der Beschleunigung über das Paradigma des Rechtschutzes. Unverzüglich soll das Gesuch umgesetzt werden, es sei denn, es liegt eine offensichtliche Verletzung der EU-Grundrechtecharta oder ein offensichtlicher Rechtsmissbrauch vor.[100] Ein solcher ließe sich aber nur auf der Grundlage der in der Beibringungsanordnung selbst gegebenen Tatsachen begründen. Inhaltlich soll die Offensichtlichkeit einer solchen Rechtsverletzung nur dann gegeben sein, wenn die Zweckbindung des Datenzugriffs gänzlich ignoriert wurde. Die Inhalte des Verfahrens und die Reichweite des Grundrechtsschutzes, der sich gerade in Beweisverboten manifestiert, bleibt somit vorrangig dem Ermessen der ersuchenden Justizbehörde überlassen. Das *Verfahren*, das der Legitimation des Eingriffs dient, bleibt *fragmentarisch.*[101]

- Erodierter Datenschutz – weltweit

Schließlich: Der Entwurf versucht sich Legitimation zu verschaffen, indem er ein Kontrollverfahren beim Zugriff auf in Drittstaaten gespeicherte Daten etabliert, mit dem Ziel Rechtskonflikte zwischen dem betroffenen Dienstleister und dem Drittstaat zu vermeiden. Jedoch lässt sich jede justizielle Kontrolle konfligierender Rechte mit Hilfe von Exekutiv-Vereinbarungen zwischen der Europäischen Union und einem Drittstaat unterlaufen. Die Figur des „Executive Agreements" wird so angesichts der Tendenz eines unilateralen Zugriffs auf Daten im virtuellen Kriminaljustizsystem das

97 Art. 9 Nr. 5 VO-Entwurf. In den durch den Europäischen Rat vorgeschlagenen Ergänzungen entfällt selbst dieser Versagungsgrund: Rat der Europäischen Union, Dokument 2018/0108(COD), 12. Dezember 2018, S. 37 (Art. 9 Nr. 5).

98 Art. 14 VO-Entwurf.

99 Art. 14 Nr. 2 VO-Entwurf.

100 Art. 14 Nr. 4 VO-Entwurf.

101 Das Fragmentarische des Entwurfs wird durch die Ergänzungen des Rates der Europäischen Union noch unterstrichen. Art. 7 a des Ratsdokuments sieht nun eine auf Inhaltsdaten begrenzte Notifikationspflicht des ersuchenden Mitgliedstaates vor, wenn der ersuchende Mitgliedstaat zureichende Anhaltspunkte sieht, dass sich die Person, gegen die sich das Ermittlungsverfahren richtet, nicht auf dem Territorium des ersuchenden Mitgliedstaates befindet. (Vgl. Rat der Europäischen Union, 2018/018 (COD), Art 7 a, S. 34). Im Hinblick auf Transaktionsdaten wird eine Mitwirkung des ersuchten Mitgliedstaates dann notwendig, wenn es um Beschlagnahmeverbote (Journalisten, Anwälte) geht oder es sich um Regeln handelt, die aus Gründen der Meinungs- und Pressefreiheit die strafrechtliche Verantwortung begrenzen. Diese Umstände soll der ersuchende Mitgliedstaat dann erneut in hypothetischer Prüfung in den Erlass einer Beibringungsanordnung einfließen lassen. (Rat der Europäischen Union, aaO. Art. 5 Nr. 7, S. 32). All das ist zumindest unpraktikabel, jedenfalls ein schwerwiegender Verstoß gegen das Gebot der Normenklarheit.

Recht auf Datenschutz aushöhlen. In der Reziprozität von Icloud-Act und Beibringungsanordnung wird das gerade mühsam abgesicherte Recht auf den Schutz personenbezogener Daten durch die Prämisse, der Exekutive universalen Zugriff auf verfügbare Informationen und Daten zu ermöglichen, überwölbt.[102]

D. Verformung

Über die normativen Defizite des Entwurfs hinaus, entfaltet sich dessen eigentliche Bedeutung erst im Kontext eines durch europäisches Recht determinierten Ermittlungsverfahrens. Sichtbar werden mehrere Schichten, die sich sowohl vertikal als auch horizontal überlagern und die den Ermittlungsbehörden ein flexibles Instrumentarium der Informations- und Beweiserhebung und –verwertung bieten. Ermächtigungsnormen dieses europäischen Ermittlungsverfahrens „in actio" verknüpfen diverse Akteure, Formen und Inhalte strafprozessualer Ermittlungen. Es entsteht ein **„Ermittlungs-Netzwerk"**, das je nach Bedarf die Regeln des gerade diskutierten Entwurfs, der Europäischen Ermittlungsanordnung in Strafsachen, der gemeinsamen Ermittlungsgruppen sowie die Institutionen Eurojust, Europol und künftig auch den Europäischen Staatsanwalt verbindet und gegenseitig verstärkt.

Gemeinsame Ermittlungsgruppen lassen sich im Wege von Vereinbarungen bilden, die lediglich den Zweck bestimmen müssen, aber auch – sehr variabel – bestimmen können.[103] Die Regeln, denen sie folgen, richtet sich nach den Regeln des Mitgliedstaates, in dem ihr Einsatz erfolgt.[104] Bei grenzübergreifenden Ermittlungsverfahren, aber auch bei grenzübergreifender Gefahr[105] tauschen sie Daten, Informationen und Beweise, die sie erlangt haben untereinander aus.[106] Die Europäische Ermittlungsanordnung sieht die grenzübergreifende Telekommunikationsüberwachung vor, nach Zustimmung und Prüfung des vollstreckenden Mitgliedstaates.[107] Sie umfasst Gesprächsinhalte, aber auch Verkehrs- und Standortdaten.[108] Die Praxis grenzübergreifender verdeckter Ermittlung wird durch exekutivische Vereinbarung ausgestaltet,[109] Befugnisse an Informationen über Bankkonten oder Bankgeschäfte zu gelangen und deren Überwachung anzuordnen, sind selbstverständlicher Teil grenzüberschreitender Ermittlungen.[110] Die Verordung über elektronische Beweise fügt dieser Informalisierung Beschleunigung, Privatisierung noch unilaterales Ermessen als Kennzeichen europäischen Strafverfahrens hinzu. Der Verdacht – als praktisch implementierte Legalität der Ermittlungen – wird in diesen Erwägungen nicht mehr mitgeführt, nach

102 Zurecht sehr kritisch, BR-Drucksache 215/18. S. 11 (Abs. 14).
103 Vgl. Rahmenbeschluss des Rates vom 13. Juni 2002 über gemeinsame Ermittlungsgruppen, Art. 1 Abs. 1.
104 aaO., Art. 1 Abs. 3, lit. b).
105 aaO., Art. 1 Abs. 10, lit. b) und c).
106 aaO., Art. 1 Abs. 9 und 10.
107 Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, Art. 30.
108 Richtlinie 2014/41/EU, Erwägungsgrund 30.
109 aaO. Art. 29, Abs. 4.
110 aaO, Art. 26 und 27.

den Regeln internationaler Rechtshilfe auf dessen begrenzende Funktion nur vertrauen lässt sich nicht mehr,[111] da die Regeln der Reziprozität erodieren. In einem solchen Geflecht findet die justizförmige Kontrolle der Beweisgewinnung durch Beweisverbote weder normative, also rechtliche Befugnisse des Beschuldigten verbindlich festlegende, noch praktisch handhabbare Anknüpfungspunkte, da sich die Quelle der Beweise kaum noch erschließen lässt.Für die Strafverteidigung bleibt dann nichts mehr übrig, was auch nur noch annähernd nach Waffengleichheit aussieht, vielleicht nur die Hoffnung, doch noch irgendwie politisch eine Expertenrolle im Rahmen europäischer Strafgesetzgebung spielen zu dürfen. Die Aussichten sind freilich trübe: Die Politik wird nach den Europawahlen im Mai 2019 den Weg frei machen für den unilateralen Zugriff auf elektronische Beweise. Es wird ein paar Kompromissformeln geben, die an den Prioritäten der Sicherheit, der politischen Flexibilität und der Stärkung exekutivischer Macht nichts wesentliches ändern. In diesem *transnationalen Ermittlungsnetzwerk* geht es um die Durchsetzung von Regeln, indes ohne eigene legitimatorische Substanz- ein grenzübergreifender Schutz von Rechten als Teil dieses Netzwerks gibt es nur deklaratorisch, rechtswirksam ist er nicht, soll er auch nicht sein. Über und in den Wolken ist die bürgerliche Freiheit nicht grenzenlos. Im Gegenteil.

111 Vgl. oben C II 2 (Fn 60).