Das Recht auf Anonymität finanzieller Transaktionen

Zugleich Stellungnahme zu den Vorschlägen der EU-Kommission und des Rats der EU für eine 5. Geldwäsche-Richtlinie

Stand: 27.12.2016

Thilo Weichert
Waisenhofstr. 41, D - 24103 Kiel
++ (49) 431 9719742
weichert@netzwerk-datenschutzexpertise
www.netzwerk-datenschutzexpertise.de

Inhalt

1 Einleitung

Derzeit wird vom deutschen und europäischen Gesetzgeber der Entwurf einer 5. Geldwäsche-Richtlinie erörtert. Damit sollen zwecks Bekämpfung der Geldwäsche und der Terrorismusfinanzierung anonyme Zahlungsverfahren im Internet abgeschafft und die Schwelle für anonyme elektronische Transaktionen am Point of Sale (POS) von 250 € auf 150 € abgesenkt werden. Parallel dazu werden weitere Bestrebungen verfolgt zur Verdrängung oder gar zur Abschaffung anonymer Zahlungsverfahren wie z. B. die Nutzung von Bargeld.[1]

Das vorliegende Gutachten des Netzwerks Datenschutzexpertise stellt die Pläne zur 5. Geldwäsche-Richtlinie vor, beschreibt den betroffenen verfassungsrechtlichen Rahmen, bewertet die Pläne zum Zurückdrängen anonymer Zahlungsverfahren und leitet politische Forderungen ab.

2 Entwurf 5. Geldwäsche-Richtlinie (GWRL)

Am 05.07.2016 hat die Kommission der Europäischen Union (EU) ihren Vorschlag zur Überarbeitung der 4. Geldwäscherichtlinie (4. GWRL) vorgelegt (5. Geldwäsche-Richtlinie – 5. GWRL).[2] Die Umsetzungsfrist der aktuell gültigen 4. GWRL[3] für die nationalen Gesetzgeber ist noch nicht abgelaufen und endet am 26.06.2017.[4] Mit der 5. GWRL soll die Effektivität der Geldwäschebekämpfung verbessert werden. Zur Bekämpfung des „Missbrauchs von anonymen Zahlungsinstrumenten“ ist dabei die „**Abschaffung der Anonymität** bei der Online-Nutzung aufladbarer und nicht aufladbarer Guthabenkarten und eine **Senkung der aktuellen Schwelle** von 250 EUR auf 150 EUR für anonyme Guthabenkarten, die in nicht rein elektronischen Transaktionen verwendet werden“, vorgesehen (S. 11).

Als **weitere verpflichtende Maßnahmen** für die EU-Mitgliedstaaten sind geplant die Schaffung „eines automatisierten, zentralen Mechanismus (z. B. zentrales Register oder elektronisches Datenabrufsystem), der auf Ebene der Mitgliedstaaten (…), um eine rasche Identifizierung von Kontoinhabern zu ermöglichen“, sowie eine bessere „Identifizierung der wirtschaftlichen Eigentümer von juristischen Personen und Rechtsvereinbarungen, die Speicherung dieser Informationen und den gestaffelten Zugang zu diesen“ (S. 11).

2.1 Geschichte der 5. GWRL

Die 5. GWRL geht zurück auf den Aktionsplan der Europäischen Kommission vom 02.02.2016. Darin schlug sie u. a. eine Senkung der Schwellenbeträge bei Zahlungen am physischen POS mit Prepaid-Zahlungsinstrumenten (für die keine Identitätsangabe erforderlich ist) und strengere Anforderungen an die Überprüfung der Kunden vor.[5] Sie sah sich in ihren Bestrebungen durch die t**erroristischen**

[1] Holland, „Krieg gegen Bargeld“: Datenschützer kritisieren Pläne für Obergrenze bei Barzahlung, www.heise.de 03.02.2016; Dettmer/Reiermann, Mit spitzen Fingern, Der Spiegel 8/2016, 85.
[2] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG, COM(2016)450 final; Ratsdok. 10678/16 = BR-Drs. 392/16 v. 01.08.2016; Seitenangaben im Text beziehen sich auf dieses Dokument.
[3] Richtlinie (EU) 2015/849, ABl. V. 05.06.2015, L 141/73.
[4] Art. 67 Abs. 1 4. GWRL.
[5] EU-Kommission, Kommission stellt Aktionsplan zur Intensivierung der Bekämpfung der Terrorismusfinanzierung vor, http://europa.eu/rapid/press-release_IP-16-202_de.htm.

Anschläge im März 2016 in Brüssel bestätigt. Die Terroristen sollen anonyme Prepaid-Karten für das Anmieten von Fahrzeugen und Wohnungen, verwendet haben, wobei jedoch mehrfach eine Grenze von 750 Euro überschritten wurde.[6]

Am 26.05.2016 verabschiedete das Europäische Parlament (EP) mit 542 Stimmen gegen 51 bei 11 Enthaltungen eine Entschließung, in der die EU-Kommission aufgefordert wird eine Task Force einzurichten, um **virtuelle Währungen**, wie zum Beispiel den Bitcoin, zu überwachen und zu verhindern, dass sie zur Geldwäsche, Terrorismusfinanzierung oder zum Steuerbetrug verwendet werden.[7]

Zu dem Vorschlag einer 5. GWRL nahm die Europäische Zentralbank am 12.10.2016 kritisch, aber nicht im Hinblick auf den Grundrechtsschutz, Stellung.[8] Auf seiner Sitzung am 07.11.2016 forderte der **federführende Ausschuss des EP** die Streichung der Customer-Due-Diligence-Anforderungen für Online-Zahlungen.[9]

Mit Datum vom 19.12.2016 veröffentlichte der **Rat der EU** seine Stellungnahme zum Kommissionsvorschlag.[10] Darin werden die Regelungen zum Verbot der Anonymität bei Online-Zahlungen leicht dadurch abgeschwächt, dass zunächst für 3 Jahre ein Schwellenwert von 50 € gelten soll, bevor Anonymität vollständig verboten wird (s. u. 2.5, Erwägungsgrund 11 des Rates).

Im **3. Fortschrittsbericht der EU-Kommission** zu einer wirksamen und echten Sicherheitsunion vom 21.12.2016 ist die Bekämpfung von Terrorfinanzierung und Geldwäsche der zentrale Schwerpunkt. Die Überarbeitung der 4. GWRL wird jedoch lediglich mit einem einzigen Satz erwähnt.[11]

Nunmehr steht die abschließende Stellungnahme des EP aus. Die Beschlussfassung über die 5. GWRL ist im **Trilog-Verfahren** geplant.

In **Deutschland** nahmen die zuständigen Ausschüsse des Bundesrats von dem Richtlinienvorschlag Kenntnis.[12] Der Rechtsausschuss des Bundesrats gab „ zu bedenken, dass eine nicht von der Pflicht zur Meldung eines Verdachtsfalls abhängige Auskunftspflicht für Angehörige unabhängiger rechtsberatender Berufe in einem Spannungsverhältnis zu ihrer beruflichen Schweigepflicht steht“ und bezweifelte insofern, dass der Vorschlag „dem Grundsatz der Verhältnismäßigkeit hinreichend gerecht

[6] PaySys Consultancy GmbH, 5AMLD: The end of anonymous online payments, 07.11.2016, S. 1, 5.
[7] PE EP 26.05.2016, http://www.europarl.europa.eu/news/de/news-room/20160524IPR28821/virtuelle-w%C3%A4hrungen-%C3%BCberwachen-%E2%80%93-geldw%C3%A4sche-und-terrorfinanzierung-bek%C3%A4mpfen, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0228+0+DOC+XML+V0//DE&language=DE
[8] Opinion of the European Central Bank of 12 October 2016 (CON/2016/49, https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf.
[9] PaySys Consultancy (Fn. 6), S. 6.
[10] Council of the European Union, 19 December 2016, 2016/208 (COD), http://data.consilium.europa.eu/doc/document/ST-15605-2016-INIT/en/pdf.
[11] Third progress report towards an effective and genuine Security Union v. 21.12.2016, COM(2016) 831 final, S. 9; Kirchner, Auf dem Weg zur Sicherheitsunion, SZ 22.12.2016, 6.
[12] BR-Drs. 392/16 v. 01.08.2016.

wird“. Weitergehende verfassungsrechtliche Bedenken wurden nicht vorgetragen.[13] Der Bundesrat nahm ohne weitere Stellungnahme und ohne Debatte am 23.09.2016 von dem Vorschlag Kenntnis.[14]

Mit dem Vorschlag der EU-Kommission befasst sich die Financial Matters Subgroup der Artikel 29-Arbeitsgruppe – der Zusammenschluss der **unabhängigen Datenschutzbehörden** in der EU. In der Subgroup ist auch die deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) vertreten. Von der Subgroup, der Artikel 29-Arbeitsgruppe, dem Europäischen Datenschutzbeauftragten (s. u. 2.2) und der BfDI liegen bisher keine inhaltlichen Stellungnahmen zum Vorschlag für eine 5. GWRL vor.

2.2 Kommissionsbegründung

Gemäß der Kommissionsbegründung wurden bei der Entwurfserarbeitung die in der europäischen Grundrechte-Charta (GRCh) garantierten Rechte berücksichtigt: „Folgende in der Charta verankerten **Grundrechte** haben für diesen Vorschlag besondere Bedeutung: das Recht auf Achtung des Privat- und Familienlebens (Artikel 7), das Recht auf Schutz personenbezogener Daten (Artikel 8) und das Recht auf unternehmerische Freiheit (Artikel 16 der Charta). (…) Die Rechtsvorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung verlangen von den Verpflichteten, die Identität ihrer Kunden – sowie bestimmter anderer Personen, die nicht immer ihre Kunden sind, (z. B. wirtschaftliche Eigentümer) – zu kennen und die damit verbundenen Risiken von Geldwäsche und Terrorismusfinanzierung zu bewerten. Zu diesem Zweck müssen die Verpflichteten personenbezogene Daten erheben, verarbeiten und speichern“ (S. 11).

Gemäß der Begründung wurde jeweils die Option ausgewählt, „die aus Sicht der Kosten, der Auswirkungen und der Legitimität die **meisten Vorteile** bietet“ (S. 12). Zu den Auswirkungen der Regelungen zur Abschaffung der Anonymität elektronischer Transaktionen auf das Grundrecht auf Datenschutz werden aber keine Aussagen gemacht. Vielmehr heißt es: „Die Verringerung der Anonymität im Zusammenhang mit virtuellen Währungen wird einen wichtigen Beitrag zur Steigerung des Vertrauens im guten Glauben handelnder Nutzer liefern. (…) Die strengeren Vorschriften für den Zugang zu Informationen über den wirtschaftlichen Eigentümer wurden unter dem Gesichtspunkt der Wahrung der Artikel 7 und 8 der Charta gründlich analysiert. Die vorgeschlagenen Änderungen sollen ein angemessenes Gleichgewicht zwischen dem Schutz der Privatsphäre und personenbezogener Daten einerseits und dem Bedarf an mehr Transparenz finanzieller und wirtschaftlicher Tätigkeiten andererseits gewährleisten“ (S. 13).

Bei der Vorbereitung des Richtlinienentwurfs war der **Europäische Datenschutzbeauftragte (European Data Protection Supervisor – EDPS)** im Konsultationsprozess involviert. Zu diesem Zeitpunkt stand allerdings der jetzige Vorschlag einer Nullgrenze für Internetzahlungen noch nicht zur Diskussion. Eine Stellungnahme des EDPS ist bis heute nicht öffentlich bekannt. Eingebunden waren in die Vorbereitungen gemäß der Richtlinien-Begründung auch „Verbraucherorganisationen“ (S. 9). Welche Positionen der EDPS und die Verbraucherorganisationen vertreten und wie diese berücksichtigt wurden, ist dem Entwurf nicht zu entnehmen. .[15]

[13] BR-Drs. 392/1/16 v. 12.09.2016.
[14] BR Plenarprotokoll 948, Top 66, 372 C.
[15] Ebenso Erwägungsgrund 42.

Anders als im Hinblick auf die Abschaffung anonymer Zahlungsverfahren gibt es zur Schaffung und Nutzung **automatisierter zentralisierter Mechanismen** Ausführungen zum Datenschutz: „Um die Wahrung der Privatsphäre und den Schutz personenbezogener Daten zu gewährleisten, sollten in diesen Registern jedoch nur die Mindestdaten gespeichert werden, die für die Durchführung von Ermittlungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung benötigt werden. Zudem sollten die Datensubjekte darüber informiert werden, dass ihre Daten von den zentralen Meldestellen erfasst und zugänglich gemacht werden, und sollte ihnen eine Anlaufstelle genannt werden, bei der sie ihre Rechte auf Zugang und Berichtigung der Daten ausüben können. Auf nationaler Ebene sollten maximale Aufbewahrungsfristen für die Speicherung personenbezogener Daten in den Registern festgelegt (und die Speicherungsdauer angemessen begründet) werden. Ferner sind Vorkehrungen zu treffen, um sicherzustellen, dass die Daten vernichtet werden, sobald sie zu dem genannten Zweck nicht mehr erforderlich sind. Der Zugang zu diesen Registern und Datenbanken sollte nur gewährt werden, wenn die Kenntnis der Informationen notwendig ist“.[16]

Zur **elektronischen Identifizierung** wird Folgendes ausgeführt: „Eines der Ziele der vierten Geldwäsche-Richtlinie besteht darin, Parteien (natürliche oder juristische Personen) einer Transaktion und/oder einer Zahlung zu ermitteln und zu überprüfen. Deshalb sind bei der Eröffnung eines Bankkontos oder beim Zugang zu Mitteln und/oder der Nachverfolgung elektronischer Transaktionen elektronische Identifizierung und Vertrauensdienste (d. h. zwei Aspekte, die unter die eIDAS-Verordnung fallen) von Bedeutung. Der durch die eIDAS-Verordnung geschaffene Rahmen ist derzeit einer der Eckpfeiler des digitalen Binnenmarktes, der alle Elemente der elektronischen Identifizierung und Authentifizierung erfasst“ (S. 21, 22).

2.3 Erwägungsgründe

Erwägungsgrund 7 des Richtlinienvorschlags macht Ausführungen zur Anonymität des Zahlungsverkehrs: „Die Glaubwürdigkeit virtueller Währungen wird nicht zunehmen, solange diese für kriminelle Zwecke genutzt werden. Für die Verbreitung **virtueller Währungen** und ihres potenziellen Nutzens wird die Anonymität in diesem Zusammenhang eher hinderlich als förderlich sein. Durch die Erfassung von Plattformen für den Tausch von virtuellen Währungen und von Anbietern von elektronischen Geldbörsen wird das Problem der Anonymität des virtuellen Währungstauschs allerdings nur teilweise angegangen, da ein Großteil des virtuellen Währungstausches weiterhin anonym bleiben wird, weil die Nutzer solche Transaktionen auch ohne derartige Plattformen oder Anbieter elektronischer Geldbörsen durchführen können. Zur Bekämpfung der Risiken im Zusammenhang mit der Anonymität sollten die nationalen zentralen Meldestellen für Geldwäsche-Verdachtsanzeigen die Möglichkeit haben, der Identität des Eigentümers von virtuellen Währungen virtuelle Währungsadressen zuzuordnen. Darüber hinaus sollte die Möglichkeit, den Nutzern zu erlauben, gegenüber den benannten Behörden eine Selbsterklärung auf freiwilliger Basis abzugeben, weiter ausgelotet werden.“

Zu **Guthabenkarten** heißt es in Erwägungsgrund 11: „Allgemein verwendbare Guthabenkarten haben legitime Verwendungszwecke und tragen zur finanziellen Inklusion bei. Anonyme Guthabenkarten hingegen lassen sich ohne weiteres zur Finanzierung von terroristischen Anschlägen oder zu logistischen Vorkehrungen dafür nutzen. Damit Terroristen ihre Machenschaften nicht auf diesem Wege finanzieren können, ist es daher unerlässlich, die Obergrenzen und die Höchstbeträge, unterhalb

[16] Ebenso Erwägungsgrund 16.

der die Verpflichteten bestimmte in der Richtlinie (EU) 2015/849 festgelegte Sorgfaltsmaßnahmen nicht anzuwenden brauchen, abzusenken. Anders ausgedrückt: Es ist von wesentlicher Bedeutung, die geltenden Schwellenbeträge für allgemein verwendbare anonyme Guthabenkarten zu senken und die für die Online-Nutzung geltende Befreiung von der Sorgfaltspflicht gegenüber dem Kunden abzuschaffen, gleichzeitig jedoch den Bedürfnissen der Verbraucher in Bezug auf für die allgemeine Verwendung bestimmte Zahlungsinstrumente auf Guthabenbasis Rechnung zu tragen und sicherzustellen, dass die Nutzung derartiger Zahlungsinstrumente für die Förderung der sozialen und finanziellen Inklusion nicht verhindert wird."

Erwägungsgrund 30 erklärt die **europäische Datenschutzrichtlinie** und die neue Datenschutz-Grundverordnung (DSGVO) für anwendbar: „Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, die durch die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ersetzt werden soll, regelt die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie."

2.4 Bisherige Regelung

Die Ausgangsregelung der 4. GWRL: Bisher ist dort in Art. 10 vorgesehen, dass Kredit- und Finanzinstituten das **Führen anonymer Konten und Sparbücher untersagt** wird. Art. 11 regelt, dass Sorgfaltspflichten bestehen bei a) Begründung einer Geschäftsbeziehung, b) der Ausführung von Einzel-Transaktionen ab 15.000 € sowie Transfers über „Zahlungsdienstleister"[17] ab 1.000 €, c) Bargeldtransaktionen ab 10.000 €, d) Glückspieltransaktionen ab 2.000 €, e) dem Verdacht der Geldwäsche und der Terrorismusfinanzierung sowie f) Zweifeln an der Richtigkeit zuvor erhaltener Kundenidentifikationsdaten.

Gemäß Art. 13 Abs. 1 4. GWRL gehören zu den **Sorgfaltspflichten** a) die Identitätsfeststellung der Kundenidentität auf der Grundlage von Dokumenten oder einer anderen „glaubwürdigen und unabhängigen Quelle", b) die Feststellung des wirtschaftlichen Eigentümers, c) die Hinterfragung des Geschäftszwecks und d) die kontinuierliche Überwachung der Geschäftsbeziehung.

Von den Sorgfaltspflichten kann bei **E-Geld-Kunden** gemäß Art. 12 Abs. 1 4. GWRL bei „geringem Risiko" abgesehen werden, wenn „alle nachstehenden risikominimierenden Voraussetzungen erfüllt sind": a u. b) maximaler Speicherbetrag 250 € und eine monatliche Begrenzung des Umsatzes auf 250 € (für wieder aufladbare Produkte) , c) Nutzung nur für „Kauf von Waren und Dienstleistungen", d) Aufladung darf nicht anonym möglich sein, e) Emittent kontrolliert laufend Transaktionen. Ein Rücktausch in Bargeld wird gemäß Art. 12 Abs. 2 4. GWRL auf 100 € beschränkt.

Bisher ist in Art. 40 vorgesehen, dass die in der Richtlinie Verpflichteten gemäß dem Recht der Mitgliedstaaten zu veranlassen sind, „für die Dauer von fünf Jahren nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Zeitpunkt einer gelegentlichen Transaktion" die „**Transaktionsbelege und -aufzeichnungen**" sowie die „erhaltenen Dokumente und Informationen, die für die Erfüllung der Sorgfaltspflichten gegenüber Kunden (…) erforderlich sind" aufzubewahren. Danach sind die Dokumente grds. zu löschen.

2.5 Regelungsvorschlag

Die Änderungsvorschläge der 5. GWRL sehen der Kommission vor, dass der Maximalbetrag in Art. 12 Abs. 1 für die maximale Speicherung von **E-Geld von 250 € auf 150 € abgesenkt** wird. Der Rücktausch

[17] Art. 3 Nr. 9 Verordnung (EU) 2015/847 v. 20.05.2015.

nach Art. 12 Abs. 2 in Bargeld wird auf 50 € begrenzt. Außerdem heißt es: „Die Mitgliedstaaten stellen sicher, dass die Ausnahmeregelung nach Absatz 1 keine Anwendung bei Online-Zahlung (…) findet."

Im Ratsvorschlag wird der Verweis auf **Online-Zahlungen** in Absatz 1 gestrichen. Anstelle dessen wird ein Absatz 2a mit folgendem Wortlaut eingefügt: „Die Mitgliedstaaten stellen bei Distanz-Zahlungs-Transaktionen gemäß der Definition in Punkt (6) von Artikel 4 der Richtlinie 2015/2366/EC sicher, dass bei einer 50 Euro übersteigenden Summe der Kunde identifiziert werden muss. 36 Monate nach Inkrafttreten dieser Richtlinie muss die Identifizierung auf sämtliche Distanz-Zahlungs-Transaktionen angewendet werden."[18]

In Art. 12 wird durch die EU-Kommission zudem ein Absatz 3 angefügt mit folgendem Wortlaut: „Die Mitgliedstaaten stellen sicher, dass Kreditinstitute und Finanzinstitute der Union, die als Käufer auftreten, Zahlungen mit **in Drittländern ausgestellten Guthabenkarten** nur akzeptieren, wenn diese Karten den in Artikel 13 Absatz 1 Unterabsatz 1 Buchstaben a, b und c sowie Artikel 14 genannten Anforderungen gleichwertige Anforderungen erfüllen oder davon ausgegangen werden kann, dass sie die Anforderungen nach den Absätzen 1 und 2 erfüllen." Der Ratsvorschlag ergänzt einen weiteren Satz: „Mitgliedstaaten können bestimmen, dass auf ihrem Gebiet keine anonymen Prepaid-Karten akzeptiert werden".[19]

Art. 40 soll dadurch ergänzt werden, dass sich die Dokumentationspflicht auch bezieht auf „Informationen – soweit verfügbar –, die mittels **elektronischer Mittel für die Identitätsfeststellung** gemäß der Verordnung (EU) Nr. 910/2014 eingeholt wurden".

Außerdem wird in Art. 40 neu geregelt, dass die Dokumentationspflichten auch in Bezug auf in einem neu eingeführten Art. 32a aufgeführte zentrale Mechanismen gelten sollen. Dieser Art. 32a soll folgenden Wortlaut haben:

„1. Die Mitgliedstaaten richten zentrale Mechanismen wie **zentrale Register oder zentrale elektronische Datenabrufsysteme** ein, die die zeitnahe Ermittlung aller natürlichen oder juristischen Personen ermöglichen, die bei Kreditinstituten in ihrem Hoheitsgebiet Zahlungskonten im Sinne der Richtlinie 2007/64/EG und Bankkonten innehaben oder kontrollieren. Die Mitgliedstaaten übermitteln der Kommission eine Beschreibung der Merkmale dieser nationalen Mechanismen.

2. Die Mitgliedstaaten tragen dafür Sorge, dass die Informationen, die in den in Absatz 1 genannten zentralen Mechanismen aufbewahrt werden, den zentralen Meldestellen für Geldwäsche-Verdachtsanzeigen und den zuständigen Behörden auf nationaler Ebene direkt zugänglich sind, damit diese ihren Pflichten im Rahmen dieser Richtlinie nachkommen können. Die Mitgliedstaaten stellen sicher, dass jede zentrale Meldestelle anderen zentralen Meldestellen Informationen, die in den in Absatz 1 genannten zentralen Mechanismen aufbewahrt werden, zeitnah gemäß Artikel 53 übermitteln kann.

[18] Original in Englisch: „Member States shall ensure that in case of remote payment transactions as defined in point (6) of article 4 of the Directive 2015/2366/EC, where the amount paid exceeds EUR 50 the customer has to be identified. After 36 month from the entry into force of this directive identification shall be applied to all remote payment transactions"; Quelle siehe Fn. 10.
[19] Original in Englisch: „Member States may decide not to accept on their territory payments carried out by the anonymous prepaid cards";Quelle siehe Fn. 10.

3. Es wird sichergestellt, dass die in Absatz 1 genannten zentralen Mechanismen den Zugriff auf und die Suche in folgenden Informationen ermöglichen:

- in Bezug auf den Inhaber des Kundenkontos und jede Person, die vorgibt, im Namen des Kunden zu handeln: der Name, ergänzt durch die anderen Identifizierungsdaten, die nach den nationalen Bestimmungen zur Umsetzung von Artikel 13 Absatz 1 Buchstabe a vorgeschrieben sind, oder eine individuelle Kennnummer,

- in Bezug auf den wirtschaftlichen Eigentümer des Inhabers des Kundenkontos: der Name, ergänzt durch die anderen Identifizierungsdaten, die nach den nationalen Bestimmungen zur Umsetzung von Artikel 13 Absatz 1 Buchstabe b vorgeschrieben sind, oder eine individuelle Kennnummer;

- in Bezug auf das Bank- oder Zahlungskonto: die IBAN-Nummer und das Datum der Kontoeröffnung und -schließung."

Im Ratsvorschlag wird in Art. 32a noch ein Absatz 3a eingefügt mit folgendem Wortlaut: „Mitgliedstaaten können für zentrale Meldestellen und zuständige Behörden für deren Aufgabenerfüllung gemäß dieser Richtlinie den Zugang zu und die Suche von weiteren wichtigen Informationen über die zentralisierten Mechanismen einfordern."[20]

Im Ratsvorschlag zu Art. 40 ist die Einführung eines Unterabsatzes bzgl. der Aufbewahrungsfristen (bisher 5 Jahre) vorgesehen: „Die Aufbewahrungsperiode gemäß diesem Absatz einschließlich der weiteren Aufbewahrungsperiode, die 5 weitere Jahre nicht überschreitet, ist auch in Bezug auf Daten anwendbar, die über zentralisierte Mechanismen gemäß Artikel 32a zugänglich sind."[21]

3 Grundrechtlicher Prüfungsmaßstab

Der Entwurf der 5. GWRL enthält Überwachungs- und Kontrollmaßnahmen, die Relevanz für den Grundrechtsschutz und insbesondere für den Datenschutz haben. Im Folgenden erfolgt keine umfassende verfassungsrechtliche Bewertung. Vielmehr beschränkt sich diese auf den Plan der Aufhebung bzw. **Zurückdrängung der Anonymität** im Zahlungsverkehr.

3.1 Grundrecht auf Datenschutz

Der vorgeschlagene Wegfall anonymer Bezahlmöglichkeiten berührt das in Art. 8 Abs. 1 Europäische Grundrechte-Charta (GRCh) garantierte **Grundrecht auf Datenschutz**, das inhaltlich identisch ist mit dem vom deutschen Bundesverfassungsgericht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) abgeleitete Grundrecht auf informationelle Selbstbestimmung: „Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten".

[20] Original in Englisch: „Member States may consider requiring other information deemed essential for FIUs and competent authorities for fulfilling their obligation under this Directive to be accessible and searchable through centralized mechanisms"; Quelle in Fn. 10.
[21] Original in Englisch: „The retention period referred to in this paragraph, including the further retention period that shall not exceed five additional years, shall also apply in respect of the data accessible through the centralised mechanisms referred to in Article 32a"; Quelle in Fn. 10.

3.2 Telekommunikationsgeheimnis

Betroffen wird zudem das in Art. 7 GRCh garantierte Recht auf Schutz von Privatsphäre und Kommunikation, das inhaltlich das in Art. 10 GG garantierte **Telekommunikationsgeheimnis** mit umfasst. Bei der Kontrolle von Online-Finanztransaktionen erfolgt zugleich auch eine Überwachung des Telekommunikationsverkehrs und zwar sowohl im Hinblick auf die Umstände wie auch die Inhalte.[22]

3.3 Eigentumsschutz

Der Umgang mit Geld als vermögenswertes Recht wird in Art. 14 Abs. 1 Grundgesetz (GG) und in Art. 17 Abs. 1 Europäische Grundrechte-Charta (GRCh) geschützt, wonach der **Schutz des Eigentums** gewährleistet wird bzw. jeder Mensch das Recht hat, sein rechtmäßig erworbenes Eigentum zu nutzen und darüber zu verfügen. Inhalt und Schranken werden durch die Gesetze bestimmt. Gemäß der GRCh kann die Nutzung des Eigentums gesetzlich geregelt werden, soweit dies für das Wohl der Allgemeinheit erforderlich ist. Der Allgemeinwohlvorbehalt ist auch in Art. 14 Abs. 2 GG normiert: „Eigentum verpflichtet. Sein Gebrauch soll zugleich dem Wohl der Allgemeinheit dienen“.

Bisher wurde der verfassungsrechtliche Eigentumsschutz vorrangig unter den Aspekten des Substanzerhalts und der Verfügungsmacht gesehen. Eine Feststellung des Bundesverfassungsgerichts (BVerfG) zu Grundrechten generell gilt aber auch für das Eigentumsrecht. Danach schützen Grundrechte auch die Entscheidungsfreiheit über deren Nutzung, also hier des Eigentums, vor Beobachtung. Eine solche **informationelle Kontrolle** kann die Nutzung des Eigentums hemmen. Wer unsicher ist, welche Informationen über die Eigentumsnutzung durch wen für welche Zwecke erfolgt, kann in seiner selbstbestimmten Nutzung der Eigentumsfreiheit beschränkt werden. Insofern gibt es eine inhaltliche Überschneidung des Grundrechts auf Eigentum und des Grundrechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.[23]

Es ist erstaunlich, dass die Dokumente zur 5. GWRL Art. 17 GRCh überhaupt nicht erwähnen. Vielmehr nehmen diese neben den oben erwähnten Art. 7 und 8 GRCh lediglich Bezug auf Art. 16 GRCh, der die „**unternehmerische Freiheit**“ wie folgt gewährleistet: „Die unternehmerische Freiheit wird nach dem Unionsrecht und den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten anerkannt“ (Erwägungsgrund 40). Diese Formulierung ist gegenüber dem strengen Schutz des Eigentumsschutzes nach Art. 17 GRCh erheblich offener. Es hat den Anschein, dass Art. 17 GRCh, der alle Menschen und nicht nur die Unternehmerschaft regelt, vom europäischen Gesetzgeber vollständig übersehen wurde.

3.4 Gemeinsame Grundrechtserwägungen

Das BVerfG hat im Hinblick auf die anlasslose Vorratsdatenspeicherung von Telekommunikationsdaten (TK-Daten) Folgendes ausgeführt: „Allerdings handelt es sich bei einer solchen Speicherung um einen **besonders schweren Eingriff mit einer Streubreite**, wie sie die Rechtsordnung bisher nicht kennt. Erfasst werden (…) Daten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation: Die Speicherung

[22] BVerfG U. v. 02.03.2010, 1 BvR 256/08 u. a., NJW 2010, 833, insbes. Rn. 188 ff.; Jarass, Charta der Grundrechte der Europäischen Union, 2010, Art. 7 Rn. 43; EuGH U. v. 08.04.2014, C-23/12 u. C-594/12, Rn. 25, DVBl 2014, 708; EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 101.
[23] BVerfG NJW 1984, 422; zu weiteren digitalen Erscheinungsformen des Eigentumsschutzes Hoffmann/Luch/‘Schulz/Borchers, Die digitale Dimension der Grundrechte, 2015, S. 203 ff.

bezieht sich dabei auf Alltagshandeln, das im Alltagsleben elementar und für die Teilnahme am sozialen Leben in der modernen Welt unverzichtbar ist“.[24] Diese Aussage in Bezug auf TK-Daten lässt sich auf Daten aus Finanztransaktionen, egal ob diese online oder offline erfolgen, vollständig übertragen.

Das BVerfG hat neben der individualrechtlichen auch die gesellschaftliche Funktion des informationellen Grundrechtsschutzes betont: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über ihn weiß.“ Informationelle Selbstbestimmung ist „eine elementare **Funktionsbedingung eines** auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten **freiheitlichen demokratischen Gemeinwesens**“.[25] Diese Aussage gilt für die Inanspruchnahme aller, nicht nur der politischen Grundrechte und insbesondere auch für im Zahlungsverkehr ausgeübte wirtschaftliche Betätigungsfreiheit. Dies wurde vom BVerfG mit seiner Feststellung akzentuiert, dass es „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland“ gehört, in der persönlichen Freiheitswahrnehmung nicht total erfasst und registriert zu werden.[26]

Die Bewertung des BVerfG wird im Hinblick auf die europäischen Grundrechte vom Europäischen Gerichtshof (EuGH)[27] voll geteilt. Eine allgemeine und unterschiedslose Vorratsspeicherung kann mit dem Argument der Kriminalitätsbekämpfung nicht gerechtfertigt werden, insbesondere wenn keine Differenzierungen, Einschränkungen oder Ausnahmen in Hinblick auf das verfolgte Ziel, die betroffenen Personen, die elektronischen Kommunikationsdienste, den geografischen Raum, den Zeitraum und Berufsgeheimnisse gemacht werden.[28] Die Regelung zu derartigen Vorratsspeicherungen überschreitet die Grenzen „des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden.[29]

Unsere freie wirtschaftliche Betätigung darf nicht total erfasst und registriert werden. Gemäß dem deutschen wie europäischen Verfassungsrecht ist die **Anonymität des Zahlungsverkehrs** der geforderte Urzustand, der nur nach besonderer Rechtfertigung und nur soweit erforderlich verlassen werden darf.

3.5 Zahlungsverkehr als Grundrechtsbetätigung

Die **Nutzung von Eigentum** erfolgt in großem Umfang über Zahlungsverkehr. Dieser wird zunehmend elektronisch durchgeführt und hinterlässt dabei digitale Spuren. Durch den Wechsel vom anonymen und weitgehend spurenlosen Zahlungsverkehr mit analogem Bargeld zum elektronischen Zahlen (electronic Cash, ePayment) gewinnt der Datenschutz in diesem Bereich eine zunehmende gesellschaftliche Relevanz: Wer was wann bei welcher Gelegenheit kauft bzw. verkauft, wird beim Online-Shopping, aber schon seit längerem im Versandhandel sowie über Bonuskarten und Kundenbindungssysteme erfasst, kontrolliert und verwertet. Die Kontrolle und Überwachung unseres

[24] BVerfG NJW 2010, 838, Rn. 210.
[25] BVerfG NJW 1984, 422.
[26] BVerfG, NJW 2010, 839, Rn. 218.
[27] EuGH, U. v. 08.04.2014, C-293/12, C-594/12, Rn. 38 ff., NVwZ 2014, 709 ff. – Vorratsdatenspeicherung I; EuGH U. v. 06.10.2016, C-362/14, Rn. 91 ff., NJW 2015, 3151 ff. – Safe Harbor; EuGH U. v. 21.12.2016, C-203/15 u. C-698/15 – Vorratsdatenspeicherung II.
[28] EuGH U. v. 08.04.2014, C-23/12 u. C-594/12, Rn. 51-60, DVBl 2014, 711; EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 103-106.
[29] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 107.

Konsums ist die eine Seite der informationellen Beschränkung unserer marktwirtschaftlichen Freiheit. Die andere Seite ist die Erfassung und Registrierung, wer was wann wofür und bei welcher Gelegenheit bezahlt.

3.5.1 Bedeutungsverlust des Bargeldverkehrs

Angesichts moderner forensischer Techniken wird die Anonymität des Zahlungsverkehrs, die seit Jahrhunderten durch das **Bargeld** gewährleistet wird, zunehmend brüchig. Mit Fingerabdrücken ist es seit Jahrzehnten nachträglich möglich festzustellen, wer eine Münze oder einen Geldschein in der Hand hatte. Heute bestehen zudem chemische und biotechnische Methoden zur Identifizierung von Personen, die Bargeld in der Hand hatten. Doch bleiben diese sehr aufwändigen Erkenntnismöglichkeiten eingeschränkt. Sie lassen sich durch Handschuhe oder durch Geldwäsche – im Wortsinn – vermeiden oder zumindest einschränken. Zudem ist die Angabe, dass jemand Bargeld in der Hand hatte, weniger aussagekräftig als die Information, wer was wann zu welchem Preis bezahlt hat.

3.5.2 Fortschritte bei elektronischen Zahlungsverfahren

Mit der Digitalisierung werden der Austausch analogen, relativ anonymen Geldes in immer mehr Lebensbereichen zur Ausnahme und das elektronische Zahlen zum Regelfall. Bei der Zahlung mit Geld-, Giro- oder Kreditkarte, Lastschrift oder Überweisung, Online-Payment (ePayment) oder unter Nutzung eines sog. FinTech wird die anonymisierende Funktion von Bargeld aufgehoben.

Der Siegeszug elektronischer Zahlungsverfahren hat zunächst technisch-ökonomische Gründe: Bei den in unserer globalisierten Gesellschaft zunehmenden **Distanzgeschäfte** sind direkte Bargeldzahlungen zumeist praktisch nicht möglich.

Aber auch bei einem **direkten Kontakt der Vertragspartner**, also bei der Zahlung am „Point of Sale“, gewinnen elektronische Zahlungsverfahren immer mehr an Bedeutung. Der Umgang mit elektronischen Buchungen ist weniger aufwändig, arbeitsintensiv und damit höhere Kosten verursachend als das Sammeln, Zahlen, Zählen und Wechseln von Münzen und Scheinen. Für viele Waren und Dienstleistungen werden diese als Gegenleistung gar nicht mehr angenommen, etwa in manchen Hotels oder beim Mieten eines Autos. Das Wechseln von Bargeld wird in Banken oder Geschäften immer öfter verweigert. Mit Geld funktionierende Automaten werden weniger, sind oft defekt und ein beliebtes Angriffsziel von Kriminellen.

3.5.3 Besonderheiten von Finanztransaktionsdaten

Mit guten Gründen haben sowohl das Bundesverfassungsgericht wie auch der Europäische Gerichtshof die ausnahmslose und anlasslose Speicherung und Nutzung von Telekommunikations- (TK-) Daten auf Vorrat mit der Intention einer eventuellen Verwendung für Sicherheitszwecke für grundrechtswidrig erklärt (s. o. 3.4). Während es für eine mittel- oder längerfristige Speicherung von TK-Daten keine originäre Legitimation gibt[30], ist die praktische und rechtliche **Rechtfertigung der längeren Speicherung** von ePayment-Daten durch Finanzdienstleister einfacher. Sie können darauf verweisen, dass sie im Reklamationsfall mittel- und teilweise sogar langfristig gegenüber den Kunden nachweispflichtig sind. Im Hinblick auf gewerbliche Finanztransaktionen und diese begründende

[30] Siehe aber EuGH U. v. 19.10.2016, C-582/14.

Geschäftsbriefe bestehen aus handels- und steuerrechtlichen Gründen Speicherpflichten von sechs oder gar zehn Jahren (§ 147 AO; § 257 HGB).[31]

Finanztransaktions-Daten haben regelmäßig eine höhere **Aussagekraft** als TK-Verkehrsdaten. Bei finanzrelevanten Online-Aktionen gibt es große inhaltliche Überschneidungen zwischen diesen Datenarten. Doch erlauben Informationen dazu, wer wann bei welcher Gelegenheit wie viel für welchen Zweck an wen bezahlt hat, noch tiefere Einblicke in die Persönlichkeit der Betroffenen. Sie geben Auskunft über die Inhalte von Beziehungen und deren ökonomischen Bewertung.

Dies gilt in besonderem Maße für **sensitive Vorgänge**: Spenden für politische, karitative oder religiöse Zwecke, Zahlungen für sexuelle Dienstleistungen[32], die kostenpflichtige Inanspruchnahme psychologischer, medizinischer oder sozialer Hilfe, das Entgelt für ungesunden Konsum – in all diesen Fällen lassen sich weitgehende Rückschlüsse auf eine Persönlichkeit ziehen.

Unabhängig von jeder Sensibilität im Einzelfall gibt es zudem kaum etwas Aussagekräftigeres über die Persönlichkeit eines Menschen als die **Gesamtheit seiner Zahlungsdaten**. In unserer Wirtschaftsordnung ist fast nichts umsonst. Der Alltag des Menschen wird geprägt von seinen Finanztransaktionen. Diese sind für den Homo Oekonomicus identitätsbestimmend.

4 Staatliche Begehrlichkeit an digitalen Transaktionsdaten

Schon 2011 warnten die **Datenschutzbeauftragten des Bundes und der Länder** vor einem Gesetzentwurf der Bundesregierung zur Geldwäschebekämpfung, der eine Identifizierungspflicht von allen denjenigen vorsah, die auch nur kleine Summen von elektronischem Geld erwerben.[33] Seitdem haben die hoheitlichen Begehrlichkeiten an digital verfügbaren oder verfügbar zu machenden Finanztransaktionsdaten zugenommen. Diese sind für vielerlei staatliche Zwecke nützlich, weshalb viele sich dafür engagieren, Formen des anonymen Zahlens, sei es per Bargeld oder durch anonymisierte elektronische Zahlungsverfahren, zurückzudrängen:

Im Vordergrund steht die **Strafverfolgung**. So meinte Prof. Peter Bofinger, einer der fünf sogenannten Wirtschaftsweisen, Mitglied des Sachverständigenrats der Bundesregierung, Bargeld sei ein Anachronismus, nicht nur wegen der dadurch stattfindenden Medienbrüche, sondern auch zum Austrocknen der Märkte für Schwarzarbeit und Drogen.[34] Zur Bekämpfung des illegalen Online-Glücksspiels war im Glücksspielstaatsvertrag ein sog. Financial Blocking vorgesehen, das an den elektronischen Zahlungsdaten anknüpfte.[35] Die Überwachung internationaler Finanztransaktionen über den Finanzdienstleister Society for Worldwide Interbank Financial Telecommunication (SWIFT) durch US-Behörden im Rahmen des „Terrorist Finance Tracking Program“ steht seit 2006 in der öffentlichen

[31] Weichert, Datenschutz bei FinTechs, Compliance-Berater (CB) 2016, 113 f.
[32] Graff, Die Entblößung der Welt, SZ 22.09.2015, 11; Schirrmacher, Nach Ashley-Madison-Hack: Erbeutete Daten veröffentlicht, www.heise.de 19.08.2015.
[33] DSB-Konferenz, Anonymes elektronisches Bezahlen muss möglich bleiben, Entschließung vom 28./29.09.2011.
[34] „Bargeld ist ein Anachronismus“, Der Spiegel 21/2015, 56.
[35] ULD, Datenschutzrechtliche Bewertung der Regelungen zum „Financial Blocking“ zur Verhinderung illegalen Glücksspiels im Internet, https://www.datenschutzzentrum.de/artikel/860-.html.

Diskussion.[36] Ein großangelegter Angriff auf SWIFT durch Cyber-Kriminelle 2016 zeigte, wie anfällig derartige Transaktionssysteme sein können.[37]

Es ist interessant, dass die politische Legitimation für die Abschaffung der Anonymität von digitalen Zahlungen bisher ausschließlich mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung erfolgt. Tatsächlich hat eine Speicherpflicht von digitalen Finanztransaktionen zur Folge, dass die gespeicherten Daten auch für **Zwecke der Steuererhebung** und der Kontrolle der Steuerpflicht genutzt werden können. Tatsächlich werden bestehende Mechanismen zur Finanztransaktionskontrolle wie z. B. der bestehende Kontodatenabruf nicht nur für Zwecke der Bekämpfung schwerer Straftaten verwendet, sondern weitgehend auch für Zwecke der Sicherung der Steuereinnahmen und der „steuerlichen Belastungsgleichheit“, die das BVerfG immer wieder als Rechtfertigung für informationelle Eingriffe anerkannt hat.[38] Das Ausblenden des Nutzens der Vorratsspeicherung von Finanztransaktionsdaten für steuerliche Zwecke könnte zum Hintergrund haben, dass damit die Betroffenheit der gesamten Bevölkerung aus dem Blick gerät, die sich von Maßnahmen gegen Geldwäsche und Terrorismusfinanzierung nicht betroffen wähnt.

Eine weitere Funktion einer identifizierenden Überwachung von Finanztransaktionen kann die finanz- und wirtschaftspolitische **Kontrolle des Finanzverkehrs** sein.[39]

5 Privatwirtschaftliche Begehrlichkeiten an Finanztransaktionsdaten

Die digitalen Spuren elektronischer Zahlverfahren sind auch für die Privatwirtschaft von größtem Interesse. Eine hoheitliche Verpflichtung zur Erhebung und Aufbewahrung von elektronischen Transaktionsdaten hat zwangsläufig den Wunsch zur Folge, diese Daten auch für eigene Zwecke zu nutzen. Die Praxis der **Erfassung, Speicherung und Auswertung von elektronischen Zahlvorgängen** ist bisher wenig durchleuchtet und noch weniger öffentlich diskutiert.

Anbieter elektronischer Zahlverfahren begründen die von Ihnen praktizierte **Intransparenz** gern mit ihren Verschwiegenheitspflichten – insbesondere mit dem Schutz von Betriebs- und Geschäftsgeheimnissen sowie mit ihrem Vertraulichkeitsversprechen gegenüber ihren Kunden. Letzteres erfolgt in Einzelfällen sogar gegenüber den Kunden selbst, wenn diese mehr Transparenz in Bezug auf die Verarbeitung ihrer Daten einfordern. Finanz-Transaktionsdaten können für Bonitätsbewertungen genutzt werden, die bei der Kreditvergabe, aber zunehmend auch bei sonstigen wirtschaftlichen Betätigungen eine für Betroffene oft existenzielle Rolle spielen. Eine unzureichende Kontrolle der Betroffenen hierüber kann zur Folge haben, dass sie die Eigenkontrolle über ihr gesamtes Leben verlieren.[40]

[36] Weichert in Müller-Heidelberg u. a., Grundrechte-Report 2007, S. 46 ff.; ders. in Müller-Heidelberg u. a., Grundrechte-Report 2010, 35 ff.
[37] Tandriverdi/Zydra, Ins Herz getroffen, SZ 27.04.2016, 17.
[38] BVerfG B. v. 13.06.2016, 1 BvR 1550/03 u. a., Rn. 128 – Kontostammdatenabfrage, NJW2007, 2469.
[39] Vgl. Seith, Blind in die Blase, Der Spiegel 45/2016, 86.
[40] Zur Intransparenz bei der Bonitätskontrolle Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, S. 41 ff.

Finanzdienstleistern ist bewusst, dass die von ihnen verarbeiteten Transaktionsdaten für die Kunden von höchster Sensibilität sind und dass diese Vertraulichkeit erwarten. Dies hat zur Folge, dass derartige Daten auf dem freien Markt nur eingeschränkt verfügbar sind. Die **Vertraulichkeitserwartung ihrer Kunden** hält die Unternehmen aber oft nicht davon ab, umfassende interne Auswertungen vorzunehmen und die Ergebnisse kommerziell zu nutzen.

Payment-Dienstleister hatten selbst in Deutschland schon damit begonnen, die Daten für **Marketingzwecke** zu verwenden.[41] Dass Big Data-Analysen durch US-amerikanische ePayment-Anbieter stattfinden, ist bekannt, auch wenn Details hierüber nur selten öffentlich werden.

Derartige Bestrebungen reichen inzwischen bis in den Bereich der als seriös angesehenen großen **Banken und Versicherungen** hinein. Diese suchen nach zusätzlichen Geschäftsmodellen mit ihren Daten, nachdem wegen der Niedrigzinsen, der globalen Konkurrenz, auch von Online-Anbietern, und wegen des Fehlens freier Marktsegmente im klassischen Finanzgeschäften nur noch beschränkte Verdienstmöglichkeiten bestehen. Es gibt derzeit kaum einen Finanzdienstleister, der sich nicht Gedanken darüber macht, die personalen Transaktionsdaten für andere kommerzielle Zwecke zu nutzen.[42]

Besonders einschneidend ist es, wenn die Angaben über Finanztransaktionen mit sonstigen Daten, etwa aus sog. sozialen Netzwerken, kombiniert und mit **Big Data-Methoden ausgewertet** werden. Für Anbieter wie Google, Amazon oder Facebook, die eigene Internetzahlungsangebote auf dem Markt etabliert haben, ergeben sich hierdurch völlig neue lukrative Geschäftsmodelle.[43]

Diese Angebote werden den Kunden als für sie vorteilhaft beworben. „Guten Kunden“ werden Vorteile versprochen. Ob diese tatsächlich vorteilhaft sind, ist für die Kunden oft nicht nachvollziehbar. Mit einem individuell möglicherweise gewährten Vorteil korrespondiert in jedem Fall die Benachteiligung der anderen. Hierdurch kann sich eine **Marktdiskriminierung** für bestimmte Gruppen von Personen ergeben, die bestimmte finanzrelevante Merkmale aufweisen oder nicht aufweisen. Personalisierte Angebote können nicht nur dazu führen, dass transaktionsschwache Menschen ausgeschlossen und diskriminiert werden, sondern auch, dass von transaktionsstarken Kunden hohe Preise gefordert werden, da sie ja ohnehin nicht so genau auf den Preis schauen.

Auf der Strecke bleibt zudem die **Transparenz** der Datenverarbeitungen wie des Marktes generell. Den Marktbeteiligten ist regelmäßig nicht bekannt, ob, und weshalb, d. h. wegen welcher Merkmale, jemand bevorzugt oder benachteiligt wird. Kunden, Verbraucher- und Datenschützer, die im Wettbewerb stehende Konkurrenz, ja selbst die Finanzaufsichtsbehörden haben bisher keinen Einblick in die Formen der Auswertung von Daten, die einmal erfasst worden sind.

[41] Eichler/Weichert, EC-Kartennutzung, elektronisches Lastschriftverfahren und Datenschutz, DuD 2011, 201 ff.
[42] Fromme, Suche nach Datenhoheit, SZ 10.06.2014, 26; Hesse/Mahler Interview mit Bäte, „Wir brauchen Waffengleichheit“, Der Spiegel 3/2016, 74 ff.; zur Rechtslage Weichert CB 2016, 112 f.
[43] Glaser, Der blaue Planet, SZ 30./31.01.2016, 13 ff.

6 Verhältnismäßigkeitsprüfung der 5. Geldwäsche-Richtlinie

Grundrechtseingriffe sind nur zulässig, wenn sie verhältnismäßig sind, d. h. wenn sie zur Erreichung eines legitimen gesetzlichen Ziels geeignet, erforderlich und angemessen sind.[44] Eine derartige **explizite Prüfung** lässt der Entwurf für eine 5. GWRL nicht erkennen.

Zwar werden relevante (nicht alle) Grundrechte benannt. Im Meinungsbildungsprozess scheinen auch relevante Stakeholder wie der Europäische **Datenschutzbeauftragte und Verbraucherorganisationen** befragt worden zu sein. Welche Position diese zu dem Vorschlag bezogen haben, ist nicht bekannt. Das Bezahlen mit Prepaid-Karten sowie das elektronische Bezahlen im Internet hat direkte Verbraucherrelevanz. Das Zurückdrängen der Anonymität im Zahlungsverkehr beeinträchtigt den Verbraucherschutz. Dieser findet in Art 38 GRCh seine ausdrückliche Gewährleistung.

Die Regelung, deren Begründung sowie die Erwägungsgründe lassen nicht erkennen, dass eine Verhältnismäßigkeitsprüfung mit einer dabei erforderlichen **Abwägung** tatsächlich durchgeführt wurde, welche Aspekte erörtert und wie diese gewichtet wurden. Vielmehr werden begründungsfrei die vorgeschlagenen Maßnahmen als erforderlich und grundrechtskompatibel dargestellt.

6.1 Geeignetheit

Die Bekämpfung der Terrorismusfinanzierung und die Verhinderung von Geldwäsche sind legitime Aufgaben. Es ist nicht zu bestreiten, dass elektronische Zahlungsmittel zur Terrorismusfinanzierung und zur Geldwäsche genutzt werden. Insofern ist eine **grundsätzliche Geeignetheit** verstärkter Identifizierungspflichten anzunehmen. Jedes Identifizierungsmittel ist grds. geeignet, Straftaten aufzuklären, wenn der identifizierte Vorgang mit diesen in einem Zusammenhang stehen.

Eine **Spezifizierung der Geeignetheit** der Identifizierungspflicht bei elektronischen Zahlungen wird in der Begründung zur 5. GWRL nicht vorgenommen. Es ist zu unterscheiden zwischen einer Eignung zur Abwehr von terroristischen Anschlägen und zur Erleichterung einer späteren Aufklärung. Auch ist von Bedeutung, ob die Identifikation direkt auf eine Tat, oder lediglich auf dessen Umfeld bezogen wird. Insofern kann festgestellt werden, dass eine personale Zuordnung von elektronischer Zahlungen allenfalls eine nachträgliche Ermittlung und wohl kaum die Prävention erleichtert. Die Finanzierung spielt sich regelmäßig im Vorfeld von Terrorismus oder sonstigen Kapitaldelikten ab, anders als dies bei weniger schwerwiegenden Delikten, etwa Betrug, Unterschlagung oder auch Geldwäsche, der Fall ist. Die Jahresberichte der Financial Intelligence Unit (FIU) des Bundeskriminalamtes (BKA) stellen fest, dass sich seit Einführung strenger Betragslimits in Deutschland im Jahr 2011 Verdachtsmeldungen im Bereich elektronischer Zahlungssysteme auf einem niedrigen Niveau bewegen. Die britische Regierung bescheinigte in ihrer nationalen Risikobewertung vom Oktober 2015 E-Geld-Produkten nur ein geringes Risiko, zum Zweck der Terrorismusfinanzierung missbraucht zu werden.[45]

Der Erwägungsgrund 7 zur 5. GWRL weist zurecht darauf hin, dass die Anonymität **virtueller Währungen** wie z. B. Bitcoin oder anderer Blockchainverfahren durch die vorgeschlagenen

[44] BVerfG NJW 1984, 419 ff.; EuGH U. v. 21.12.2016, C-203/15 u. C-698/15 Rn. 94-96.
[45] PVD, Positionspapier des Prepaid Verbands Deutschland zur Überarbeitung der Geldwäscherichtlinie, Stand August 2016, http://www.prepaidverband.de/news/positionspapier-zur-ueberarbeitung-der-geldwaescherichtlinie/ S. 2.

Maßnahmen nicht erfasst wird.[46] Es ist nahe liegend, dass solche Verfahren zur Terrorismusfinanzierung und Geldwäsche genutzt werden. Es werden keine Ausführungen dazu gemacht, welche Erkenntnisse über die (potenzielle) Nutzung virtueller Währungen bestehen. So kann auch nicht beurteilt werden, inwieweit bei einer Verschärfung der Identifizierungspflichten Terrorismusfinanzierer und Geldwäscher auf diese Verfahren umsteigen werden. Sollte dies der Fall sein, so ist keine Geeignetheit gegeben. Dass dies der Fall ist, ist zu vermuten, da diese Verfahren bei professionellen Kriminellen, um die es sich hier weitgehend handelt, inzwischen etabliert sind.

Das parallel zum Bankensystem verbreitete **Hawala-Transfersystem** von Finanztransaktionen über vertrauenswürdige Mittelsmänner[47] entzieht sich ebenso der Kontrolle durch Aufsichtsbehörden.

Hinterfragt werden muss zudem, ob eine **Erfassung im Bagatellbereich**, also z. B. bei Transaktionen bis zu 250 € wirklich einen Beitrag zur Bekämpfung von Geldwäsche und Terrorismus leisten kann. Es gibt keinen Hinweis, dass die vollständige Abschaffung der Anonymität beim Online-Kauf von Waren und Dienstleistungen für die Bekämpfung von Geldwäsche und Terrorismus eine Wirkung haben kann. Insofern liegen keine Erkenntnisse vor. Es ist äußerst unwahrscheinlich, dass eine solche Erfassung auch nur einen kleinen Beitrag für Ermittlungen in diesem Bereich leisten wird. In diesem Bereich dürften regelmäßig größere Beträge umgesetzt werden. Hinzu kommt, dass im Bagatellbereich weiterhin die Nutzung von Bargeld problemlos möglich ist. Würde also bekannt, dass elektronische Zahlungen identifizierbar sind, so können und werden Kriminelle und insbesondere Terroristen auf die Bargeld-Nutzung oder auf illegale elektronische Angebote ausweichen.

6.2 Erforderlichkeit

Die Änderung der Geldwäscheregelungen wird zu einem Zeitpunkt vorgeschlagen, zu dem die 4. GWRL **noch nicht in nationales Recht umgesetzt** ist und angewendet wird. So konnten mit den dort vorgesehenen Maßnahmen keine Erfahrungen gemacht werden, auch im Hinblick auf verschärfte Identifizierungspflichten. Art. 12 Abs. 1 GWRL sieht bisher vor, dass Mitgliedstaaten in Fällen, in denen erwiesenermaßen ein geringes Risiko besteht, beim Ergreifen strikter risikominimierender Maßnahmen E-Geld von der Pflicht zur Feststellung und Überprüfung der Identität von Vertragspartnern und wirtschaftlichen Eigentümern freigestellt werden können. Derartige risikominimierende Rahmenbedingungen sind, wenn E-Geld-Produkte ausschließlich zum Erwerb von Waren und Dienstleistungen verwendet werden und nur ein geringer Betrag identifizierungsfrei zugelassen wird. Die Erforderlichkeit der Reduzierung dieses Betrags von 250 auf 150 € ist willkürlich und nicht nachvollziehbar. Die Erforderlichkeit ist insofern ebenso wenig dargelegt wie die der Beseitigung jeglichen Schwellenwertes bei Online-Käufen.

Geringer eingreifende Maßnahmen wurden nicht erprobt, geschweige denn evaluiert und mit der geplanten Abschaffung anonymer Zahlung verglichen. Eine Erforderlichkeit der Maßnahmen ist nicht gegeben.

[46] Allerdings führt die 5. GWRL in Art. 3 UnterAbs. 18 den Begriff der „virtuellen Währungen“ ein und verpflichtet nach Art. 47 Abs. 1 die Anbieter von Umtauschmöglichkeiten von virtueller in „echte“ Währungen zur Zulassung und Eintragung und zum Know Your Customer, also zur Kundenidentifizierung (vgl. Begründung S. 8 u. Erwägungsgründe 6, 7).
[47] Vgl.: die Erläuterungen des Hawala-Finanzsystems bei Wikipedia, https://de.wikipedia.org/wiki/Hawala.

6.3 Angemessenheit

Derzeit ist in § 13 Abs. 6 S. 1 **Telemediengesetz** (TMG) geregelt, dass die „Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen (ist), soweit dies technisch möglich und zumutbar“ ist. Diese Norm müsste, wenn die 5. GWRL in Kraft träte, zumindest in Bezug auf entgeltliche Medien, aufgehoben werden.

Die Regelung im TMG basiert auf der Erkenntnis, dass die Inanspruchnahme von digitalen Dienstleistungen, die einen immer größeren Raum im Wirtschaftsleben gewinnen, in jedem Fall Vertrauen und Vertraulichkeit zu den Dienstleistern voraussetzt. Ein derartiges Vertrauen ist angesichts der Anonymität der meisten Dienstleister oft nur begrenzt herzustellen. Umso wichtiger ist es, dass es für die Kunden die Möglichkeit gibt, anonym zu bleiben. Mit der 5. GWRL wäre diese Möglichkeit nicht mehr gegeben, was für Online-Dienstleistungen und den Online-Handel zu einer Vertrauenskrise führen kann. Insofern ist die geplante Regelung **wirtschaftsfeindlich**. Mit der Überregulierung in diesem Bereich würde zudem ein Innovationshemmnis für elektronische Zahlungssysteme entstehen, das insbesondere europäische Entwickler betrifft und Systemen aus Drittländern, insbesondere aus den USA, einen Wettbewerbsvorteil verschaffen würde.

Es ist den **Akzeptanzstellen** elektronischer Zahlungen nicht zuzumuten, im vorgesehenen Maße ihre Kunden zu überprüfen und zu kontrollieren. Um sicherzugehen, dass von außerhalb der EU stammende Zahlungsmittel den Anforderungen genügen, müssten die Akzeptanzstellen entweder eine umfangreiche Prüfung im Einzelfall vornehmen oder die Zahlungsannahme zu verweigern. Eine solche Prüfung ist faktisch überhaupt nicht möglich. Die Verweigerung von Zahlungsmitteln von außerhalb der EU wäre nicht zumutbar.

Die Maßnahmen mit dem Ziel der Bekämpfung von Geldwäsche und der Finanzierung von Terrorismus stehen in keinem angemessenen Verhältnis zu der Einschränkung informationeller Selbstbestimmung für die gesamte Bevölkerung. Je massiver der Eingriff in das Recht auf anonyme Transaktion ist, desto höhere Anforderungen sind an dessen Zulässigkeit zu stellen. Die 5. GWRL benennt keine solche Anforderungen. Sie trifft mit ihrer Streuwirkung zu fast hundert Prozent Personen, die keine Veranlassung für ihre Erfassung gegeben haben. Betroffen werden dadurch nicht nur den Regelungsinhalt der Grundrechte von Art. 7, 8 u. 17 GRCh, sondern auch deren **Wesensgehalt**.[48]

Um den Erfordernissen der Grundrechte zu genügen, muss eine „Regelung **klare und präzise Regeln über die Tragweite und Anwendung** einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendig beschränkt wird.“[49] Beschränkungen können im Hinblick auf die Bekämpfung schwerer Straftaten, hinsichtlich der Datenkategorien, der erfassten (Kommunikations-)Mittel, der

[48] EuGH U. v. 06.10.2015, C-362/14, Rn. 94, NJW 2015, 3157; dazu Bock/Engeler DVBl 2016, 593 ff.
[49] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 109 mit Verweis auf EuGH U. v. 08.04.2014, C-23/12 u. C-594/12, Rn. 54.

betroffenen Personen und der vorgesehenen Daten der Vorratsspeicherung vorgenommen werden. Die materiellen Voraussetzungen der Vorratsspeicherung müssen „objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen“, die sich zudem als „in der Praxis geeignet“ erweisen.[50]

Diesen Anforderungen genügt die 5. GWRL nicht. Eine undifferenzierte Speicherfrist von 5 Jahren und evtl. gemäß nationalen Regelungen von länger (Art. 40, Erwägungsgrund 16 des Ratsentwurfs) geht weit über das „absolut Notwendige“ hinaus. Die Voraussetzungen für den behördlichen Zugriff auf die Vorratsdaten sind nicht definiert und **in keiner Weise eingeschränkt**.[51] Es fehlt an „einer vorherigen Kontrolle entweder durch ein Gericht oder einer unabhängige Verwaltungsstelle“.[52] Ja selbst die Nutzung der Vorratsdaten durch die Zahlungsdienstleister wird nicht begrenzt, geschweige denn verboten.[53] Eine Benachrichtigung der Betroffenen bei einem Zugriff auf die Vorratsdaten und angemessene Vorkehrungen zur technischen und organisatorischen Sicherheit fehlen.[54] Damit wird das grundrechtlich Gebotene weit unterschritten.

Es ist zu vermuten, dass geplant ist, für das in Art. 32a 5. GWRL vorgesehene „zentrale elektronische Datenabrufsystem“ das 2003 eingeführte **Kontoabrufverfahren**, das vom Bundeszentralamt für Steuern durchgeführt wird, verwendet wird. Hierüber könnte eine Echtzeitkontrolle praktisch aller elektronischer Zahlverfahren vorgenommen werden. Das Kontoabrufverfahren wurde ursprünglich zu engen Zwecken der Terrorismusbekämpfung eingeführt und danach immer weiter – insbesondere in den Bereichen des Steuer- und des Sozialrechts – ausgeweitet. Es ist zu erwarten, dass eine Einbeziehung in das Verfahren nach der 5. GWRL dieses auf privaten Unternehmens- (Bank-)Daten basierende System, das derzeit schon verfassungsrechtlichen Bedenken unterliegt, weiter zur Kontrolle der gesamten Bevölkerung ausgebaut wird.[55]

In der Geldwäsche-Richtlinie werden die zum Informationserhalt und zur Informationsauswertung berechtigten Behörden, die im Englischen „**Financial Intelligence Unit**“ (FIU) genannt werden, mit „zentrale Meldestellen für Geldwäsche-Verdachtsanzeigen“ (so z. B. Erwägungsgründe 7, 13) bezeichnet. Während bei dem englischen Begriff – realistischerweise – die Assoziation zu Geheim- und Nachrichtendiensten naheliegt, erinnert der deutsche Begriff eher an Meldebehörden, die relativ wenig sensitive Daten sammeln und evtl. weitergeben, nicht aber umfassend auswerten und nutzen und eigenständig ermitteln, so wie dies vorgesehen ist (Erwägungsgründe 13 ff.; Art. 32 ff. GWRL). Ebenso unverdächtig ist der weitere verwendete Begriff der auch mit den Transaktionsdaten versorgten „anderen zuständigen Behörden“ (z. B. Erwägungsgrund 15)

Die Begründung für die Richtlinie nimmt Bezug auf die europäische **Datenschutz-Grundverordnung**. Wesentliche der in der DSGVO fixierten Prinzipien werden durch die 5. GWRL ignoriert: So wird in Art. 5 Abs. 1 DSGVO verlangt, dass die personenbezogene Datenverarbeitung „nach Treu und Glauben und

[50] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 108, 110.
[51] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 118; EuGH U. v. 08.04.2014, C-23/12 u. C-594/12, Rn. 61.
[52] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 120 mit Verweis auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte; EuGH U. v. 08.04.2014, C-23/12 u. C-594/12, Rn. 62.
[53] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 117.
[54] EuGH U. v. 21.12.2016, C-203/15 u. C-698/15, Rn. 121, 122.
[55] Dazu BVerfG U. v. 13.06.2007, 1 BvR 1550/03 u. a., NJW 2007, 2464; zu u. a. Entwicklung, Rechtsgrundlagen, Nutzung https://de.wikipedia.org/wiki/Kontenabruf.

in einer für die betroffene Person nachvollziehbaren Weise“ erfolgt (lit. a). Die Zweckänderung der Transaktionsdaten ist in keiner Weise eingeschränkt und führt dadurch nicht nur zu einer Verletzung der vorgegebenen Zweckbindung (lit. b), sondern ist mit dem ursprünglichen Zweck nicht vereinbar (vgl. Art. 6 Abs. 4 DSGVO). Die Prinzipien der Datenminimierung und der Speicherbegrenzung werden missachtet (lit. c, e). Spezifische Maßnahmen zur Sicherstellung der Integrität und Vertraulichkeit (lit. f) und zur Sicherung der Verantwortlichkeit (Art. 6 Abs. 2 DSGVO) sind in der 5. GWRL nicht getroffen.[56]

7 Schlussfolgerungen

Eine Überprüfung der 5. GWRL ergibt, dass die darin vorgesehene Senkung des Schwellenwertes zulässiger Prepaidverfahren und das Ende der Anonymität bei Online-Zahlungen mittels E-Geld gegen die verfassungsrechtlichen Vorgaben des deutschen Grundgesetzes und der Europäischen Grundrechte-Charta verstößt. Auf diese Regelungen **muss ersatzlos verzichtet werden**. Eine Überarbeitung der 4. GWRL ist erst dann angebracht, nachdem diese in Kraft gesetzt wurde und sich hierbei Änderungsbedarf erwiesen hat.

Die **Diskussion** über die Identifizierungspflicht bei Telekommunikation und Zahlungsverkehr hat begonnen. Sie wird nicht nur innerhalb Deutschlands und der EU geführt. Der Europäische Gerichtshof für Menschenrechte hat eine Beschwerde gegen ein deutsches Gesetz aus dem Jahr 2004 zugelassen, das die Registrierungspflicht der Anschlussinhaber von SIM-Karten vorsieht. Prüfungsmaßstab ist das Grundrecht auf Achtung des Privatlebens gemäß Art. 8 der Europäischen Menschenrechtskonvention, die über die EU hinaus Gültigkeit hat.[57]

Anstelle vage Behauptungen zugrunde zu legen, wonach Identifizierungspflichten wirksame Instrumente gegen Terrorismus und Geldwäsche seien, müssen auf Fakten und empirischen **wissenschaftlichen Untersuchungen** basierende Feststellungen gemacht werden, welchen Beitrag diese Pflichten leisten können. In einem weiteren Schritt bedarf es einer öffentlichen politischen Diskussion, welche Eingriffe in das Recht auf Anonymität im Zahlungsverkehr zugelassen werden sollen. Hierbei muss die grundrechtliche Dimension und der Umstand, dass die gesamte Bevölkerung betroffen sein kann, berücksichtigt werden.

Parallel zu der Diskussion über die Identifizierungspflicht im Bereich des elektronischen Zahlens wird über die **Abschaffung des Bargeldes** und dessen vollständige Ersetzung durch elektronische Zahlungsverfahren diskutiert. Ein derartiger Schritt wäre verfassungsrechtlich nicht akzeptabel. Neben weiteren Gründen würde mit der Abschaffung des Bargeldes die zuverlässigste Form des anonymen Zahlens abgeschafft und damit das Recht auf Anonymität des Zahlungsverkehrs unverhältnismäßig eingeschränkt. Bargeld muss als Zahlungsmittel erhalten bleiben.

Angesichts der schon heute teilweise bestehenden faktischen Alternativlosigkeit elektronischer Zahlverfahren in vielen Bereichen muss zudem darüber nachgedacht werden, für welche existenziellen

[56] Ähnlich, auch in Bezug auf die JI-Richtlinie Schaar, Kurzgutachten zum Vorschlag der Europäischen Kommission für die Überarbeitung der Vierten EU-Geldwäscherichtlinie (RL 2015/849) aus datenschutzrechtlicher Sicht, 05.09.2016 = https://www.eaid-berlin.de/?p=1317.
[57] Beuth, Anonymität wird zum Fall für den Menschenrechtsgerichtshof, www.zeit.de 08.06.2016; Kurz, Wir haben euch alle im Blick, FAZ 05.09.2016.

Zahlungsvorgänge eine **gesetzliche Pflicht zur Annahme von Bargeld** oder zumindest von anonymen Zahlungsformen zu normieren ist, auch wenn Bargeld in vielen Lebenssituationen, etwa bei Distanzgeschäften, kein geeignetes Zahlungsmittel ist.

Zwar lässt sich absolute Anonymität elektronisch nicht realisieren. Zum Zweck der Abwicklung einer elektronischen Transaktion bedarf es immer einer elektronischen Spur und deren korrekter Zuordnung. Doch die personale Verbindung zu einer konkreten Person lässt sich technisch kappen. Der Intermediär kann die Funktion eines Anonymisierungsdienstes übernehmen. Seit Jahrzehnten sind nicht-personalisierte **Prepaid-Karten**, bei denen die ausgebenden Stellen eine solche Funktion im Markt wahrnehmen.

Ein anderer Ansatz sind **Blockchain-Zahlungsverfahren** wie z. B. Bitcoin oder vergleichbare Angebote. Dabei werden elektronische Zahlungen nicht über einen Dienstleister vorgenommen, sondern direkt durch Versenden von Datenpaketen zwischen Absender und Empfänger, die gegenüber allen anderen Interessierten anonym bleiben. Ob solche vom hoheitlich regulierten Zahlungsverkehr losgelösten Verfahren sich durchsetzen werden und dürfen, hängt von vielen Voraussetzungen ab, deren Eintritt noch nicht prognostiziert werden kann – von der Stabilität dieser digitalen Zahlungsform, der Anwendungsfreundlichkeit und letztlich der Akzeptanz durch Markt und Gesetzgeber.

Der Schutz unserer Grundrechte verbietet es, dass solchen Produkten die rechtliche Grundlage entzogen wird. Es ist die Pflicht der Gesellschaft, des Staates generell und des Gesetzgebers speziell, die faktischen und rechtlichen Voraussetzungen für **anonymes elektronisches Bezahlen** zu wahren. Dies gilt sicher nicht für Großtransaktionen im fünf- und mehrstelligen Eurobereich. Diese sind möglicherweise von hoher gesellschaftlicher Relevanz, so dass hieran ein öffentliches Interesse bestehen kann. Wohl gilt dies aber für die Alltagsgeschäfte und insbesondere für den Verbraucherbereich, wo heute immer mehr Menschen, die keinerlei Anlass für eine Überwachung geben, auf elektronischem Wege zahlen. Die persönlichkeitsrechtliche Aussagekraft der darüber generierten Daten wie auch die damit verbundenen Manipulations- und Diskriminierungsrisiken sind gewaltig, ohne dass hier staatliche Sicherheitsanliegen überwiegen, geschweige denn legitime private Auswertungsinteressen. Es ist Aufgabe des Staates, die demokratische Gesellschaft vor Geld- und Machtmissbrauch durch die „großen Fische“ zu schützen; es darf nicht seine Aufgabe sein, den „kleinen Mann“ einer Totalkontrolle zu unterwerfen.

Es sind **intelligente und sichere elektronische Lösungen** gefordert, mit denen die Anonymität vollständig oder zumindest weitgehend gewahrt bleibt. Statt normativ die Anonymität von elektronischen Zahlverfahren auszuschließen, sollten derartige Lösungen weiter erforscht, entwickelt und eingeführt werden.

Die Digitalisierung des Zahlungsverkehrs auf den letzten Metern, also im Bereich der Alltagsgeschäfte, steht gerade vor dem Durchbruch. Es ist eine politische Aufgabe – zur Verteidigung unserer Grundfreiheiten – hierbei dessen **Anonymität zu wahren**.

Abkürzungen

ABl.	Amtsblatt
Abs.	Absatz
AO	Abgabenordnung
Art.	Artikel
BR	Bundesrat
BR-Drs.	Bundesrats-Drucksache
BVerfG	Bundesverfassungsgericht
CB	Compliance-Berater (Zeitschrift)
ders.	derselbe
d. h.	das heißt
DSGVO	Europäische Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl	Deutsches Verwaltungsblatt (Zeitschrift)
eIDAS	Verordnung über elektronische Identifizierung und Vertrauensdienste
EG	Europäische Gemeinschaften
EP	Europäisches Parlament
EU	Europäische Union
EuGH	Europäischer Gerichtshof
eXX	electronic XX
FAZ	Frankfurter Allgemeine Zeitung
ff.	fortfolgende
Fn.	Fußnote
GG	Grundgesetz
GRCh	Europäische Grundrechte-Charta
GWRL	Geldwäsche-Richtlinie
HGB	Handelsgesetzbuch
i. V. m.	In Verbindung mit
lit.	Buchstabe
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
PE	Presseerklärung
POS	Point of Sale (Ort des Verkaufs)
PVD	Prepaid Verband Deutschlands
Rn.	Randnummer
S.	Seite od. Satz
SZ	Süddeutsche Zeitung
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TK	Telekommunikation(s)
Top	Tageordnungspunkt
U.	Urteil
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
v.	von
vgl.	vergleiche
z. B.	zum Beispiel