

Duygu Damar-Blanken | Hanne Roggemann | Sally Peters | Jana Lenze | Daniel Daneshian Sherbaf

# Digital Abgehängt

Barrieren im Zahlungsverkehr überwinden

12. Februar 2025

**Im Auftrag von:**

Bundesverband der Verbraucherzentralen und Verbraucherverbände –  
Verbraucherzentrale Bundesverband e.V.  
Rudi-Dutschke-Straße 17, 10969 Berlin

**Name des Teams**

T +49 30 25800-0  
[finanzmarkt@vzbv.de](mailto:finanzmarkt@vzbv.de)  
[vzbv.de](http://vzbv.de)

**Stand:**

Februar, 2025

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

# Inhalt

<b>Zusammenfassung .....</b>	<b>4</b>
<b>Summary .....</b>	<b>7</b>
<b>I. Einleitung .....</b>	<b>10</b>
<b>II. Hintergrund .....</b>	<b>13</b>
1. Das Zahlungsverhalten in Deutschland .....	13
2. Übersicht über die aktuelle und künftige Regulierung .....	17
2.1 Bargeld .....	17
2.2 Zahlungsdienste .....	18
2.3 Basiskonto .....	20
2.4 Digitaler Euro .....	20
2.5 Barrierefreiheit .....	21
2.6 Betrug und Betrugsprävention .....	22
2.7 Datenschutz .....	23
2.8 Prävention von Geldwäsche und Terrorismusfinanzierung .....	24
<b>III. Zugang und Nutzbarkeit im Zahlungsverkehr .....</b>	<b>25</b>
1. Steigende Notwendigkeit einer Teilnahme am digitalen Zahlungsverkehr .....	25
1.1 Einschränkungen im Zugang zu Bargeld bei Banken .....	25
1.2 Beschränkungen im Einzelhandel .....	27
2. Barrieren des Zugangs und der Nutzung des digitalen Zahlungsverkehrs .....	29
2.1 Praktische Barrieren .....	29
2.2 Mangelnde Kompetenz .....	31
2.3 Fehlende Bereitschaft .....	33
2.4 <b>Regulatorische Barrieren</b> .....	43
3. Zwischenfazit .....	45
<b>IV. Implikationen für die Stärkung der Teilhabe am Zahlungsverkehr .....</b>	<b>46</b>
1. Abbau von praktischen Barrieren .....	47
1.1 Infrastrukturelle Barrieren abbauen .....	47
1.2 Akzeptanz von Bargeld: Nutzungsmöglichkeiten erhöhen .....	52
1.3 Kosten für Verbraucher:innen gering halten .....	53
2. Umgang mit fehlender Kompetenz .....	55
2.1 Finanzielle und digitale Kompetenzen aufbauen .....	55
2.2 Unterstützungsmöglichkeiten: Kompetenzen verbessern und Kapazitäten aufbauen .....	56
3. Fehlende Bereitschaft adressieren .....	59
3.1 Anonymität bzw. Schutz der Privatsphäre ermöglichen .....	59
3.2 Vertrauen stärken durch Betrugsprävention .....	60

3.3 Mangelnde Bereitschaft durch Anbieter adressieren.....	73
4. Regulatorische Barrieren.....	74
5. Ein Blick in die Zukunft: Digitaler Euro für alle Verbrauchergruppen .....	75
<b>V. Fazit .....</b>	<b>77</b>
<b>VI. LITERATURVERZEICHNIS .....</b>	<b>79</b>

# Zusammenfassung

Der Zahlungsverkehr bildet das Fundament für den Austausch von Gütern, Dienstleistungen und finanziellen Verpflichtungen. Die Teilhabe am Zahlungsverkehr kann als Teil der Daseinsvorsorge angesehen werden und sollte für alle Menschen zugänglich sein.

Barrieren für Verbraucher:innen führen dazu, dass bestimmte Personengruppen ohne Unterstützung vom Zahlungsverkehr ausgeschlossen sind und an der fortschreitenden Entwicklung neuer Bezahlmethoden nicht teilhaben können. Barrieren zum digitalen Zahlungsverkehr können sowohl auf der Ebene der Zahlungsdienstleister, der gesetzlichen Regulierung, aber auch auf Seiten der Verbraucher:innen existieren. Die Barrieren können durch die vier verschiedenen Kategorien zusammengefasst werden.

1. **Praktische Barrieren** umfassen eine mangelnde technische Ausstattung auf Seiten der Verbraucher:innen sowie Kosten, die mit der Teilnahme am digitalen Zahlungsverkehr einhergehen.
2. Bei der Barriere der **mangelnden Kompetenz** geht es um eine mangelnde finanzielle und digitale Kompetenz auf Seiten der Verbraucher:innen, aber auch um die mangelnde Kompetenz auf Seiten der Zahlungsdienstleister, eine gruppenorientierte Unterstützung der Verbraucher:innen beim Zugang zu und bei der Nutzung von Zahlungsdiensten zu leisten.
3. Die dritte Barriere umfasst die **fehlende Bereitschaft** sowohl auf Seiten der Verbraucher:innen, die „neuen“ Technologien misstrauen, als auch auf Seiten der Anbieter, die vorhandene Regulierungen nicht umsetzen.
4. **Regulatorische Barrieren** liegen vor, wenn die Regulierung selbst den Zugang zum Zahlungsverkehr behindert.



Zahlungsdienste ermöglichen es den Verbraucher:innen, am Wirtschaftsverkehr teilzunehmen und ihre wirtschaftlichen Pläne zu verwirklichen. Zahlungsdienste müssen somit ohne Hürden und kostengünstig nutzbar sein und dies, ohne die Privatsphäre zu verletzen. Allerdings sind in dieser Hinsicht weder Bargeld noch digitale Zahlungsmethoden perfekt. Das vorliegende Gutachten setzt sich mit unterschiedlichen Barrieren beim Zugang und bei der Nutzung von Zahlungsdiensten auseinander, analysiert die aktuelle und künftige Rechtslage auch anhand der vorliegenden EU-Vorschläge und arbeitet Lösungsansätze aus.

Bei der Bearbeitung der Barrieren für den Zugang und die Nutzung digitaler Zahlungsdienste muss als Alternative zu digitalen Zahlungsmitteln auch der Zugang zu Bargeld berücksichtigt werden. Die Teilnahme am Zahlungsverkehr sollte als Teil der Daseinsvorsorge auch in einer marktwirtschaftlich geprägten Gesellschaft, die auf Abschlussfreiheit basiert, staatlich sichergestellt werden. Insbesondere sollte den Verbraucher:innen ein Portfolio an Alternativen für die Begleichung ihrer finanziellen Verpflichtungen barrierefrei zur Verfügung gestellt werden. In diesem Portfolio sollte auch Bargeld weiterhin einen Platz einnehmen. Nicht ohne Grund wird den Verbraucher:innen von öffentlichen Stellen empfohlen, einen Bargeldvorrat zu halten, denn was alle digitale Zahlungsmethoden eint, ist die unbedingte Abhängigkeit von Strom. Zudem haben längst nicht alle Verbraucher:innen Zugang zum Internet, oder wollen dieses nicht nutzen. Es wird also nicht möglich sein, alle Verbraucher:innen in das digitale Zahlungssystem zu inkludieren. Aus diesem Grund beziehen die im Folgenden vorgestellten Implikationen zum Abbau der Barrieren den Zugang und die Nutzung von Bargeld mit ein.

Das Gutachten arbeitet verschiedene Implikationen zum Umgang mit den oben zusammengefassten Barrieren heraus. Diese sind zum Teil bereits in den EU-Vorschlägen verankert. Im Gutachten wird detailliert dargestellt, inwiefern diese Vorschläge ergänzt bzw. bereichert werden können, um den Schutz der Verbraucher:innen im Zahlungsverkehr zu stärken, aber eben auch, um weitere Barrieren für den Zugang zu und die Nutzung von digitalen Zahlungsdiensten abzubauen. Die wichtigsten Implikationen zur Bearbeitung der identifizierten Kategorien von Barrieren werden im Folgenden dargestellt.

Praktische Barrieren:

1. Zugang zum Bargeld sichern: Banken sollten mittels konkreter Vorgaben dazu verpflichtet werden, über ihre Filialstruktur, Banking Hubs, Geldautomaten oder Bargeldlieferungen ihre Kund:innen mit Bargeld auszustatten und über diese Zugangsmöglichkeiten zu kommunizieren.
2. Rückgang von Bargeldakzeptanz entgegenwirken: Die Akzeptanz von Bargeld als gesetzliches Zahlungsmittel stärken, indem die Akzeptanzpflicht europäisch gesetzlich klargestellt, Ausnahmen zur Akzeptanzpflicht stark eingeschränkt und kostengünstiges Bargeldhandling ermöglicht wird.
3. Einfache Technologien verwenden und alternative Mittel anbieten: Bezahlssysteme müssen schnellstmöglich barrierefrei gestaltet sein, damit sie niedrigschwellig genutzt werden können und auch für physisch bzw. psychisch eingeschränkte Menschen zugänglich sind. Zudem braucht es bei der Umsetzung der Regelung zur starken Kundenauthentifizierung die Bereitstellung von mehreren alternativen Mitteln, um die Autorisierung von Zahlungsaufträgen tatsächlich barrierefrei und für alle Verbrauchergruppen zugänglich zu gestalten.
4. Kostenbarrieren abbauen: Hierfür müssen Gebühren für Basiskonten deutlich gesenkt werden, die Kosten für Bargeldabhebungen durch die Banken getragen werden sowie die Kosten für eine barrierefreie Nutzung des digitalen Zahlungsverkehrs bei der Höhe der Sozialleistungen angemessen berücksichtigt werden.

Barriere der mangelnden Kompetenz:

1. Aufbau finanzieller und digitaler Kompetenz: Da der Zahlungsverkehr immer mehr digital stattfindet, muss digitale Kompetenz als Teil der finanziellen Kompetenz gefördert werden.
2. Unterstützungsmöglichkeiten verbessern: Um Zugangsbarrieren in Bezug auf fehlende Kompetenz auf Verbraucherseite zu beheben, bedarf es persönlicher Unterstützung des digitalen Zahlungsverkehrs von Seiten der Anbieter. Neben der Kapazitätsfrage ist

der Zugang zur Unterstützung auch eine Frage der Kompetenzen der Bankmitarbeiter:innen. Entsprechend sollten Banken ihre Mitarbeiter:innen zielgruppenorientiert sensibilisieren, beispielsweise indem die Schulungspflicht im Zahlungsverkehr um die Kundenorientierung erweitert wird.

Barriere der fehlenden Bereitschaft:

1. Anonymität bzw. den Schutz der Privatsphäre ermöglichen: Die Verarbeitung personenbezogener Daten im Rahmen der digitalen Zahlungsdienste sollte auf das Notwendigste beschränkt werden.
2. Vertrauen in die Digitalisierung stärken durch Betrugsprävention, indem
  - a. zur Unterstützung von informierten Entscheidungen der Verbraucher:innen statistische Informationen zu den Betrugsfällen und zum Verhalten der Bank bezüglich der Erstattungsansprüche von Verbraucher:innen offengelegt werden.
  - b. die Empfängerüberprüfung ohne Verzichtsmöglichkeit gestaltet wird.
  - c. die konkreten Maßnahmen in Verbindung mit Transaktionsüberwachungsmechanismen, wie etwa der Blockierung des Zahlungsauftrags oder der Sperrung des Zahlungsinstruments, verpflichtend gestaltet werden.
  - d. ein Widerrufsrecht für die Zahlungsaufträge eingeführt wird.
  - e. ein einfach anwendbares, unkompliziertes und verbraucherfreundlicheres Haftungsregime für Betrugsfälle gestaltet wird.
3. Mangelnde Bereitschaft auf Seiten der Anbieter adressieren: Um Umgehungsstrategien bestehender Regulierung durch Anbieter zu vermeiden, sollte die Zahlungsdiensteaufsicht gestärkt werden und die Regulierung klar und eindeutig formuliert sein.

Regulatorische Barrieren:

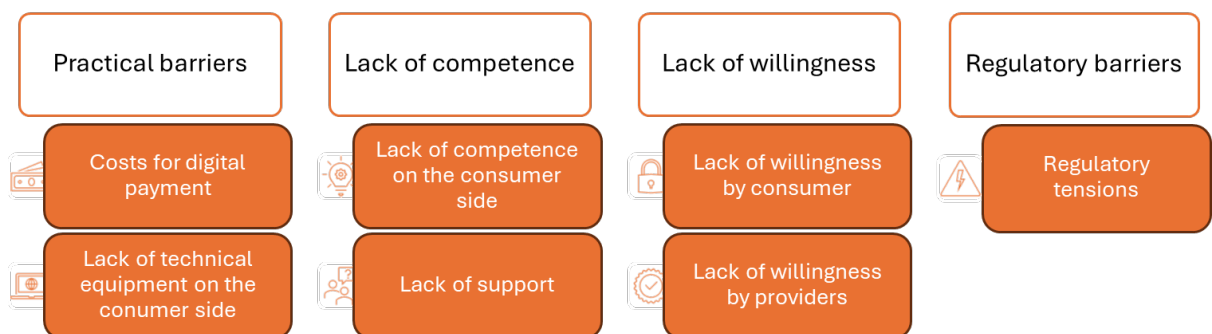
1. Regulatorische Spannungsverhältnisse auflösen: Gesetzgebungsverfahren und Gesetzesevaluierung sollten unintendierte Exklusionseffekte für vulnerable Verbrauchergruppen stärker in den Fokus nehmen. So sollte bei der Anwendung des Geldwäschegesetzes die Expertise von Vertretungsorganisationen eingeholt werden.

# Summary

The payment system forms the foundation for the exchange of goods, services, and financial obligations. Participation in the payment system can be considered part of essential public services and should be accessible to all individuals.

Barriers for consumers result in certain groups being excluded from the payment system if they lack support, preventing them from participating in the ongoing development of new payment methods. Barriers to digital payment systems can exist at the level of payment service providers, legal regulations, or on the consumer side and can be categorized into four distinct groups:

1. **Practical barriers** include a lack of technical equipment on the part of consumers as well as costs associated with participating in digital payment systems.
2. **Competency barriers** pertain to a lack of financial and digital literacy among consumers, as well as insufficient competency on the part of payment service providers to offer group-specific support to consumers in accessing and using payment services.
3. **Willingness barriers** affect both consumers, who distrust “new” technologies, and providers, who do not implement existing regulations.
4. **Regulatory barriers** arise when regulations themselves hinder access to the payment system.



Payment services enable consumers to participate in the economy and manage their economic plans. Therefore, payment services must be easily accessible and affordable without compromising privacy. However, neither cash nor digital payment methods are perfect in this regard. This report examines various barriers to accessing and using payment services, analyzes the current and future legal framework, including existing EU proposals, and develops solutions.

When addressing barriers to accessing and using digital payment services, access to cash must also be considered as an alternative to digital payment methods. Participation in the payment system should be guaranteed by the state as part of essential public services, even in a market-driven society based on the principle of freedom of contract.

Consumers, in particular, should be provided with a portfolio of barrier-free alternatives for meeting their financial obligations, in which cash should continue to play a role. Public authorities recommend that consumers keep a cash reserve for a reason—what all digital payment methods have in common is their absolute dependence on electricity. Moreover, not all consumers have access to the internet or wish to use it. As a result, it will not be possible to include all consumers in the digital payment system. For this reason, the

implications presented below for reducing barriers also take into account access to and the use of cash.

This report identifies various implications for addressing the summarized barriers, some of which are already incorporated into EU proposals. The report provides a detailed analysis of how these proposals can be supplemented or enhanced to strengthen consumer protection in payments while also further reducing barriers to accessing and using digital payment services. The key implications for addressing the identified categories of barriers are outlined in the following sections.

#### Practical Barriers:

1. Ensuring access to cash: Banks should be required to provide cash through their branch networks, banking hubs, ATMs, or cash delivery services and communicate these access points clearly.
2. Counteracting the decline of cash acceptance: Strengthening the acceptance of cash as legal tender by legally clarifying the obligation to accept cash payment at the European level, significantly restricting exceptions to this obligation, and enabling cost-effective cash handling.
3. Using simple technologies and offering alternatives: Payment systems must be designed to be fully accessible so that they can be used easily by all, including individuals with physical or mental disabilities. Additionally, strong customer authentication regulations should include multiple alternative methods to ensure truly barrier-free access for all consumer groups.
4. Reducing cost barriers: Basic account fees should be significantly lowered, banks should cover cash withdrawal costs, and the costs of accessible digital payment options should be adequately considered in social benefit calculations.

#### Competency Barriers:

1. Improving financial and digital literacy: As payments become increasingly digital, digital literacy must be promoted as a fundamental part of financial literacy.
2. Enhancing support options: To overcome access barriers related to a lack of consumer competence, digital payment services must include personal support options from providers. In addition to capacity considerations, access to support is also a matter of employee competence. Banks should train their staff to provide targeted support for different consumer groups, for example, by expanding mandatory training requirements to include customer-oriented service in payments.

#### Willingness Barriers:

1. Ensuring anonymity and privacy protection: The processing of personal data in digital payments should be limited to what is strictly necessary.
2. Strengthen trust through fraud prevention, by:
  - a. disclosing statistical information on fraud cases and the bank's behavior regarding consumers' refund claims to support consumers' informed decisions.
  - b. designing the recipient verification without the possibility of waiver.
  - c. making the specific measures in connection with transaction monitoring mechanisms, such as the blocking of the payment order or the blocking of the payment instrument, mandatory.
  - d. introducing a right of revocation for payment orders.
  - e. designing an easily applicable, uncomplicated and consumer-friendly liability regime for cases of fraud.

3. Addressing the lack of willingness among providers: To prevent service providers from circumventing existing regulations, payment service supervision should be strengthened, and regulations must be clearly and unambiguously formulated.

Regulatory Barriers:

4. Resolving regulatory conflicts: Legislative procedures and the evaluation of legislation should focus more on unintended exclusionary effects for vulnerable consumer groups. For example, the expertise of representative organizations should be sought when applying the Money Laundering Act.

# I. Einleitung

Der Zahlungsverkehr in Deutschland bildet das Fundament für den Austausch von Gütern, Dienstleistungen und finanziellen Verpflichtungen. Ob im täglichen Einkauf, bei Online-Transaktionen oder im internationalen Handel – effiziente und sichere Zahlungsmethoden sind entscheidend für das reibungslose Funktionieren von Geschäfts- und Privatleben. Dabei spielen Banken, Fintech-Unternehmen und Regulierungsbehörden eine zentrale Rolle dabei, die Bedürfnisse von Verbraucher:innen und Unternehmen gleichermaßen zu erfüllen. Deutschland verfügt grundsätzlich über ein modernes Zahlungssystem, das sowohl traditionelle Bargeldzahlungen als auch innovative digitale Zahlungsdienste umfasst; zugleich gibt es in verschiedenen Bereichen Herausforderungen, die es Verbraucher:innen erschweren, am Zahlungsverkehr teilzunehmen.

Die Teilhabe am Zahlungsverkehr kann als Teil der Daseinsvorsorge angesehen werden. Eine Definition zu dem verwandten Thema des Basisbedarfes bei Finanzdienstleistungen liefert ein entsprechendes Gutachten des *iff*:

„Ein Basisbedarf an Finanzdienstleistungen ist ein solcher Bedarf, ohne dessen Deckung erhebliche Nachteile für Verbraucher:innen oder die Gesellschaft bereits sichtbar – oder zu erwarten sind. Solche Nachteile können beispielsweise Armut, soziale Ausgrenzung, Überschuldung oder sonstige erhebliche Beeinträchtigungen sein.“<sup>1</sup>

Dass dies auch für den Zahlungsverkehr zutrifft, ist in der Begründung für die Verpflichtung, ein Pfändungsschutzkonto<sup>2</sup> zur Verfügung zu stellen, zu finden. „Der bargeldlose Zahlungsverkehr hat für die Teilnahme am modernen Wirtschaftsleben eine besondere Bedeutung.“<sup>3</sup>

- Als Daseinsvorsorge sollte die Teilhabe am Zahlungsverkehr für alle Personen gewährleistet sein. Die finanzielle Inklusion stellt sicher, dass Finanzdienstleistungen für Verbraucher:innen und Unternehmen zugänglich sind, eine hohe Produkt- und Servicequalität verbrieft und einfach genutzt werden können. Darin eingeschlossen sind auch gefährdete Gemeinschaften, einschließlich einkommensschwacher Gruppen.

Dabei ist die Förderung von finanzieller Inklusion nicht nur eine soziale Verantwortung, sondern auch ein Mittel, um wirtschaftliches Wachstum und soziale Stabilität zu fördern. Die Studie The Global Findex Database<sup>4</sup> zeigt zum Beispiel, dass ein höherer Anteil an Menschen mit Zugang zu Bankkonten und anderen Finanzdienstleistungen die wirtschaftliche Teilhabe fördert und gleichzeitig die Nutzung

---

<sup>1</sup> Knobloch u. a. (19.11.2012), S. 46.

<sup>2</sup> Ein Pfändungsschutzkonto (P-Konto) ist ein spezielles Girokonto, das in Deutschland eingerichtet werden kann, um die/den Kontoinhaber:in vor einer Kontopfändungen zu schützen. Es ermöglicht, dass im Falle einer Pfändung ein gesetzlich festgelegter Freibetrag trotzdem auf dem Konto erhalten bleibt.

<sup>3</sup> Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Reform des Kontopfändungsschutzes. Bundesrat Drucksache 663/07 v. 28.09.07 S. 1. (*iff\_2012\_Basisprodukte-Finanzdienstleistungen-Gutachten*, S. 10). S. hierzu auch LG Bremen, Urt. v. 16.6.2005 – 2 O 408/05, VuR 2005, 350 (351); LG Stuttgart, Urt. v. 6.9.1996 – 27 O 343/96, NJW 1996, 3347 (3348); AG Essen, Urt. v. 28.10.1993 – 23 C 548/93, NJW-RR 1994, 1330 (1330 f.).

<sup>4</sup> Die Global Findex-Datenbank ist die weltweit umfassendste Datenbank darüber, wie Erwachsene sparen, Kredite aufnehmen, Zahlungen leisten und Risiken managen. Sie wird anhand von national repräsentativen Umfragen bei mehr als 150.000 Erwachsenen ab 15 Jahren in mehr als 140 Volkswirtschaften erhoben und erhebt Informationen über den Zugang zu und die Nutzung von formellen und informellen Finanzdienstleistungen.

von Ersparnissen, Krediten und Versicherungen erhöht. Diese Elemente werden als zentral für wirtschaftliches Wachstum und Stabilität betrachtet.<sup>5</sup>

Barrieren führen dazu, dass einige Personengruppen ohne Unterstützung vom Zahlungsverkehr ausgeschlossen sind und somit auch an der fortschreitenden Entwicklung neuer Bezahlmethoden nicht teilhaben können. Grundsätzlich sollte die Wahlfreiheit erhalten bleiben, also, je nach der spezifischen Situation und den Präferenzen, die jeweils beste Bezahlmethode wählen zu können. Gerade diese Wahlfreiheit ist aber praktisch nicht für alle Verbraucher:innen gleichermaßen gegeben. Mit der steigenden Bedeutung digitaler Bezahlssysteme ist eine steigende Alternativlosigkeit bei Transaktionen des täglichen Lebens, z. B. bei Online-Käufen, verbunden. Wird also eine Digitalisierung von Zahlungsdiensten nicht gleichzeitig mit einer Absicherung der Teilhabe daran durch gefährdete Bevölkerungsgruppen verbunden, bedroht das deren wirtschaftliche und weitergehende gesellschaftliche Teilhabe, auch mit negativen Konsequenzen für Wachstum und soziale Stabilität.

Barrieren zum Zahlungsverkehr können sowohl auf Ebene der Zahlungsdienstleister, der gesetzlichen Regulierung aber auch auf Seiten der Verbraucher:innen existieren und in vier verschiedene Kategorien zusammengefasst werden (siehe Abbildung 1). Praktische Barrieren umfassen eine mangelnde technische Ausstattung auf Seiten der Verbraucher:innen sowie eine unzureichende Infrastruktur, auf die Verbraucher:innen zurückgreifen können. Bei der Barriere durch mangelnde Kompetenz geht es zum einen um eine mangelnde finanzielle und digitale Kompetenz auf Seiten der Verbraucher:innen, aber zum anderen auch um die mangelnde Kompetenz auf Seiten der Zahlungsdienstleister, durch die beispielsweise eine Unterstützung der Verbraucher:innen bei der Anwendung digitaler Tools fehlt. Ergänzt werden diese beiden Kategorien um die Barriere durch eine fehlende Bereitschaft sowohl auf Seiten der Verbraucher:innen, die „neuen“ Technologien misstrauen, als auch auf Seiten der Anbieter, die aus betriebswirtschaftlichen Gründen vorhandene Regulierungen nicht umsetzen. Bei der vierten Kategorie geht es um regulatorische Barrieren, die vorliegen, wenn die Regulierung selbst dazu führt, dass der Zugang zum Zahlungsverkehr behindert wird.

Abbildung 1: Schema- Barrieren des Zahlungsverkehrs



Quelle: Eigene Darstellung.

<sup>5</sup> Demircuc-Kunt u. a. (2018); Demircuc-Kunt u. a. (2022).

Vielfältig sind vor allem die praktischen Barrieren, die sowohl in der Ausstattung der Verbraucher:innen mit den notwendigen „Tools“, aber auch im Angebot der Zahlungsdienstleister zu finden sind. Entsprechend sind Beispiele für eine praktische Barriere fehlende Zugänge zur Technologie von digitalen Zahlungssystemen wie das Fehlen eines Smartphones, eines Computers oder gar Internetanschlusses. Bei einem Leben ohne Internet ist der Zugang zu Angeboten und Leistungen der öffentlichen Verwaltung und hierbei insbesondere zu Dienstleistungen im Zusammenhang mit dem Finanzamt bereits derzeit die größte Herausforderung. Am zweithäufigsten werden Einschränkungen bei Bankgeschäften genannt.<sup>6</sup> Bedeutsam ist dabei auch die sogenannte Barrierefreiheit. Barrierefreiheit bedeutet, dass alle Menschen – unabhängig von körperlichen, geistigen oder sensorischen Beeinträchtigungen – gleichberechtigt Zugang zu den verschiedenen Bereichen des Zahlungsverkehrs haben sollten.<sup>7</sup> Relevant sind bei den praktischen Barrieren aber auch eine instabile Infrastruktur sowie die lückenhafte Akzeptanz für unterschiedliche Zahlungsmittel im (Online-)Handel.

Gerade in Bezug auf den barrierefreien Zugang zu Zahlungsdienstleistungen ist die Vielfältigkeit der von Einschränkungen betroffenen Menschen in Deutschland zu beachten. In Deutschland leben ca. 10,4 Millionen Menschen mit einer offiziell anerkannten Behinderung in privaten Haushalten.<sup>8</sup> Davon haben rund 7,9 Millionen Menschen (9,3 Prozent der Gesamtbevölkerung) eine anerkannte Schwerbehinderung.<sup>9</sup> Nur etwa 3 Prozent der Behinderungen sind angeboren oder treten unmittelbar nach der Geburt auf; knapp 91 Prozent der Behinderungen in Deutschland entstehen im Lebensverlauf, zumeist durch Krankheiten, die häufig erst im höheren Alter auftreten.<sup>10</sup> Zudem gibt es in Deutschland Schätzungen zufolge etwa 6,2 Millionen funktionale Analphabeten. Die davon betroffenen können nur einzelne Wörter oder Sätze lesen und schreiben. Sie haben ferner Schwierigkeiten, zusammenhängende Texte zu verstehen oder selbst zu verfassen.<sup>11</sup>

Im vorliegenden Gutachten werden die unterschiedlichen Barrieren für den Zugang zum Zahlungsverkehr vor dem Hintergrund der digitalen Entwicklung diskutiert. In einer Übersicht über den Zahlungsverkehr in Deutschland und die aktuelle und künftige Regulierung werden die vier verschiedenen Kategorien von Barrieren unter Berücksichtigung der Rechtslage und der Erkenntnisse aus der Literaturanalyse sowie aus den Expert:inneninterviews in Kapitel III analysiert. Daraus abgeleitete Implikationen zur Stärkung der Teilhabe am Zahlungsverkehr werden in Kapitel IV vorgestellt. Kapitel V zieht das Fazit.

---

<sup>6</sup> BAGSO (2022), S. 6.

<sup>7</sup> Kalisz (2023), S. 292.

<sup>8</sup> Statistisches Bundesamt (2021), S. 75.

<sup>9</sup> Statistisches Bundesamt (19.07.2024); Statistisches Bundesamt (2024).

<sup>10</sup> Statistisches Bundesamt (19.07.2024).

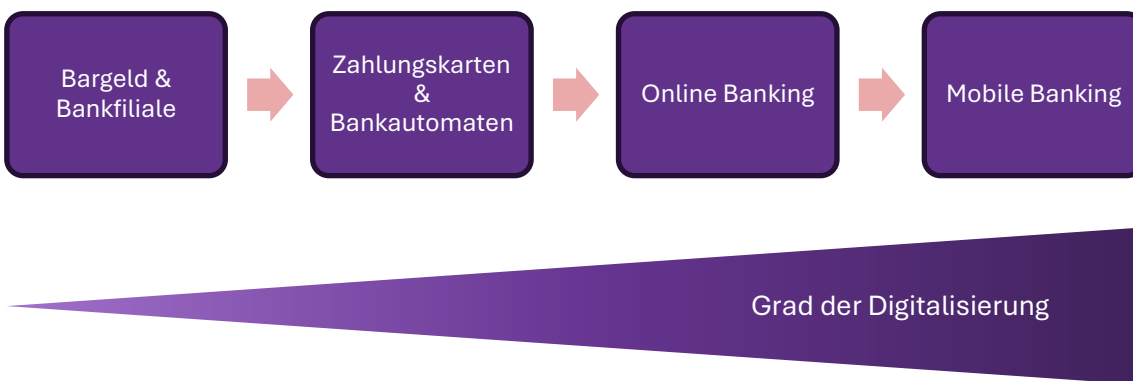
<sup>11</sup> Grotlüschen u. a. (2019), S. 5.

## II. Hintergrund

### 1. Das Zahlungsverhalten in Deutschland

Für den Zahlungsverkehr stehen unterschiedliche Zugangsoptionen zur Verfügung. Etabliert haben sich dabei über die Jahrzehnte hinweg die Barzahlung und der bargeldlose Zahlungsverkehr mithilfe von Karten und Überweisungsformularen sowie Überweisungen über Banking Terminals. Dazu gekommen sind seit einiger Zeit digitale Bezahlssysteme wie Online-Banking, Online-Kauf und Mobile-Banking wie E-Wallets und mobile Payment-Apps. Die Entwicklung und Bedeutung digitaler Bezahlssysteme steigt fortlaufend; sie sind aber zugleich für potenzielle Nutzer:innen mit neuen Herausforderungen verbunden. Im Folgenden wird dargestellt, mit welchem Nutzungsverhalten Verbraucher:innen auf die Entwicklung neuer Zahlungsmethoden reagieren.

Abbildung 2: Digitalisierung des Zahlungssystems



Quelle: Eigene Darstellung

Laut einer Bundesbankstudie aus dem Jahr 2023 bleibt in diesem Jahr Bargeld das am häufigsten verwendete Zahlungsmittel, obwohl der Anteil weiterhin rückläufig ist. Über die Hälfte der Transaktionen (51 Prozent) wird in bar durchgeführt, was etwa 26 Prozent der Gesamtausgaben entspricht.<sup>12</sup> Abhängig vom Zahlungsort variiert der Einsatz von Bargeld als Zahlungsmittel bei den Verbraucher:innen erheblich. Bargeld wird insbesondere im stationären Handel (d. h. sämtliche Geschäfte des Einzelhandels sowie Tankstellen), in der Gastronomie, im Freizeitbereich, bei Dienstleistungen und im privaten Umfeld häufiger verwendet als unbare Zahlungsmittel. Im stationären Handel bleibt Bargeld mit einem Anteil von 50 Prozent an den Transaktionen das am häufigsten genutzte Zahlungsmittel.<sup>13</sup>

Das Zahlungsverhalten der Verbraucher:innen zeigt eine deutliche Heterogenität, und zwar in Abhängigkeit vom Zahlungsbetrag sowie dem sozioökonomischen Hintergrund der Verbraucher:innen. Kleinbeträge unter 20 Euro werden überwiegend in bar beglichen, während bei höheren Beträgen zwischen 20 und 500 Euro zunehmend unbare Zahlungsmethoden, insbesondere

<sup>12</sup> Deutsche Bundesbank (Juli 2024), S. 6.

<sup>13</sup> Deutsche Bundesbank (Juli 2024), S. 42.

Debitkarten, bevorzugt werden.<sup>14</sup> Ältere Menschen sowie Personen mit niedrigem Einkommen neigen stärker zur Nutzung von Bargeld. So liegt der Anteil bargeldbasierter Transaktionen bei der jüngsten Altersgruppe (18 bis 24 Jahre) bei etwa 35 Prozent, während er in der ältesten Gruppe (ab 65 Jahren) 64 Prozent erreicht. Auch Personen aus der niedrigsten Einkommensgruppe (Haushaltseinkommen unter 2.500 €) tätigen mit 59 Prozent Zahlungen häufiger in bar.<sup>15</sup>

Der meistgenutzte Abhebeort für Bargeld in Deutschland ist weiterhin der Geldautomat. 96 Prozent der Befragten beschafft sich dort Bargeld. Die Ladenkasse wurde im Jahr 2023 nur von 41 Prozent der Befragten zum Abheben genutzt.<sup>16</sup>

Eine zentrale Rolle bei unbaren Zahlungsmitteln spielen Zahlungsdienste. Ein Zahlungsdienst bezeichnet eine Dienstleistung, die es ermöglicht, Geldbeträge zwischen verschiedenen Parteien zu transferieren. Diese Dienste erleichtern Zahlungen und Überweisungen und sind ein wichtiger Bestandteil des Finanzwesens. Zahlungsdienste können sowohl von Banken als auch von spezialisierten Zahlungsdienstleistern angeboten werden. Es gibt verschiedene Arten von Zahlungsdiensten, darunter:

- Überweisungen (Banküberweisungen oder Überweisungen via Online-Banking),
- Karten- und Lastschriftzahlungen (Zahlungen, die über Kreditkarten, Debitkarten oder Lastschriftverfahren abgewickelt werden),
- E-Wallets (elektronische Geldbörsen, die für Online-Zahlungen genutzt werden, wie PayPal, Apple Pay oder Google Pay),
- Zahlungsabwicklungen im E-Commerce (Systeme, die Online-Zahlungen für Webshops und Dienstleistungen ermöglichen),
- Mobile Payments (Zahlungen, die über mobile Geräte und Apps durchgeführt werden, etwa via QR-Codes oder durch NFC-Technologie z. B. kontaktlose Zahlungen).

Zahlungsdienste stellen sicher, dass Gelder sicher, schnell und effizient zwischen den Beteiligten ausgetauscht werden, und sie unterliegen oft regulatorischen Bestimmungen, um Betrug und Missbrauch zu verhindern.<sup>17</sup>

Zahlungskarten<sup>18</sup> sind ein integraler Bestandteil des Zahlungsverhaltens deutscher Verbraucher:innen und werden oft als Alternative zu Bargeld genutzt. Beim unbaren Zahlungsverhalten haben Debitkarten mit einem Anteil von gut einem Drittel an den Gesamtausgaben an Popularität gewonnen. Damit werden sie häufiger verwendet als Überweisungen und Lastschriften (20 Prozent) sowie Kreditkarten (10 Prozent). Die Akzeptanz unbarer Zahlungsmittel ist auch seit der Covid-19-Pandemie deutlich gestiegen. Mittlerweile können 80 Prozent der Zahlungen vor Ort mit Karte oder unbaren Zahlungsmitteln erfolgen.<sup>19</sup>

---

<sup>14</sup> Deutsche Bundesbank (Juli 2024), S. 37.

<sup>15</sup> Deutsche Bundesbank (Juli 2024), S. 39.

<sup>16</sup> Deutsche Bundesbank (Juli 2024), S. 16.

<sup>17</sup> Siehe dazu auch BaFin (2024).

<sup>18</sup> Eine Zahlungskarte ist eine Karte, die zur bargeldlosen Bezahlung von Waren und Dienstleistungen verwendet werden kann. Es gibt verschiedene Arten von Zahlungskarten, darunter Debitkarten, Kreditkarten, Prepaid-Karten, Ladekarten oder Kundenkarten sowie die virtuelle Karte.

<sup>19</sup> S-Payment (Juni 2024), S. 9.

In Deutschland verfügen 97 Prozent der deutschsprachigen Bevölkerung ab 18 Jahren über ein Girokonto,<sup>20</sup> was für diese den Zugang zu Bank- und Finanzdienstleistungen und somit die finanzielle Teilhabe ermöglicht bzw. erleichtert. Die Verwendung von Online-Banking ist weiterhin sehr verbreitet und im Vergleich zu 2021 nochmals angestiegen. 81 Prozent der Befragten der Bundesbank-Studie 2023, die das Internet nutzen, geben an, Bankgeschäfte über Online-Banking abzuwickeln. Trotz rückläufigem Trend, führen die meisten Teilnehmenden ein Konto bei einer Sparkasse; den höchsten Zuwachs verzeichnen allerdings Direktbanken.<sup>21</sup>

Die Nutzung von Online-Banking hat in allen Alters- und Einkommensgruppen zugenommen. Jüngere und einkommensstärkere Bevölkerungsgruppen greifen besonders häufig auf diese Form des Bankings zurück: In der Altersgruppe der 18- bis 24-Jährigen liegt der Anteil der Online-Banking-Nutzer:innen bei 94 Prozent, während er bei den über 65-Jährigen lediglich 66 Prozent beträgt. Ebenso zeigt sich eine klare Einkommensabhängigkeit, wobei der Anteil der Online-Banking-Nutzer:innen in Haushalten mit einem Einkommen über 5.000 Euro um 20 Prozentpunkte höher ist als in Haushalten mit weniger als 2.500 Euro.<sup>22</sup> Der Bildungsgrad und die Erwerbstätigkeit korrelieren positiv mit der Nutzung von Online-Banking; Menschen mit einem höheren Bildungsgrad und einer Erwerbstätigkeit neigen also eher dazu, Online-Banking zu nutzen. Trotz dieser Unterschiede ist seit 2021 in allen Bevölkerungsgruppen ein signifikanter Anstieg der Nutzung von Online-Banking zu verzeichnen. Befördert wird diese Entwicklung sicherlich auch dadurch, dass im Jahr 2023 bereits 91,7 Prozent der Haushalte in Deutschland einen Internetzugang besaßen.<sup>23</sup>

Parallel zur zunehmenden Verbreitung von Online-Banking gewinnen web- und app-basierte Bezahlverfahren im Onlinehandel an Bedeutung. Zu den bekanntesten Anbietern zählen PayPal, Klarna und digitale Wallets.<sup>24</sup> Im Bereich des Onlinehandels erweist sich das Internetbezahlverfahren PayPal mit einer Nutzungsrate von 79 Prozent als führendes Zahlungsmittel. Die zweitbeliebteste Option ist der Kauf auf Rechnung, den 62 Prozent der Kunden bevorzugen. Kreditkarten werden von 38 Prozent der Online-Käufer für Transaktionen genutzt. Jüngere Verbraucher:innen (14-29 Jahre) bevorzugen bei Online-Einkäufen deutlich häufiger Debitkarten (wie die Girocard, Mastercard Debit oder Visa Debit) als Zahlungsmethode, ältere Verbraucher:innen (60-78 Jahre) nutzen dagegen häufiger Zahlungen auf Rechnung oder Kreditkarten. Seit 2021 hat sich die Hinterlegung von Debit- und Kreditkarten in digitalen Wallets kaum verändert. 24 Prozent der Debitkarten- und 33 Prozent der Kreditkartenbesitzer:innen nutzen eine Wallet zur Speicherung ihrer Karten, sodass sie diese für Zahlungen an Ladenkassen und online einsetzen können.<sup>25</sup> Zudem wächst die Bedeutung von In-App-Zahlungen stetig. 81 Prozent der Verbraucher:innen in Deutschland kaufen Waren oder Dienstleistungen direkt über eine Nutzung von Apps ein.<sup>26</sup> Die Verwendung von In-App-Käufen zeigt ebenfalls eine klare Altersabhängigkeit: Jüngere Generationen tätigen deutlich häufiger In-App-Käufe als ältere. So nutzen beispielsweise jüngere Verbraucher:innen mehr als doppelt so häufig In-App-Zahlungen im

---

<sup>20</sup> Deutsche Bundesbank (Juli 2024), S. 19.

<sup>21</sup> Deutsche Bundesbank (Juli 2024), S. 19.

<sup>22</sup> Deutsche Bundesbank (Juli 2024), S. 24.

<sup>23</sup> Eurostat (2023). Nach eigener Berechnung.

<sup>24</sup> Deutsche Bundesbank (Juli 2024), S. 25.

<sup>25</sup> Deutsche Bundesbank (Juli 2024), S. 24.

<sup>26</sup> S-Payment (Juni 2024), S. 15.

Vergleich zu älteren Verbraucher:innen.<sup>27</sup> Der Anteil mobiler Transaktionen hat sich bei den 18- bis 24-Jährigen fast verdreifacht, während er bei den 25- bis 34-Jährigen sogar von 4 Prozent auf 14 Prozent gestiegen ist und sich somit fast vervierfacht hat.<sup>28</sup>

Die Voraussetzungen für mobile Zahlungen haben sich durch die steigende Verbreitung mobiler Endgeräte verbessert: 91 Prozent der Deutschen besitzen ein Smartphone und 12 Prozent nutzen eine Smartwatch. Beim mobilen Bezahlen an der Ladenkasse kommen vor allem Smartphones zum Einsatz. 27 Prozent der Smartphone-Besitzer:innen, die mindestens ein innovatives Bezahlverfahren kennen, haben bereits damit an der Kasse bezahlt, was einen Zuwachs von 10 Prozentpunkten im Vergleich zu 2021 bedeutet.<sup>29</sup> Trotz der zunehmenden Verbreitung mobiler Bezahlmethoden verzichten aber viele weiterhin auf deren Nutzung.

Bei der oben dargestellten Vielfalt an möglichen Zahlungsmitteln, erfreut sich Bargeld als Zahlungsmittel nach wie vor großer Beliebtheit. Allerdings nimmt der Anteil kontinuierlich ab und gleichzeitig der Anteil bargeldloser Zahlungsmittel zu. In einer Befragung der Deutschen Bundesbank<sup>30</sup> gaben 44 Prozent der Menschen an, dass sie am liebsten unbar zahlen, 28 Prozent bevorzugen Bargeld und 28 Prozent sind unentschlossen. Während insbesondere jüngere und einkommensstarke Menschen gerne auf bargeldlose Zahlungsmittel zurückgreifen, bevorzugen ältere Menschen und Personen mit niedrigeren Einkommen Bargeld.<sup>31</sup>

Trotz der sinkenden Bargeldnutzung erachten 69 Prozent es als sehr wichtig bzw. wichtig, dass sie die Möglichkeit zur Bargeldnutzung haben.<sup>32</sup> Zwei Drittel der Teilnehmer:innen an einer Umfrage wünschen sich, auch in 15 Jahren genauso häufig mit Bargeld bezahlen zu können wie heute. Für bestimmte Bevölkerungsgruppen ist es besonders wichtig, diese Möglichkeit zu haben.<sup>33</sup> So nimmt mit steigendem Alter der Befragten die Bedeutung von Bargeld zu. Unabhängig vom Alter schätzen 74 Prozent der Befragten, die ihre eigene finanzielle Situation als schlecht einschätzen, die Bargeldnutzung als sehr oder ziemlich wichtig ein.<sup>34</sup>

Verbraucher:innen legen großen Wert auf sichere Zahlungslösungen, die ihre persönlichen Daten und Transaktionen schützen. Das zeigt zum Beispiel der „Payment Behavior Report“ der Europäischen Zentralbank (EZB), auch SPACE-Report genannt, der 2019 und 2022 eine Umfrage unter Bürger:innen im Euroraum durchführte.<sup>35</sup> Zu solchen Möglichkeiten gehören moderne Verschlüsselungstechnologien, aber auch die Möglichkeit, Zahlungen zu überwachen und bei Bedarf zu sperren.

Personen, die gar nicht am digitalen Zahlungsverkehr teilnehmen möchten oder dies aus verschiedenen Gründen nicht können, sehen sich mit zusätzlichen Kosten und Nachteilen

---

<sup>27</sup> S-Payment (Juni 2024), S. 21.

<sup>28</sup> Deutsche Bundesbank (Juli 2024), S. 38.

<sup>29</sup> Deutsche Bundesbank (Juli 2024), S. 26.

<sup>30</sup> Die durchgeführte telefonische Befragung ist repräsentativ für die deutschsprachige Bevölkerung ab 18 Jahren in der Bundesrepublik Deutschland. Es wurden 5.698 Telefoninterviews durchgeführt (vgl. Deutsche Bundesbank (Juli 2024), S. 11).

<sup>31</sup> Deutsche Bundesbank (Juli 2024), S. 28.

<sup>32</sup> Deutsche Bundesbank (Juli 2024), S. 50.

<sup>33</sup> Ehrenberg-Silies u. a. (Januar 2024), S. 9.

<sup>34</sup> Deutsche Bundesbank (Juli 2024), S. 50.

<sup>35</sup> European Central Bank (2022), S. 43.

konfrontiert. Viele Banken und Finanzdienstleister haben ihre Dienstleistungen zunehmend auf digitale Kanäle umgestellt, was dazu führt, dass Personen, die weiterhin auf traditionelle, nicht-digitale Angebote angewiesen sind, oft mit höheren Gebühren belastet werden. Ein Beispiel sind die immer häufiger nur digital zur Verfügung gestellten Kontoauszüge, wohingegen die Papierform mit Zusatzgebühren verbunden ist.<sup>36</sup> Laut Verbraucherumfrage der Bundesbank sind die Kosten je Transaktion bei Bargeld am niedrigsten. Bei der Kostenanalyse wurden dabei Gebühren, zum Beispiel für die Kontoführung, für Barabhebungen an Geldautomaten oder für Zahlungskarten, finanzielle Schäden bei Verlust und Betrug ebenso wie Zeitaufwand oder Kosten der Datenpreisgabe berücksichtigt. Allein die Anschaffungskosten für Hard- und Software blieben bei dieser Analyse außen vor. Wird der Transaktionsbetrag bei der Analyse berücksichtigt, zeigt die Analyse, dass Debitkartenzahlungen auf Grund des geringeren Zeitaufwands günstiger sind.<sup>37</sup>

## 2. Übersicht über die aktuelle und künftige Regulierung

Nachdem das Zahlungsverhalten und die diesbezüglichen Präferenzen von Verbraucher:innen dargestellt wurden, widmet sich dieses Kapitel den aktuellen und künftigen Regulierungen, die den Zugang und die Barrieren zum Zahlungsverkehr betreffen. Entsprechend wird im Folgenden die Regulierung von Bargeld als gesetzlichem Zahlungsmittel, von Zahlungsdiensten, inklusive Zahlungskonten und hier insbesondere von Basiskonten und dem Digitalen Euro vorgestellt. Zudem gibt das Kapitel eine kurze Übersicht zur Regulierung der Barrierefreiheit. Mit Bezug auf die Barriere „fehlende Bereitschaft“ schließt sich eine Übersicht über die Regulierung der Betrugsprävention an und als vertrauensbildende Institution ein Überblick über Datenschutz. Als regulatorisches Spannungsfeld wird im letzten Unterkapitel die Regulierung der Prävention von Geldwäsche und Terrorismusfinanzierung behandelt.

### 2.1 Bargeld

Bargeld ist sowohl im deutschen als auch im europäischen Recht das gesetzliche Zahlungsmittel. Im deutschen Recht wird dies in § 14 Abs. 1 S. 2 BBankG<sup>38</sup> und im europäischen Recht in Art. 128 Abs. 1 S. 3 AEUV sowie in Art. 10 Abs. 2 und Art. 11 S. 2 der Verordnung über die Einführung des Euro normiert.<sup>39</sup> Eine Geldschuld erlischt, soweit keine abweichende Vereinbarung vorliegt, lediglich durch Barzahlung (vgl. § 362 BGB).<sup>40</sup> Insofern besteht regelmäßig keine Möglichkeit, die Erfüllung einer Geldschuld durch ein gesetzliches Zahlungsmittel, also Barzahlung, abzulehnen oder auszuschließen.<sup>41</sup>

Nach der deutschen und europäischen Rechtsprechung ist es allerdings möglich, Ausnahmen von dieser Regel zu statuieren. Diese sind u. a. im öffentlichen Interesse beispielsweise durch nationale

---

<sup>36</sup> BAGSO (2022), S. 23.

<sup>37</sup> Knümann u. a. (2024), 36f.

<sup>38</sup> Gesetz über die Deutsche Bundesbank in der Fassung der Bekanntmachung vom 22. Oktober 1992, BGBl. I 1782.

<sup>39</sup> Verordnung (EG) Nr. 974/98 des Rates vom 3. Mai 1998 über die Einführung des Euro, ABl. 1998 L 139/1. Allerdings umfasst die Regelung des Art. 128 Abs. 1 AEUV lediglich die Euro-Banknoten, wohingegen die Verordnung über die Einführung des Euro sowohl die Euro-Banknoten als auch die Euro-Münzen umfasst.

<sup>40</sup> M.w.N. BGH, Urt. v. 20.5.2010 – Xa ZR 68/09, NJW 2010, 2719 (2720, Rn. 29); Fetzner, in: Säcker u. a. (2023), BGB § 362 Rn. 19.

<sup>41</sup> EuGH, Urt. v. 26. Januar 2021 – Rs. C-422/19 und C-423/19 (*Hessischer Rundfunk*), Rn. 46 ff.

**Digital Abgehängt**

Vorschriften zur Geldwäschebekämpfung<sup>42</sup> oder durch Allgemeine Geschäftsbedingungen (AGB) für Angebote im Fernabsatz<sup>43</sup> zu finden. Um unter anderem um die Eigenschaft des Bargelds als gesetzliches Zahlungsmittel zu festigen, hat die Europäische Kommission 2023 einen Vorschlag für eine Verordnung über Euro-Banknoten und Euro-Münzen als gesetzliches Zahlungsmittel unterbreitet (BargeldVO-Vorschlag).<sup>44</sup>

Da das Bargeld gesetzliches Zahlungsmittel ist, muss es akzeptiert werden, wenn die Vertragsparteien nichts anderes vereinbaren. Allerdings steht es einem Verkäufer oder Dienstleister frei, auch andere Zahlungsmethoden wie Überweisungen, Kartenzahlungen oder digitale Zahlungsmethoden zu akzeptieren. Zudem gilt in Deutschland die Vertragsfreiheit, d. h., die Parteien eines Vertrags (z.B. Käufer:in und Verkäufer:in) können vereinbaren, durch welche Zahlungsmethode die vertragliche Zahlungspflicht zu erfüllen ist.

## 2.2 Zahlungsdienste

Die Teilnahme am digitalen Zahlungsverkehr und der Zugang zum Bargeld finden durch Zahlungskonten statt. Das Recht des Zahlungsverkehrs ist auf europäischer Ebene in der zweiten Zahlungsdiensterichtlinie (auf Englisch „Payment Services Directive 2“ oder kurz „PSD2“)<sup>45</sup> geregelt.<sup>46</sup> Die zivilrechtlichen Vorschriften der PSD2 wurden im BGB und durch das ZAG ins deutsche Recht umgesetzt.<sup>47</sup> Gemäß § 675f Abs. 2 BGB (Art. 4 Nr. 21 PSD2) wird durch einen Zahlungsdiensterahmenvertrag der Zahlungsdienstleister, i. d. R. eine Bank,<sup>48</sup> verpflichtet, für Nutzer:innen einzelne und aufeinander folgende Zahlungsvorgänge auszuführen sowie für sie ein Zahlungskonto zu führen. Insofern handelt es sich bei den Verträgen zur Eröffnung und Führung eines Zahlungskontos um Zahlungsdiensterahmenverträge i. S. v. § 675f Abs. 2 BGB. Der Vorschlag für eine Verordnung über Zahlungsdienste im Binnenmarkt (auf Englisch „Payment Services Regulation“ oder kurz „PSR-E“)<sup>49</sup> ändert diese zivilrechtliche Konstellation nicht.<sup>50</sup>

---

<sup>42</sup> EuGH, Urt. v. 26. Januar 2021 – Rs. C-422/19 und C-423/19 (*Hessischer Rundfunk*), Rn. 59 ff.

<sup>43</sup> BGH, Urt. v. 20.5.2010 – Xa ZR 68/09, NJW 2010, 2719 (2720, Rn. 32 ff.).

<sup>44</sup> Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Euro-Banknoten und Euro-Münzen als gesetzliches Zahlungsmittel, COM(2023) 364 final.

<sup>45</sup> Auf Wunsch des Auftraggebers wird die gängige Abkürzung in englischer Sprache „PSD2“ verwendet.

<sup>46</sup> Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl. 2015 L 337/35.

<sup>47</sup> Die aufsichtsrechtlichen Vorschriften der PSD2 werden durch den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt, zur Änderung der Richtlinie 98/26/EG und zur Aufhebung der Richtlinien (EU) 2015/2366 und 2009/110/EG, COM(2023) 366 final (PSD3-E). Der Analyse in diesem Gutachten wurde auch die Version des Vorschlags nach der ersten Lesung im Europäischen Parlament zugrunde gelegt, s. <https://data.consilium.europa.eu/doc/document/ST-10651-2024-INIT/DE/pdf>, Letzter Abruf: 6. Januar 2025. Wenn diese Version zitiert wird, wird sie als „PSD3-E, EP-Bericht“ gekennzeichnet.

<sup>48</sup> Vgl. § 1 Abs. 1 ZAG i.V.m. § 675c Abs. 3 BGB.

<sup>49</sup> Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010, COM(2023) 367 final. Auf Wunsch des Auftraggebers wird die gängige Abkürzung in englischer Sprache „PSR-E“ verwendet. In diesem Gutachten wurde auch die Version des Vorschlags nach der ersten Lesung im Europäischen Parlament zugrunde gelegt, s. [https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST\\_10664\\_2024\\_INIT](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_10664_2024_INIT), Letzter Abruf: 29. Oktober 2024. Wenn diese Version zitiert wird, wird sie als „PSR-E, EP-Bericht“ gekennzeichnet.

<sup>50</sup> Vgl. Art. 18 ff. PSR-E; vgl. Zahrtke (2024a), S. 135 f.

**Digital Abgehängt**

Der Zahlungsdienstleister hat Zahlungsaufträge der Zahlungsdienstnutzer:innen innerhalb eines Geschäftstages auszuführen.<sup>51</sup> Die Parteien des Zahlungsdiensterahmenvertrages können allerdings vereinbaren, dass bestimmte Zahlungsaufträge schneller als an einem Geschäftstag auszuführen sind. Dies geschieht in der Praxis als Echtzeit- bzw. Sofortüberweisung, die regelmäßig für ein gesondertes Entgelt angeboten wird.<sup>52</sup> Durch die Verordnung zu Echtzeitüberweisungen in Euro<sup>53</sup> hat der europäische Gesetzgeber Vorschriften zu Echtzeitüberweisungen in die SEPA-VO<sup>54</sup> eingefügt und alle Zahlungsdienstleister dazu verpflichtet, die Versendung und den Empfang von Echtzeitüberweisungen<sup>55</sup> im einheitlichen Euro-Zahlungsverkehrsraum (auf Englisch „Single Euro Payment Area“ oder kurz „SEPA“) zu ermöglichen (Art. 5a Abs. 1 SEPA-VO).<sup>56</sup> Wird der Zahlungsdienstleister mit einer Echtzeitüberweisung beauftragt, ist er verpflichtet, den Auftrag sofort auszuführen (Art. 5a Abs. 4 lit. b SEPA-VO).<sup>57</sup>

Der Zugang zum Bargeld wird regelmäßig über Zahlungskonten gewährleistet. Die Zahlungsdienstnutzer:innen haben gem. §§ 667, 675 BGB einen Anspruch auf Auszahlung des Kontoguthabens, das eine Geldschuld der jeweiligen Bank (des Zahlungsdienstleisters) darstellt. Wie oben erläutert, ist diese Geldschuld durch Barzahlung zu erfüllen, soweit die Vertragsparteien nichts anderes vereinbart haben. In der Praxis machen die Zahlungsdienstnutzer:innen ihren Anspruch u. a. durch Abheben von Bargeld an Bargeldautomaten geltend. Wenn die Zahlungsdienstnutzer:innen an den Geldautomaten ihrer Bank oder des Verbunds, wozu auch ihre Bank gehört (wie z. B. Cash Group oder Cash Pool) Geld abheben, verursacht dies in der Regel keine zusätzlichen Kosten, da eine Abhebung von Geld als Zahlungsvorgang (Art. 4 Nr. 5 PSD2; § 675f Abs. 4 BGB) im Rahmen des Zahlungsdiensterahmenvertrages getätigt wird.

Gleichwohl gibt es auch Geldautomatenbetreiber, die keine Zahlungsdienste erbringen, sondern lediglich Bargeldabhebungsdienste anbieten. Diese sind vom Anwendungsbereich der PSD2 und ZAG ausgeschlossen (Art. 3 lit. o PSD2; § 2 Abs. 1 Nr. 14 ZAG). Allerdings sind sie verpflichtet, die Zahlungsdienstnutzer:innen über alle Gebühren für Geldabhebungen sowohl vor der Abhebung als auch auf der Quittung nach dem Erhalt von Bargeld zu informieren (Art. 3 lit. o PSD2; Art. 248 § 17a EGBGB).

---

<sup>51</sup> Wenn es sich um einen Zahlungsvorgang innerhalb des Europäischen Wirtschaftsraums handelt. D. h. konkret, dass der Zahlungsdienstleister verpflichtet ist, sicherzustellen, dass der Zahlungsbetrag spätestens am Ende des auf den Zugangszeitpunkt des Zahlungsauftrags folgenden Geschäftstags beim Zahlungsdienstleister des/der Zahlungsempfänger:in eingeht. Für in Papierform ausgelöste Zahlungsvorgänge kann diese Frist um einen weiteren Geschäftstag verlängert werden (Art. 83 Abs. 1 PSD2, § 675s Abs. 1 BGB). Der Zahlungsdienstleister des/der Zahlungsempfänger:in ist i. d. R. verpflichtet, dem/der Zahlungsempfänger:in den Zahlungsbetrag unverzüglich verfügbar zu machen, nachdem der Betrag auf dem Konto des Zahlungsdienstleisters eingegangen ist (Art. 87 Abs. 2 PSD2, § 675t Abs. 1 BGB).

<sup>52</sup> Vgl. Omlor (2024), S. 3478.

<sup>53</sup> Verordnung (EU) 2024/886 des Europäischen Parlaments und des Rates vom 13. März 2024 zur Änderung der Verordnungen (EU) Nr. 260/2012 und (EU) 2021/1230 und der Richtlinien 98/26/EG und (EU) 2015/2366 im Hinblick auf Echtzeitüberweisungen in Euro, ABL. L vom 19.3.2024.

<sup>54</sup> Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009. ABL. 2012 L 94/22 (SEPA-VO).

<sup>55</sup> Spätestens zu welchem Datum die Versendung und der Empfang von Echtzeitüberweisungen angeboten werden müssen, regelt die Verordnung unterschiedlich, s. Art. 5a Abs. 8 SEPA-VO. Die Pflicht zum Empfang von Echtzeitüberweisungen gilt für die Zahlungsdienstleister im Euroraum ab 9. Januar 2025; die Pflicht zur Versendung und dem Empfang von Echtzeitüberweisungen gilt für in der EU ansässige Zahlungsdienstleister, E-Geld-Institute und Zahlungsinstitute spätestens ab 9. Juli 2027; s. Omlor (2024), S. 3478.

<sup>56</sup> Das Entgelt für diese darf das Entgelt für andere Überweisungen nicht übersteigen.

<sup>57</sup> Der Zahlungsdienstleister des/der Zahlungsempfänger:in ist ebenfalls verpflichtet, den Zahlungsbetrag innerhalb von zehn Sekunden nach Eingang des Zahlungsauftrags für eine Echtzeitüberweisung dem Zahlungskonto des/der Zahlungsempfänger:in gutzuschreiben (Art. 5a Abs. 4 lit. c SEPA-VO). Mehr dazu s. Omlor (2024), S. 3479 ff.

## 2.3 Basiskonto

Zahlungskonten haben sich insbesondere in den letzten Jahrzehnten zu einem Grundbedürfnis im Zusammenhang mit einer Teilnahme am Markt etabliert. Eine Deckung dieses Grundbedürfnisses kristallisiert sich immer stärker als notwendige Voraussetzung für eine umfassende Teilhabe am Wirtschaftsleben heraus.<sup>58</sup> Personen ohne ein Zahlungskonto sind somit darin eingeschränkt, notwendige Dienstleistungen in Anspruch zu nehmen. Zudem haben sie keinen Zugang zu digitalen Zahlungssystemen.

Dieser Tatsache ist der europäische Gesetzgeber mit der Zahlungskonten-Richtlinie (ZKRL) entgegengekommen,<sup>59</sup> um die Teilhabe am Binnenmarkt und an der Nutzung seiner Vorteile durch einen Zugang zu einem Zahlungskonto für alle Verbraucher:innen zu ermöglichen. Der deutsche Gesetzgeber hat die Richtlinie durch das Zahlungskontengesetz (ZKG)<sup>60</sup> in nationales Recht umgesetzt. Seitdem regelt es die Bedingungen für die Nutzung von Zahlungskonten und soll den Zugang zu grundlegenden Bankdienstleistungen für alle Verbraucher:innen sicherstellen.

Alle Verbraucher:innen haben – unabhängig von der eigenen finanziellen Lage – seit dem Jahr 2016 einen Anspruch auf Abschluss eines Zahlungskontovertrags mit grundlegenden Funktionen, also auf ein Basiskonto (§§ 30 f. ZKG). Der Antrag auf Abschluss eines Basiskontovertrags kann nur in gesetzlich festgelegten Fällen abgelehnt werden, z. B. wenn Verbraucher:innen bereits Inhaber:innen eines Zahlungskontos sind (§ 35 ZKG).<sup>61</sup> Damit soll sichergestellt werden, dass auch sozial benachteiligte oder vorübergehend finanziell belastete Personen Zugang zu einem Konto haben. Der Zahlungsdienstleister ist durch einen Basiskontovertrag u. a. dazu verpflichtet, Kontoinhaber:innen Barein- und auszahlungen sowie die Teilnahme am digitalen Zahlungsverkehr zu ermöglichen (§ 38 ZKG). Dafür dürfen die Zahlungsdienstleister ein angemessenes Entgelt verlangen (§ 41 ZKG). Die Formulierung „angemessenes Entgelt“ stellt zugleich eine unbestimmte Formulierung dar und wird regelmäßig unterschiedlich beurteilt.<sup>62</sup>

## 2.4 Digitaler Euro

Da das Bargeld derzeit das einzige gesetzliche Zahlungsmittel ist, ist die Erfüllung einer Geldschuld durch bargeldlose Zahlung nur dann möglich, wenn die Vertragsparteien sich darüber einigen.<sup>63</sup> Bei den digitalen Zahlungen per Karte, Online- oder Mobilebanking wird allerdings kein durch die Zentralbank, sondern durch Geschäftsbanken geschaffenes Geld verwendet, also Buch- bzw. Giralgeld. Beim Buch- bzw. Giralgeld handelt es sich juristisch wie ökonomisch um Geldforderungen gegen Kreditinstitute.<sup>64</sup> Die Übertragung von Buchgeld, also eine Überweisung,

---

<sup>58</sup> Erwägungsgrund 7 PSD2; LG Bremen, Urt. v. 16.6.2005 – 2 O 408/05, VuR 2005, 350 (351); LG Stuttgart, Urt. v. 6.9.1996 – 27 O 343/96, NJW 1996, 3347 (3348); AG Essen, Urt. v. 28.10.1993 – 23 C 548/93, NJW-RR 1994, 1330 (1330 f.).

<sup>59</sup> Richtlinie 2014/92/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten und den Zugang zu Zahlungskonten mit grundlegenden Funktionen, ABl. 2014 L 257/214.

<sup>60</sup> Gesetz über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten sowie den Zugang zu Zahlungskonten mit grundlegenden Funktionen (Zahlungskontengesetz - ZKG) vom 11. April 2016, BGBl. I 720.

<sup>61</sup> Für die sonstigen Ablehnungsgründe s. §§ 36 f. ZKG.

<sup>62</sup> Siehe unten II.2.3 in diesem Bericht.

<sup>63</sup> Grundmann, in: Säcker u. a. (2023), BGB § 245 Rn. 111.

<sup>64</sup> M.w.N. Grundmann, in: Säcker u. a. (2023), BGB § 245 Rn. 6; Schefold, in: Ellenberger/Bunte (2022), § 98 Rn. 94 ff.

setzt voraus, dass beide Vertragsparteien über ein Zahlungskonto (§ 2 Abs. 4 ZKG) verfügen.<sup>65</sup> Das Buchgeld ist Eins-zu-eins in Zentralbankgeld konvertierbar, d. h. die Kreditinstitute haben die Geldforderung gegen sie durch Bargeld zu erfüllen, wenn die Erfüllung in Bargeld verlangt wird, z. B. an einem Geldautomaten.

Derzeit plant die EU, den digitalen Euro<sup>66</sup> einzuführen, um von der Zentralbank geschaffenes Geld als gesetzliches Zahlungsmittel auch in digitaler Form zur Verfügung zu stellen. Zu diesem Zweck hat die Europäische Kommission 2023 einen Vorschlag für eine Verordnung zur Einführung des digitalen Euro unterbreitet (DigEUR-Vorschlag).<sup>67</sup> Hauptziel der Einführung des digitalen Euro ist seine Nutzung als einheitliche Währung mit Status als gesetzliches Zahlungsmittel im Euro-Währungsgebiet.<sup>68</sup> Insofern werden die Eigenschaft des digitalen Euro als gesetzliches Zahlungsmittel und die Annahmepflicht ausdrücklich geregelt (Art. 7 DigEUR-Vorschlag). Allerdings sind dabei auch einige Ausnahmen zur Annahmepflicht vorgesehen. Insbesondere Kleinstunternehmen, die keine elektronischen Zahlungsmittel annehmen, gemeinnützige Rechtsträger und natürliche Personen, die in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten handeln, werden von der Verpflichtung zur Annahme von Zahlungen in digitalem Euro ausgenommen (Art. 9 DigEUR-Vorschlag). Im Übrigen wird es nicht möglich sein, einseitig die Annahme des digitalen Euro, beispielsweise durch AGB, auszuschließen (Art. 10 DigEUR-Vorschlag). Der digitale Euro wird zum Nennwert sowohl in Bargeld als auch in Girogeld und elektronisches Geld konvertierbar sein (Art. 12 Abs. 1, Art. 13 Abs. 5 DigEUR-Vorschlag).

## 2.5 Barrierefreiheit

Derzeit unterliegen die Anbieter von Finanzdienstleistungen noch keinen allgemeinen Anforderungen, die die Barrierefreiheit der von ihnen angebotenen Dienstleistungen gewährleisten. Es bestehen lediglich Formerfordernisse zu vorvertraglichen und vertraglichen Informationspflichten. Diese Erfordernisse betreffen allerdings vor allem Form und Inhalt der Informationen, aber nicht die Barrierefreiheit (vgl. Art. 248 § 2 EGBGB).<sup>69</sup> Aus diesem Grund ist es derzeit dem Ermessen des Zahlungsdiensteanbieters überlassen, ob er den Zugang zu digitalen Zahlungsdienstleistungen und zum Bargeld barrierefrei gestalten möchte.

Um den Zugang zu Dienstleistungen, u. a. zu den Bank- und Finanzdienstleistungen nicht nur theoretisch, sondern auch praktisch zu ermöglichen, hat der europäische Gesetzgeber 2019 die Barrierefreiheitsrichtlinie (BFRL) verabschiedet.<sup>70</sup> Der deutsche Gesetzgeber hat die Richtlinie durch das Barrierefreiheitsstärkungsgesetz (BFSG) und die Verordnung zum

---

<sup>65</sup> Schmieder, in: Ellenberger/Bunte (2022), § 25 Rn. 4.

<sup>66</sup> Der digitale Euro ist eine geplante digitale Währung der Eurozone, die von der EZB und den nationalen Zentralbanken der EU-Mitgliedstaaten eingeführt werden soll. Er wird als digitale Form des physischen Euro verstanden, die jedoch ausschließlich in digitaler Form existiert. Der Digitale Euro befindet sich derzeit noch in der Entwicklungs- und Testphase. Die Entscheidung, ob und wann er vollständig eingeführt wird, hängt von weiteren Untersuchungen und einer breiten öffentlichen und politischen Diskussion ab.

<sup>67</sup> Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung des digitalen Euro, COM(2023) 369 final.

<sup>68</sup> Erwägungsgrund 21 DigEUR-Vorschlag.

<sup>69</sup> Auskunft der BaFin auf Anfrage.

<sup>70</sup> Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen, ABl. 2019 L 151/70.

Barrierefreiheitsstärkungsgesetz (BFSGV) ins nationale Recht umgesetzt.<sup>71</sup> Wie die Richtlinie vorschreibt (Art. 131 Abs. 2 BFRL), wird das BFSG für Produkte und Dienstleistungen, die nach dem 28. Juni 2025 in den Verkehr gebracht oder erbracht werden (§ 1 BFSG) anwendbar. Die BFRL und das BFSG zielen darauf ab, dass Menschen mit Behinderungen, die Bank- und Finanzdienstleistungen in der gesamten Union nutzen, fundierte Entscheidungen treffen und sich angemessen, in gleicher Weise wie alle anderen Verbraucher:innen geschützt wissen können.<sup>72</sup> In diesem Zusammenhang sind die Zahlungsdienste und auch die Identifizierungsmethoden barrierefrei zu gestalten.

Die Umsetzung des BFSG und der BFSGV obliegt der noch zu gründenden nationalen Marktbeobachtungsbehörde. Eine Beaufsichtigung der Barrierefreiheit von Finanzdienstleistungen oder im elektronischen Geschäftsverkehr angebotenen Dienstleistungen findet entsprechend nicht durch die BaFin statt. Sie ist auch nicht an der Entwicklung der Marktbeobachtungsstelle beteiligt, da dies nach dem BFSG Sache der Länder ist (§ 28 BFSG i.V.m. § 1 Nr. 22 BFSG). Dies gilt jedoch nicht für einzelne Anforderungen an die Barrierefreiheit, die aktuell durch Finanzaufsichtsgesetze geregelt sind wie beispielsweise Anforderungen an das Format von verschiedenen näher bestimmten Informationen, die von den beaufsichtigten Unternehmen Verbraucher:innen zur Verfügung zu stellen sind.<sup>73</sup>

## 2.6 Betrug und Betrugsprävention

Wirksame Zahlungsvorgänge bedürfen der Zustimmung der Zahler:innen, also der Autorisierung durch sie (Art. 64 Abs. 1 PSD2, § 675j Abs. 1 BGB).<sup>74</sup> Die Form der Zustimmung zur Ausführung von Zahlungsvorgängen wird zwischen Zahler:innen und Zahlungsdienstleistern vereinbart. Zur digitalen Abwicklung von Zahlungsvorgängen werden den Zahlungsdienstnutzer:innen Zahlungsinstrumente und personalisierte Sicherheitsmerkmale zur Verfügung gestellt. Ein Zahlungsinstrument ist jedes personalisierte Instrument oder Verfahren, das zur Erteilung eines Zahlungsauftrags verwendet wird (Art. 4 Nr. 14 PSD2, § 1 Abs. 20 ZAG), beispielsweise eine Zahlungskarte.<sup>75</sup> Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die Zahlungsdienstleister zur Überprüfung der Identität von Nutzer:innen oder zur Überprüfung der berechtigten Verwendung eines bestimmten Zahlungsinstruments, also zur Authentifizierung, bereitstellen (Art. 4 Nr. 29, 31 PSD2, § 1 Abs. 23, 25 ZAG),<sup>76</sup> z. B. persönliche Identifikationsnummern (PIN) oder Transaktionsnummern (TAN).<sup>77</sup> Die Authentifizierung dient also der nachprüfaren Urheberschaft einer Willenserklärung.<sup>78</sup>

Bei der Auslösung eines Fernzahlungsvorgangs sind die Zahlungsdienstleister verpflichtet, eine starke Kundenauthentifizierung zu verlangen (Art. 97 Abs. 1 PSD2, § 55 Abs. 1 ZAG). Es handelt sich

---

<sup>71</sup> Gesetz zur Umsetzung der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (Barrierefreiheitsstärkungsgesetz - BFSG), BGBl. 2021 I 2970.

<sup>72</sup> Erwägungsgrund 39 BFRL.

<sup>73</sup> Auskunft der BaFin auf Anfrage.

<sup>74</sup> Durch Art. 3 Abs. 34a PSR-E wird Autorisierung als „eine Genehmigung, die in einem Verfahren erteilt wird, bei dem der Zahlungsdienstnutzer einen bestimmten Vorgang freiwillig und in voller Kenntnis aller relevanten Fakten authentifiziert“ definiert.

<sup>75</sup> Jungmann, in: Säcker u. a. (2023), BGB § 675j Rn. 52.

<sup>76</sup> Art. 3 Nr. 34 und 37 PSR-E behalten diese Legaldefinitionen bei.

<sup>77</sup> Maihold, in: Ellenberger/Bunte (2022), § 33 Rn. 21 ff.

<sup>78</sup> Jungmann, in: Säcker u. a. (2023), BGB § 675j Rn. 64.

um einen Fernzahlungsvorgang, wenn der Zahlungsvorgang über das Internet oder mittels eines Geräts, das für die Fernkommunikation verwendet werden kann, ausgelöst wird (Art. 4 Nr. 6 PSD2, § 1 Abs. 19 ZAG). Eine starke Kundenauthentifizierung (auf Englisch „Strong customer authentication“ oder kurz „SCA“) ist so ausgestaltet, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist und sie unter Heranziehung von mindestens zwei voneinander unabhängigen Elementen, also einer Zwei-Faktor-Authentifizierung, geschieht (Art. 4 Nr. 30 PSD2, § 1 Abs. 24 ZAG).<sup>79</sup> Bei der starken Kundenauthentifizierung werden in der Praxis entweder Mobilgeräte, wie z. B. Smartphones und Tablets oder TAN-Generatoren eingesetzt.

Die Zahlungsdienstnutzer:innen unterliegen Sorgfalts- und Anzeigepflichten mit Bezug auf Zahlungsinstrumente und personalisierte Sicherheitsmerkmale. Sie sind vor allem verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um die Zahlungsinstrumente und personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen (Art. 69 Abs. 2 PSD2, § 675l Abs. 1 BGB).<sup>80</sup> Beispielsweise haben sie die Zahlungskarte nach dem Einsatz sofort zurückzunehmen, an Geldautomaten und Zahlungsterminals ihre Karten-PIN möglichst verdeckt einzugeben, ihre Computer und Smartphones z. B. mittels spezieller Programme vor unberechtigtem Zugriff zu schützen.<sup>81</sup> Zudem müssen sie den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Zahlungsinstruments unverzüglich anzeigen, nachdem sie hiervon Kenntnis erlangt haben (Art. 69 Abs. 1 lit. b PSD2, § 675l Abs. 1 BGB). Zahlungsdienstleister haben vorvertraglich die Zahlungsdienstnutzer:innen zu informieren, wie sie die Anzeigepflicht ihnen gegenüber erfüllen können.<sup>82</sup>

## 2.7 Datenschutz

Der Verarbeitung personenbezogener Daten unterliegt in der EU der Datenschutz-Grundverordnung (DSGVO).<sup>83</sup> Dementsprechend ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn u. a. die Verarbeitung für die Durchführung des Vertrags bzw. vorvertraglicher Maßnahmen oder zur Erfüllung einer rechtlichen Verpflichtung bzw. zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist oder wenn die betroffene Person in die Verarbeitung eingewilligt hat (Art. 6 DSGVO).

Die DSGVO kommt auch im Rahmen des digitalen Zahlungsverkehrs oder beim Zugang zum Bargeld zur Anwendung. Art. 94 PSD2 weist auf den Vorgänger der DSGVO hin, allerdings gilt dieser Verweis als ein Verweis auf die DSGVO (Art. 94 DSGVO). Als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO verarbeiten die Zahlungsdienstleister die personenbezogenen Daten der Zahlungsdienstnutzer:innen entweder aufgrund ihrer Einwilligung (vgl. Art. 94 Abs. 2 PSD2), oder aufgrund der Erforderlichkeit für die Durchführung des Zahlungsdiensterahmenvertrages, oder

---

<sup>79</sup> S. auch Art. 3 Nr. 35 und 85 PSR-E. Die Einzelheiten und Ausnahmen zur starken Kundenauthentifizierung werden in der Delegierten Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (SKA-DVO) geregelt, worauf auch § 55 Abs. 5 ZAG Bezug nimmt.

<sup>80</sup> Die gleichen Pflichten werden in Art. 52 PSR-E geregelt.

<sup>81</sup> Jungmann, in: Säcker u. a. (2023), BGB §675l Rn. 35, 40.

<sup>82</sup> Art. 52 Nr. 5 lit. a und e PSD2, Art. 248 § 4 Abs. 1 Nr. 5 lit. a und e EGBGB i. V. m. § 675d Abs. 1 BGB.

<sup>83</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1.

aufgrund der Erforderlichkeit zur Erfüllung einer rechtlichen Pflicht, z. B. den Pflichten aus dem GwG oder zur Betrugsprävention (vgl. Art. 94 Abs. 1 PSD2).

## 2.8 Prävention von Geldwäsche und Terrorismusfinanzierung

Die Regulierung zur Prävention von Geldwäsche und Terrorismusfinanzierung ist ein Beispiel für regulatorische Barrieren. Dabei geht es um Regulierungen, deren strenge Anwendung die Barrieren für den Zugang zum Zahlungsverkehr verursachen bzw. verstärken können. Entsprechend wird im Folgenden auf diese Regulierung eingegangen.

Die Banken müssen nach dem Geldwäschegesetz (GwG)<sup>84</sup> und der Abgabenordnung (AO)<sup>85</sup> ihre Vertragspartner:innen identifizieren, auch zum Zwecke der Eröffnung jeglicher Konten (§§ 1, 10 f. GwG; § 154 AO). Gemäß § 1 Abs. 3 GwG hat die Bank die Identität ihrer Vertragspartner:innen festzustellen und zu überprüfen. Wenn andere Personen für Vertragspartner:innen auftreten, z. B. gesetzliche Betreuer:innen oder Vertreter:innen der Kontoinhaber:innen, muss die Bank auch die Identität dieser Personen prüfen (§ 10 Abs. 1 Nr. 1 GwG). Zu prüfen sind bei natürlichen Personen i. d. R. anhand eines gültigen amtlichen Ausweises (wie z. B. Personalausweis oder Reisepass) Vor- und Nachname, Geburtsort, Geburtsdatum, Staatsangehörigkeit und die Wohnanschrift (§§ 11 Abs. 4, 12 Abs. 1 GwG). Die Identifizierungspflicht gehört zu den allgemeinen Sorgfaltspflichten der Bank im Rahmen des GwG (§ 10 Abs. 1 Nr. 1 GwG).

Bei dem Identifizierungsverfahren sind auch die Verwaltungsakte der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) einschlägig. Diese befinden sich vor allem in den Auslegungs- und Anwendungshinweisen zum Geldwäschegesetz<sup>86</sup> und im Rundschreiben zum Videoidentifizierungsverfahren.<sup>87</sup>

Am 10. Juli 2027 wird die EU-Geldwäscheverordnung (GwVO)<sup>88</sup> wirksam. Art. 20 GwVO schreibt auch vor, dass u. a. Kredit- und Finanzinstitute (Art. 3 Nr. 1 und 2 GwVO) verpflichtet sind, vor der Begründung einer Geschäftsbeziehung die Identität der Kund:innen festzustellen und zu überprüfen (Art. 19 Abs. 1 lit. a, Art. 20 Abs. 1 lit. a, Art. 23 Abs. 1 GwVO). In diesem Zusammenhang haben sie alle Vor- und Nachnamen, Geburtsort und -datum, Staatsangehörigkeit, den gewöhnlichen Aufenthaltsort bzw. die Postanschrift sowie, falls verfügbar, die Steueridentifikationsnummer (Art. 22 Abs. 1 GwVO) festzustellen. Diese Informationen werden durch die Vorlage eines Personalausweises, Passes oder eines gleichwertigen Ausweisdokuments oder durch die Nutzung elektronischer Identifikationsmittel eingeholt (Art. 22 Abs. 6 GwVO).<sup>89</sup>

---

<sup>84</sup> Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG) vom 23. Juni 2017, BGBl. I 1822.

<sup>85</sup> Abgabenordnung (AO) in der Fassung der Bekanntmachung vom 1. Oktober 2002, BGBl. I 3866.

<sup>86</sup> BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Stand: November 2024, S. 40 ff., 76 ff., abrufbar auf [https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl\\_ae\\_auas\\_gw.pdf?\\_\\_blob=publicationFile&v=1](https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_gw.pdf?__blob=publicationFile&v=1), Letzter Abruf: 9. Januar 2025.

<sup>87</sup> BaFin, Rundschreiben 3/2017 (GW) vom 10. April 2017 zum Videoidentifizierungsverfahren, abrufbar auf [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs\\_1703\\_gw\\_videoident.html?nn=9450904#doc9143870bodyText8](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html?nn=9450904#doc9143870bodyText8), Letzter Abruf: 19. November 2024.

<sup>88</sup> Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, ABl. L vom 19.6.2024.

<sup>89</sup> Elektronische Identifizierung hat die Erfordernisse eines substanziellen oder hohen Sicherheitsniveaus nach der Verordnung über elektronische Identifizierung (eIDAS-VO, Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. 2014 L 257/73) zu erfüllen.

# III. Zugang und Nutzbarkeit im Zahlungsverkehr

## 1. Steigende Notwendigkeit einer Teilnahme am digitalen Zahlungsverkehr

Zumindest theoretisch haben Verbraucher:innen die Wahlfreiheit zwischen Barzahlung und der Nutzung unterschiedlicher digitaler Bezahlmethoden. Vor allem die Nutzung von Bargeld wird im Gegensatz zum digitalen Zahlungsverkehr für Verbraucher:innen als voraussetzungsfrei angesehen. Die Praxis weist allerdings auf Barrieren hin, die sowohl den Zugang zu als auch die Nutzung von Bargeld im Zahlungsverkehr immer häufiger einschränken. Diese Barrieren gilt es im Folgenden zu beleuchten. Sie machen auf das dringliche Erfordernis aufmerksam, existierende Barrieren im digitalen Zahlungsverkehr abzubauen, um finanzielle Exklusion zu vermeiden. Verbraucher:innen sollten Zugang zu Bargeld und digitalen Bezahlmethoden haben. Es kommt darauf an, den Verbraucher:innen auch praktisch Wahlfreiheit zwischen sämtlichen Bezahlmethoden zu ermöglichen. Darauf wird in Kapitel IV ausführlich eingegangen, wo auch Möglichkeiten eines Barriereabbaus bei Bargeld vorgestellt werden.

### 1.1 Einschränkungen im Zugang zu Bargeld bei Banken

Obwohl Bargeld nach wie vor gesetzliches Zahlungsmittel ist, gehen die Zugangsmöglichkeiten zu Bargeld immer weiter zurück.<sup>90</sup> Vor allem die Schließung von Bankfilialen und der Abbau von Geldautomaten zeichnen dafür verantwortlich. **Fehler! Verweisquelle konnte nicht gefunden werden.** zeigt, dass sich die Anzahl der Bankfilialen in den letzten 10 Jahren fast halbiert hat (2012: 38.336, 2022: 21.904). Die Anzahl der Bankautomaten geht hingegen erst seit 2018 kontinuierlich zurück und war bis dahin recht stabil.<sup>91</sup> Ein hierfür genannter Grund ist, dass der Betrieb der Geldautomaten auch aufgrund der vermehrten Sprengungen von Geldautomaten recht teuer ist.<sup>92</sup> Geldautomaten sind rund um die Uhr zugänglich im Gegensatz zu Bankfilialen mit oftmals sehr kurzen Öffnungszeiten.

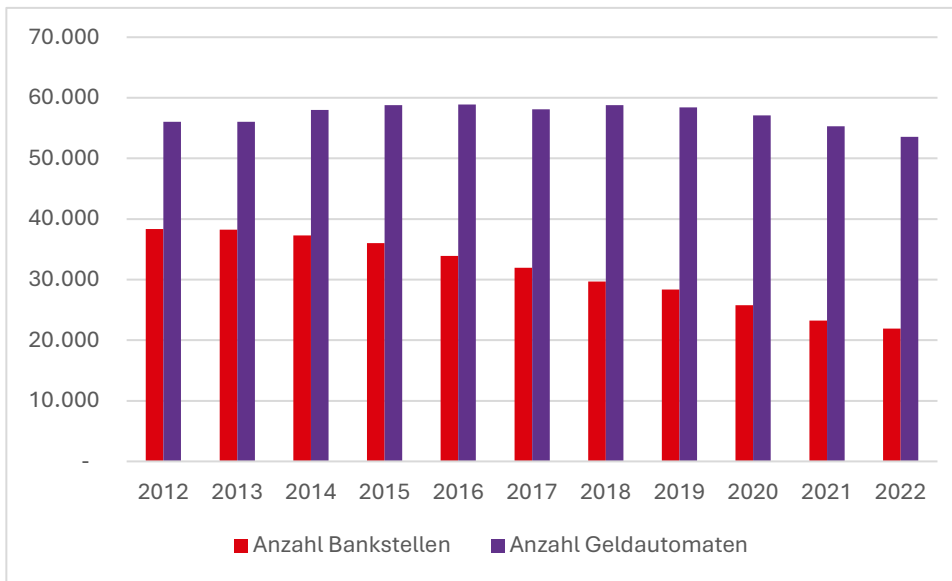
---

<sup>90</sup> Themenpapier BdZ-DG (2024b), S. 4.

<sup>91</sup> Themenpapier BdZ-DG (2024b), S. 3.

<sup>92</sup> Ehrenberg-Silies u. a. (Januar 2024), S. 68.

Abbildung 3: Anzahl Bankstellen und Geldautomaten



Eigene Darstellung nach Deutsche Bundesbank, 2022a; Deutsche Bundesbank, 2022b

Durch den Wegfall von Bankfilialen wird der Aufwand, an Bargeld zu gelangen, erschwert. Da hierdurch weitere Wege notwendig werden, geht er für alle Verbraucher:innen mit höheren Transaktionskosten einher. Erheblich ist die zusätzliche Belastung für Personen mit eingeschränkter Mobilität, also solchen Personen, die Schwierigkeiten beim Bewegen, Heben, Bücken und Gehen haben.<sup>93</sup> Betroffen davon sind vor allem mobilitätsbeschränkte Personen im hohen Alter. Für Personen mit geringem Einkommen stellen wiederum die mit weiteren Wegen verbundenen höheren Ausgaben ein Problem dar.<sup>94</sup> Hinzu kommt eine Unsicherheit darüber, wo man überhaupt an Bargeld kommen kann. So wird in einer Befragung aus den Niederlanden von einer Person auch kritisiert, dass es keine klaren Informationen darüber gebe, welche Bankfilialen noch verfügbar sind.<sup>95</sup>

Auch wenn Geldautomaten erreichbar sind, sind sie nicht immer barrierefrei und ist deren Nutzung so nicht für alle Personen möglich bzw. nicht voraussetzungsfrei.<sup>96</sup> So funktionieren Geldautomaten überwiegend über die visuelle Bedienung, was für Menschen mit Sehbehinderung eine Barriere darstellt.<sup>97</sup> Dies betrifft Größe, Helligkeit und den Farbkontrast des Textes, der gelesen werden muss.<sup>98</sup> Auch der Standort des Geldautomaten spielt eine Rolle, da Blendung oder unterschiedliche

<sup>93</sup> BAGSO (2022), S. 23; De Nederlandsche Bank (2023), 23f.

<sup>94</sup> FEANTSA (Januar 2022), S. 11.

<sup>95</sup> De Nederlandsche Bank (2023), S. 64.

<sup>96</sup> Barrierefreiheit bedeutet, dass alle Menschen – unabhängig von körperlichen, geistigen oder sensorischen Beeinträchtigungen – gleichberechtigt Zugang zu den verschiedenen Bereichen des Zahlungsverkehrs haben sollten. Das umfasst digitale Barrierefreiheit, also Webseiten, Apps und digitale Dokumente sollten so gestaltet sein, dass sie von Menschen mit Seh-, Hör- oder motorischen Einschränkungen genutzt werden können. Beispiele sind Screenreader-Kompatibilität, Untertitel für Videos oder die Möglichkeit, Inhalte per Tastatur zu navigieren. Ebenso beinhaltet es barrierefreie Kommunikation, also Informationen in leicht verständlicher Sprache bereitzustellen, Gebärdensprache zu integrieren oder alternative Kommunikationsmethoden anzubieten.

<sup>97</sup> Interview mit Herrn Markus Ertl, Deutsche Blinden- und Sehbehindertenverband e.V.; Middlesex University London (October 2018), S. 30; vgl. Kalisz (2023), S. 294.

<sup>98</sup> De Nederlandsche Bank (2023), S. 6.

Lichtverhältnisse die Lesefähigkeit beeinträchtigen können. Menschen ohne nutzbare Sehkraft benötigen taktile oder akustische Eingaben. Entsprechende Audioanschlüsse fehlen aber.<sup>99</sup> Zudem berichteten in einer Befragung aus den Niederlanden mehrere Teilnehmer:innen, dass der Geldautomat ihre Karte eingezogen hatte, weil sie die Tasten nicht in der richtigen Reihenfolge gedrückt oder eine falsche PIN eingegeben hatten.<sup>100</sup> Aber auch Personen ohne Sehbehinderung können Probleme dabei haben, die Anleitungen auf dem Geldautomaten-Bildschirm zu lesen und zu verstehen.<sup>101</sup> Dazu gehören beispielsweise Menschen mit geringer Lesekompetenz von Schriftsprache oder Menschen mit Migrationshintergrund, die der im Geldautomaten verfügbaren Sprachen nicht mächtig sind.<sup>102</sup>

## 1.2 Beschränkungen im Einzelhandel

Immer mehr Verbraucher:innen versorgen sich auch im Einzelhandel mit Bargeld.<sup>103</sup> Ein Vorteil dieser Möglichkeit besteht darin, dass die kostenlose Bargeldabhebung über die Ladentheke nicht an die kontoführende Bank gebunden ist, wie es bei Geldautomaten der Fall ist.<sup>104</sup> So kann über Cashback Bargeld an der Ladentheke abgehoben werden.

Abheben an der Ladentheke wird durch die Abhängigkeit von Bargeld-Einnahmen und Entgelte der Banken für die Bereitstellung von Bargeld eingeschränkt. So fallen im Handel für jede Cashback-Transaktion Gebühren an. Weitere Einschränkungen sind ferner Mindestbeträge für die Nutzung der Cashback-Leistung und die Öffnungszeiten des Handels.<sup>105</sup> Auch aufgrund der fehlenden Qualitätsprüfung des Bargelds sieht die Bundesbank die Bargeldbezugsmöglichkeiten an der Ladenkasse lediglich als Ergänzung, aber nicht als Ersatz für die bankgestützte Infrastruktur.<sup>106</sup>

Eine weitere Dimension bezüglich der Nutzbarkeit liegt in der Akzeptanz des Zahlungsmittels im Einzelhandel. Denn die Eigenschaft des Bargelds als gesetzliches Zahlungsmittel wäre untergraben, wenn die Annahme des Bargelds im Einzelhandel größtenteils verweigert würde. Im Einzelhandel ist für Käufe des täglichen Bedarfs überwiegend Barzahlung möglich (98 Prozent), anders sieht es allerdings im Dienstleistungssektor (84 Prozent) aus, wo immer häufiger ausschließlich auf Kartenzahlung abgestellt wird und Zahlungen in Bargeld abgelehnt werden.<sup>107</sup> Zudem gaben laut einer Umfrage der Bundesbank 18 Prozent der Befragten an, dass sie im vergangenen Monat Akzeptanzprobleme bei der Zahlung mit Karte oder digitalen Zahlverfahren hatten.<sup>108</sup>

Für Gewerbetreibende ist die Akzeptanz jedes Zahlungsmittels mit Aufwand verbunden. Insofern ist es eine betriebswirtschaftliche Frage, welche Zahlungsmittel akzeptiert werden.<sup>109</sup> So ist die

---

<sup>99</sup> Financial Services User Group (31.12.2023), S. 31; De Nederlandsche Bank (2023), S. 6.

<sup>100</sup> De Nederlandsche Bank (2023), S. 37.

<sup>101</sup> Financial Services User Group (31.12.2023), S. 34.

<sup>102</sup> De Nederlandsche Bank (2023), S. 37.

<sup>103</sup> Deutsche Bundesbank (Juli 2024), S. 6.

<sup>104</sup> Ehrenberg-Silies u. a. (Januar 2024), S. 72.

<sup>105</sup> Ehrenberg-Silies u. a. (Januar 2024), S. 71.

<sup>106</sup> Deutsche Bundesbank (2023).

<sup>107</sup> Themenpapier BdZ-DG (2024b), S. 3; Deutsche Bundesbank (Juli 2024), S. 31.

<sup>108</sup> Deutsche Bundesbank (Juli 2024), S. 32.

<sup>109</sup> Themenpapier BdZ-DG (2024b), S. 3.

Bereitstellung eines Kassensystems, inklusive Bargeldver- und entsorgung und die Sicherung der Kasse mit „vergleichsweise hohen Kosten“ auch aufgrund der Schließung der Filialen verbunden.<sup>110</sup> Wenn der Zugang zu Bargeld und dessen Akzeptanz eingeschränkt werden, wird die Nutzung von Bargeld zurückgehen. Dies wiederum führt aufgrund des hohen Fixkostenanteils für die Bargeldinfrastruktur zu steigenden Kosten pro Transaktion. Infolgedessen könnte die Bargeldakzeptanz weiter reduziert werden und eine Abwärtsspirale in Gang kommen.<sup>111</sup> Entsprechend ist bereits heute die Frage zu beantworten, inwiefern überhaupt noch eine Wahlfreiheit zwischen Bargeld und dem digitalen Zahlungsverkehr besteht.<sup>112</sup>

Die Ablehnung von Bargeld im Einzelhandel wird regelmäßig durch Schilder an den Geschäften deutlich gemacht, auf denen lediglich eine Akzeptanz von Kartenzahlungen oder Mobil-Zahlungen angekündigt wird. Dabei handelt es sich um vorformulierte Vertragsbedingungen, die den Charakter von allgemeinen Geschäftsbedingungen (AGB) aufweisen (§ 305 Abs. 1 S. 1 BGB). Die AGB zu Zahlungsmodalitäten dürfen die Vertragspartner nicht unangemessen benachteiligen (§ 307 Abs. 1 BGB). Vertragliche Vereinbarungen zur bargeldlosen Zahlung sind zwar nach dem allgemeinen Prinzip der Vertragsfreiheit zulässig, allerdings unterliegen die Bedingungen zu Zahlungsmodalitäten der Inhaltskontrolle nach § 307 BGB, wenn sie in den AGB vereinbart werden.<sup>113</sup> Eine Benachteiligung liegt beispielsweise vor, wenn von einer gesetzlichen Regelung abgewichen wird und diese unangemessen ist (§ 307 Abs. 2 Nr. 1 BGB). Bei den AGB zur bargeldlosen Zahlung liegt regelmäßig eine Benachteiligung vor, da Geldschulden nach der gesetzlichen Regelung grundsätzlich durch Barzahlung zu erfüllen sind.<sup>114</sup>

Die Wirksamkeit solcher AGB hängt davon ab, ob die Benachteiligung für die anderen Vertragspartner unangemessen ist. Bei der Angemessenheitsprüfung der Vertragsbedingungen zu Zahlungsmodalitäten berücksichtigt der BGH die Effektivität und Vereinfachung der Vertragsabwicklung und die Zumutbarkeit von dadurch für den anderen Vertragspartner entstandenen Nachteilen.<sup>115</sup> Die Zumutbarkeit solcher Vereinbarungen hat der BGH beispielsweise für den Fernabsatz bejaht, da eine Barzahlung in Fernabsatzgeschäften mit einem kaum zu rechtfertigenden Aufwand verbunden wäre.<sup>116</sup>

Es ist zweifelhaft, ob die Annahmeverweigerung von Bargeld aufgrund von AGB im Einzelhandel einer Inhaltskontrolle gem. § 307 BGB standhalten würde. § 270 BGB bestimmt den Ort, an dem die Zahlung zu erfolgen hat. Gemäß § 270 Abs. 2 BGB ist der Zahlungsort für die Geschäfte, die im Einzelhandel abgeschlossen worden sind, der Gewerbebetrieb des Gläubigers, also das Geschäft des Einzelhändlers. Es mag für den Einzelhandel effektiv und einfach sein, lediglich bargeldlose Zahlungen zu akzeptieren. Im Gegensatz zum Fernabsatz gehen allerdings Zahlungen mit Bargeld nicht mit einem hohen Aufwand einher, der nicht zu rechtfertigen wäre. Durch solche AGB werden also die Möglichkeiten der Verbraucher:innen, ihre vertragliche Zahlungspflicht zu erfüllen, in

---

<sup>110</sup> Ehrenberg-Silies u. a. (Januar 2024), 21, 38.

<sup>111</sup> Ehrenberg-Silies u. a. (Januar 2024), S. 9.

<sup>112</sup> Themenpapier BdZ-DG (2024b), S. 4.

<sup>113</sup> BGH, Urt. v. 20.5.2010 – Xa ZR 68/09, NJW 2010, 2719 (2720 Rn. 26); Urt. v. 23.1.2003 – III ZR 54/02, NJW 2003, 1237 (1238).

<sup>114</sup> BGH, Urt. v. 20.5.2010 – Xa ZR 68/09, NJW 2010, 2719 (2720 Rn. 29).

<sup>115</sup> BGH, Urt. v. 20.5.2010 – Xa ZR 68/09, NJW 2010, 2719 (2720 Rn. 26).

<sup>116</sup> BGH, Urt. v. 20.5.2010 – Xa ZR 68/09, NJW 2010, 2719 (2720 Rn. 33).

erheblichem Umfang eingeschränkt, auch weil die durch diese AGB entstandenen Nachteile für die Verbraucher:innen nicht in irgendeiner Weise ausgeglichen werden.<sup>117</sup> Folglich würde diese durch den Einzelhandel errichtete praktische Barriere durch die Rechtsprechung eventuell für unangemessen benachteiligend und daher für unwirksam erklärt

## 2. Barrieren des Zugangs und der Nutzung des digitalen Zahlungsverkehrs

Eine breite Nutzung digitaler Bezahlmethoden setzt voraus, dass insbesondere vier Barrieren abgebaut werden: Die erste Barriere betrifft eher praktische Aspekte des Zugangs und der Nutzung, die zweite Barriere Kompetenzmängel sowohl auf Seiten der Verbraucher:innen als auch der Zahlungsdiensteanbieter, die dritte Barriere bezieht sich auf die mangelnde Bereitschaft und schließlich folgt als vierte die regulatorische Barriere. Im Folgenden wird der Status Quo bezüglich dieser Barrieren beschrieben.

### 2.1 Praktische Barrieren

Mit der Digitalisierung der Zahlungsmittel nehmen auch die praktischen Voraussetzungen zur Teilnahme am digitalen Zahlungsverkehr zu. Neben der Notwendigkeit eines Zahlungskontos<sup>118</sup> braucht es ein mobiles Endgerät sowie motorische und kognitive Fähigkeiten, das Endgerät samt Zahlungsfunktionen wie Apps oder Online-Banking zu bedienen. Zudem sind Strom und ein Zugang zum Internet unabdingbar.<sup>119</sup> 2023 waren in Deutschland immerhin 8 Prozent der Haushalte mit keinem Internetzugang ausgestattet.<sup>120</sup> Auch ist WLAN nicht in allen gemeinschaftlichen Wohnformen vorhanden.<sup>121</sup> Zudem sind derzeit nicht alle mobilen Anwendungen für den Zahlungsverkehr barrierefrei zugänglich. Für sehbehinderte Menschen ist beispielsweise eine Hand-Auge-Steuerung am Touchscreen eine Herausforderung. Entsprechend ist Assistenz bei der Nutzung digitaler Zahlungsmittel für diese Personen notwendig.<sup>122</sup> Personen mit funktionellen Einschränkungen haben Schwierigkeiten, ihre Hände und Arme feinmotorisch zu kontrollieren, was bei der Nutzung des digitalen Zahlungsverkehrs wichtig wäre.<sup>123</sup>

Neben persönlicher Assistenz gibt es auch durchaus Geräte, die barrierefrei genutzt werden können, ggf. auch zusätzliche Hardware, um Personen mit entsprechenden Einschränkungen die Nutzung des digitalen Zahlungsverkehrs zu ermöglichen.<sup>124</sup> So benötigen unterstützt kommunizierende Personen, die per Augenkommunikation kommunizieren, meist zusätzliche

---

<sup>117</sup> Vgl. BGH, Urt. v. 20.5.2010 – Xa ZR 68/09, NJW 2010, 2719 (2720 Rn. 29).

<sup>118</sup> Siehe zur Regulierung zum Basiskonto auch Kapitel II.2.3

<sup>119</sup> Financial Services User Group (31.12.2023), S. 24.

<sup>120</sup> Eurostat (2023).

<sup>121</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), S. 3.

<sup>122</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), S. 2.

<sup>123</sup> Financial Services User Group (31.12.2023), S. 23.

<sup>124</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), S. 2.

Hardware, mit der sie sich in der digitalen Welt bewegen können.<sup>125</sup> Diese zusätzlichen Geräte müssen aber auch in der Praxis zu akzeptablen Preisen erhältlich und einfach zu bedienen sein.

Auch die Verwendung von Zahlungskarten ist noch nicht barrierefrei. Beispielsweise werden an den Supermarktkassen die POS-Geräte manchmal zu hoch gestellt. Diese hindern die gehbehinderten Menschen daran, die PIN ihrer Zahlungskarte eigenständig einzutippen. Nicht selten sind sie dann gezwungen, ihre PIN einem unbekanntem Dritten mitzuteilen, um den Zahlungsvorgang mit der Zahlungskarte überhaupt abschließen zu können. Die Mitteilung dieses persönlichen Sicherheitsmerkmals stellt wiederum eine Verletzung der Sorgfaltspflicht dar, personalisierte Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Ein weiteres Beispiel betrifft die Anzeigepflicht. So sind Personen mit einer Sprachbehinderung möglicherweise nicht in der Lage, verbal zu kommunizieren. Dass die Meldung eines Verlustes der Karte und die Bitte um ihre Sperrung von den Karteninhaber:innen persönlich telefonisch erfolgen muss, stellt für Personen mit Sprachbehinderung ein Problem dar.<sup>126</sup>

Die Kosten für den digitalen Zahlungsverkehr stellen eine Barriere vor allem für einkommensschwache Personen dar. Die Daten einer durch das *iff* durchgeführten Mystery-Shopping-Studie zeigen, dass Basiskonten in Deutschland mit Gebühren, die je nach Finanzinstitut zwischen 58,80 € und 143,40 € pro Jahr liegen, recht teuer sein können. Anders als in Spanien gibt es in Deutschland keine speziellen Preismodelle, die sich nach dem Grad der Verwundbarkeit der antragstellenden Person richten.<sup>127</sup> Die Kostenbarriere besteht auch in Bezug auf Soft- und Hardware, die für den digitalen Zahlungsverkehr nötig ist.

In der Literatur wird der Begriff „Nutzungslücke“ verwendet, um diesen Unterschied in der Nutzung zwischen Menschen aus einem niedrigeren und einem höheren sozioökonomischen Milieu zu beschreiben. Jemand mit geringem Einkommen kann sich zum Beispiel nur wenige oder gar keine Geräte leisten. Die digitale Transformation geht nicht nur für Unternehmen, sondern auch für Verbraucher:innen mit hohen Anschaffungskosten einher, die sich regelmäßig wiederholen, da Anwendungen zum Teil nur auf neuen Endgeräten nutzbar sind.<sup>128</sup> Erschwerend kommt hier hinzu, dass ein großer Teil der Menschen mit Behinderung in Deutschland von Sozialhilfe abhängt.<sup>129</sup> Im Regelsatz der Sozialhilfe sind monatliche Leistungen der digitalen Teilhabe zwar mit 50,35 Euro<sup>130</sup> erfasst, doch diese reichen für die Anschaffungskosten und die Deckung des Unterstützungsbedarfes nicht aus. Zu nennen sind hier beispielhaft die behinderungsspezifischen besonderen Bedarfe an besonderen Apps oder besonders leicht zu bedienbaren Tablets.<sup>131</sup>

---

<sup>125</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), S. 3; Financial Services User Group (31.12.2023), S. 5.

<sup>126</sup> Financial Services User Group (31.12.2023), S. 23.

<sup>127</sup> Finance Watch (2024), S. 10.

<sup>128</sup> SINUS (2020), S. 37; BAGSO (2022), S. 23.

<sup>129</sup> SINUS (2020), S. 37.

<sup>130</sup> Die Gelder für digitale Teilhabe laufen unter dem Posten „Post und Telekommunikation“. Regelbedarfsermittlungsgesetz vom 09.12.2020, Anlage ui § 28 SGG XII vom 01.01.2024.

<sup>131</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), S. 6.

## 2.2 Mangelnde Kompetenz

Für einen effektiven Zugang zu digitalen Zahlungsdiensten und für deren verantwortungsvolle Nutzung ist nicht nur finanzielle, sondern auch digitale Kompetenz sowohl auf Seiten der Verbraucher:innen als auch auf Seiten der Anbieter von Nöten. Für die Anbieter sind digitale Kompetenz und Nutzerschulung für die erfolgreiche Anwendung digitaler Methoden essenziell. Für Verbraucher:innen gesellt sich eine ausreichende Medienkompetenz hinzu. Alle drei Kompetenzen sind vor dem Hintergrund des Bildungsniveaus, kognitiver Fähigkeiten und des Erfahrungswissens in unserer Gesellschaft unterschiedlich verteilt. Menschen mit geringen Kenntnissen auf diesen Gebieten sind oft nicht mit allen verfügbaren Hilfsangeboten vertraut und konzentrieren sich in der Regel auf persönliche Kontakte und Kurse, die in ihrer Umgebung angeboten werden.<sup>132</sup> Besondere Medien- und Nutzungskompetenzen benötigen im Übrigen Menschen mit geistiger Behinderung, damit sie verstehen, welche Rechte und Pflichten sie beim Online-Handel haben und welche Risiken bestehen.<sup>133</sup>

Die digitale Kompetenz stellt vor allem für Ältere eine besondere Herausforderung dar. Gerade ältere Menschen haben häufig Schwierigkeiten, Anwendungen des digitalen Zahlungsverkehrs zu nutzen. Im Gegensatz zu jüngeren Generationen sind sie in einer Welt ohne digitale Technologien und Internet aufgewachsen. In einer Umfrage zum Thema Senioren und Internet gaben 51 Prozent der über 80-Jährigen an, das Internet zumindest gelegentlich zu nutzen.<sup>134</sup> Menschen im Alter von 70 Jahren und älter haben zudem mehr Schwierigkeiten mit digitalen Bankgeschäften als damit, allgemein mit den digitalen Entwicklungen Schritt zu halten. Ein Viertel der Befragten im Alter von 70 Jahren und mehr, die an einer Online-Umfrage über die Nutzung digitaler Zahlungsdienste teilnahmen, sind teilweise nicht in der Lage, digitale Bankgeschäfte zu nutzen.<sup>135</sup> Im Übrigen zählen insbesondere ältere Migrant:innen zu den Nicht-Nutzer:innen des Internets.<sup>136</sup>

Digitale Finanzkompetenz ist in Deutschland aber auch generell ausbaufähig. Laut der OECD liegt die digitale Finanzkompetenz in Deutschland im Durchschnitt bei einem Wert von 64 (von 100 möglichen) Punkten.<sup>137</sup> Dieser Wert übersteigt den europäischen Durchschnitt von 52 Punkten.<sup>138</sup> Die digitale Kompetenz umfasst beispielsweise ein Grundverständnis für die Endgeräte, Symbolverständnis und digitale Fähigkeiten.<sup>139</sup> Auch Lese- und Schreibfähigkeiten werden hier vorausgesetzt. Ähnlich wie bei Geldautomaten ist die in den Anwendungen verwendete Sprache häufig kompliziert und meist sind die verfügbaren Sprachoptionen eingeschränkt, was vor allem für Migrant:innen eine Herausforderung sein kann.<sup>140</sup>

---

<sup>132</sup> De Nederlandsche Bank (2023), S. 19.

<sup>133</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), S. 2.

<sup>134</sup> Ergebnisse der SIM-Studie 2021 (2022), S. 394.

<sup>135</sup> De Nederlandsche Bank (2023), S. 21.

<sup>136</sup> BAGSO (2022), S. 8.

<sup>137</sup> OECD (2024), S. 34.

<sup>138</sup> OECD/INFE (2023), S. 22.

<sup>139</sup> Siehe Kapitel III.2

<sup>140</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), S. 2; Financial Services User Group (31.12.2023), S. 34; De Nederlandsche Bank (2023), S. 6.

Die notwendige Assistenz zur Nutzung von Anwendungen des digitalen Zahlungsverkehrs muss regelmäßig durch unterstützende Geräte oder Personen realisiert werden. Der Personenkreis ist entsprechend regelmäßig kurzfristig abhängig von Menschen, die sie unterstützen. In Wohneinrichtungen bedarf es eines entsprechend kompetenten Personals. Ist im persönlichen Umfeld keine unterstützende Person vorhanden, werden formelle oder informelle Vermittler um Hilfe gebeten, was mit einem Sicherheitsrisiko einhergehen kann.<sup>141</sup>

Die mangelnde Kompetenz seitens der Zahlungsdiensteanbieter verkörpert sich als mangelnde Unterstützung für Verbraucher:innen und unterschiedliche Verbrauchergruppen. Unterschiedliche Personengruppen haben einen unterschiedlichen Beratungs- und Unterstützungsbedarf. Sind die Kompetenzen der Bankmitarbeiter:innen nicht oder nicht ausreichend entwickelt worden, sind sie nicht in der Lage, dem vielfältigen Unterstützungsbedarf gerecht zu werden

Das Gleiche gilt auch für die Sicherheitsrisiken, die ein Bestandteil des digitalen Zahlungsverkehrs geworden sind. Je mehr es an der diesbezüglichen Unterstützung durch die Anbieter fehlt, desto mehr sind die Verbraucher:innen ihrem eigenen Schicksal überlassen. Da die Anbieter die Zahlungsdienste zunehmend über digitale Kanäle anbieten, liegt die Verantwortung für das Sicherheitsrisiko durch mangelnde Unterstützung zumindest teilweise auch auf Ihrer Seite. Um dieser Verantwortung gerecht zu werden, bedarf es sowohl finanzieller als auch digitaler Kompetenzen und die Fähigkeit, diese kundenspezifisch und auch digital kommunizieren zu können.

Durch den Rückgang von Bankfilialen wird die Erreichbarkeit von Bankmitarbeiter:innen erschwert. Kommunikation findet immer mehr mit Maschinen statt. Anders als bei einem persönlichen Gespräch vor Ort sind diese Maschinen nur unzureichend in der Lage, sich an die individuellen Bedürfnisse der Verbraucher:innen anzupassen.<sup>142</sup> Dadurch, dass im Allgemeinen eine komplizierte Sprache verwendet wird, wird für Verbraucher:innen auch die Identifikation von Betrugsfällen erschwert. Die Verbraucherumfrage des Verbraucherzentrale Bundesverbands zeigt, dass Verbraucher:innen teilweise lernen, Prozessen zu folgen, die sie nicht komplett verstehen. Dieses Verhalten erschwert es, Betrugsfälle zu identifizieren.<sup>143</sup>

Wird auf digitale Kundenkommunikation zurückgegriffen, können Beratungslücken finanzielle Schwierigkeiten befördern. Sind Filialen nicht (mehr) erreichbar, findet die Kundenbetreuung meist über Telefon beziehungsweise über ein Videokommunikationstool statt.<sup>144</sup> Für taube Personen ist die rein telefonische Kontaktaufnahme nicht möglich.<sup>145</sup> Videotelefonie, die Lippenlesen ermöglicht, ist hier eine Alternative. Auch Chatbots werden zur digitalen Kundenbetreuung angewandt, jedoch gelingt die Kommunikation zwischen Mensch und Maschine nach Erfahrungsberichten eher schlecht.<sup>146</sup> Diese vorliegenden Hindernisse in Bezug auf digitale

---

<sup>141</sup> Financial Services User Group (31.12.2023), S. 26.

<sup>142</sup> Middlesex University London (October 2018), S. 8; Ehrenberg-Silies u. a. (Januar 2024), S. 39.

<sup>143</sup> Verbraucherzentrale Bundesverband e.V. (09.05.2024), S. 4.

<sup>144</sup> BAGSO (2022), S. 23.

<sup>145</sup> Cambier (07.08.2024), S. 2.

<sup>146</sup> De Nederlandsche Bank (2023), S. 64.

Beratung können je nach finanziellen und digitalen Kompetenzen zu Fehlanwendungen oder Fehlentscheidungen führen und damit zu finanziellen Schwierigkeiten.

## 2.3 Fehlende Bereitschaft

Eine weitere Barriere wird durch die fehlende Bereitschaft der Verbraucher:innen verursacht, am digitalen Zahlungsverkehr teilzunehmen. Diese besteht grundsätzlich zum einen aus der Präferenz der Verbraucher:innen, anonym am Zahlungsverkehr teilzunehmen (Datenschutz), und zum anderen aus einem Misstrauen in den digitalen Zahlungsverkehr. Auf diese beiden Aspekte wird im Folgenden eingegangen.

### Datenschutz

Die Verbraucherpräferenzen nach Anonymität im Zahlungsverkehr werden vor allem über Bargeld realisiert. Bargeld wird als einziges Zahlungsmittel angesehen, das es vermag, die Anonymität von Verbraucher:innen zu wahren.<sup>147</sup> Dies sehen auch immer mehr Verbraucher:innen so.<sup>148</sup> Die meisten Verbraucher:innen schätzen es nicht, online verfolgt zu werden. In einer von MdEP Patrick Breyer (Grüne, Deutschland) in Auftrag gegebenen Umfrage vom Dezember 2021 wurden 10 064 EU-Bürger:innen befragt, ob Internetnutzer:innen das Recht erhalten sollten, digitale Dienste zu nutzen, ohne dass persönliche Daten erhoben werden. 64 Prozent der Befragten sprachen sich für ein solches Recht aus (21 Prozent waren dagegen).<sup>149</sup>

Die Bedenken darüber, ob die Anonymität beim digitalen Zahlungsverkehr gewahrt bleibt, wird dadurch genährt, dass Verbraucher:innen kein Mitspracherecht darüber haben, ob sie in das Verhaltensdaten-Ökosystem einbezogen werden wollen und auf welche Weise.<sup>150</sup> Für die Nutzung des digitalen Zahlungsverkehrs müssen Verbraucher:innen Vertragsbeziehungen mit den privaten Anbietern dieser Zahlungsmittel sowie möglicher weiterer involvierter Parteien eingehen.<sup>151</sup> Jede einzelne digitale Transaktion wird mitverfolgt und gespeichert. Die Analyse dieser Informationen liefert Erkenntnisse über Gewohnheiten und Präferenzen von Verbraucher:innen, die man auf Nachfrage möglicherweise gar nicht mitgeteilt hätte.<sup>152153</sup>

---

<sup>147</sup> Beilner (2024), S. 475. Erwägungsgrund 14 BargeldVO-Vorschlag.

<sup>148</sup> Braatz, Frank (2024), S. 2.

<sup>149</sup> <https://www.patrick-breyer.de/en/survey-on-the-digital-services-act-eu-citizens-want-the-right-to-use-digital-services-anonymously/>. Letzter Aufruf BEUC (2022), S. 7.

<sup>150</sup> BEUC (2022), S. 6 Der europäische Verbraucherschutzverband BEUC verwendet hierfür den Begriff „Digitale Asymmetrie“. Damit wird beschrieben, wie moderne datengesteuerte Dienste Verbraucher:innen benachteiligen, da beispielsweise Verbraucher:innen mit Umgebungen konfrontiert werden, die durch Anbieter gestaltet sind. Nahezu jeder Dienst, mit dem sie im digitalen Umfeld in Berührung kommen, profitiert von Informationen, die sich aus der detaillierten Kenntnis ihres Lebens, ihrer Entscheidungen, ihrer Online-Suche, ihrer Korrespondenz, ihrer persönlichen Vorlieben und Schwächen ergeben. Selbst, wenn sich die Verbraucher:innen bewusst sind, dass ihre Online-Erfahrung personalisiert ist, werden sie vielleicht nie das Ausmaß oder die Mechanismen dieser Personalisierung kennen oder die Verzerrung, die sie in ihre Sicht des Marktes oder die Welt im Allgemeinen einführt, und die Entscheidungen, die sie infolgedessen treffen, s. BEUC (2022), S. 4.

<sup>151</sup> Themenpapier BdZ-DG (2024b), S. 3.

<sup>152</sup> Bock (10.09.2024), S. 3.

<sup>153</sup> BEUC (2022), S. 6 Der europäische Verbraucherschutzverband BEUC verwendet hierfür den Begriff „Digitale Asymmetrie“. Damit wird beschrieben, wie moderne datengesteuerte Dienste Verbraucher:innen benachteiligen, da beispielsweise Verbraucher:innen mit Umgebungen konfrontiert werden, die durch Anbieter gestaltet sind. Nahezu jeder Dienst, mit dem sie im digitalen Umfeld in Berührung kommen, profitiert von Informationen, die sich aus der detaillierten Kenntnis ihres Lebens, ihrer Entscheidungen, ihrer Online-Suche, ihrer Korrespondenz, ihrer persönlichen Vorlieben und Schwächen ergeben. Selbst, wenn sich die Verbraucher:innen bewusst sind, dass ihre Online-Erfahrung personalisiert ist, werden sie vielleicht nie das Ausmaß oder die Mechanismen dieser Personalisierung kennen oder die Verzerrung, die sie in ihre Sicht des Marktes oder die Welt im Allgemeinen einführt, und die Entscheidungen, die sie infolgedessen treffen, s. BEUC (2022), S. 4.

Laut europäischem Verbraucherschutz gibt es bei der Umsetzung der DSGVO beim digitalen Zahlungsverkehr Schwierigkeiten. Dies gilt, obwohl die DSGVO die Regeln für die Einwilligung gestärkt hat. Ein Problem sind verwirrende/unüberschaubare Online-Vertriebsketten, die es den Verbraucher:innen erschweren zu wissen, wer der Verantwortliche ist und wo sie eine Beschwerde einreichen können.<sup>154</sup>

### Misstrauen in den digitalen Zahlungsverkehr

Digital abgehängt zu werden, kann auch seinen Ursprung darin haben, neuen Technologien im Allgemeinen und digitalen Technologien im Zahlungsverkehr im Besonderen nicht zu vertrauen. Im Folgenden soll diese Hypothese untermauert werden, indem zunächst auf die inhaltliche Bedeutung von Vertrauen und damit zusammenhängend auf unterschiedliche Vertrauensformen ganz allgemein eingegangen wird. Darauf aufbauend wird der Bezug zu digitalen Bezahlmethoden hergestellt und es werden Möglichkeiten einer erleichterten Vertrauensbildung aufgezeigt.

Vertrauen kann definiert werden als „eine Erwartung des Vertrauensgebers, dass seine einseitige Vorleistung in der Tauschbeziehung vom Vertrauensnehmer nicht ausgebeutet wird, obwohl dieser durch die Wahl der Ausbeutungsstrategie einen höheren Nutzen erreichen könnte“.<sup>155</sup> Vertrauen zwischen Einzelpersonen oder Organisationen bedeutet, dass die Vertrauenden einer anderen Person oder Organisation eine Aufgabe anvertrauen, obwohl dabei die Möglichkeit eines Scheiterns oder sogar opportunistischen Verhaltens besteht.<sup>156</sup> Dadurch vereinfachen Vertrauende für sich die oft komplexen Anforderungen,<sup>157</sup> etwa bei einer Finanzdienstleistung, und verringern die Unsicherheit darüber, wie die andere Partei reagieren wird. Dieser Schritt wird als „leap of faith“ bezeichnet, bei dem die Unsicherheit („fuzzy uncertainty“) in ein subjektiv kalkulierbares Risiko umgewandelt wird.<sup>158</sup> Die Vertrauenden hoffen, dass die andere Seite die Erwartungen erfüllt, nehmen aber gleichzeitig das Risiko in Kauf, dass dies nicht geschieht.

Im Zusammenhang mit der Beantwortung der Frage, warum vertraut wird, unterscheidet die soziologische Vertrauensforschung unterschiedliche Vertrauensformen.<sup>159</sup> Diese existieren allerdings nicht unabhängig voneinander, sondern ergänzen sich. Personelles und institutionelles Vertrauen wurden dabei in neuerer Zeit durch technologisches Vertrauen erweitert.

Personelles Vertrauen, also das Vertrauen zu Personen, beschreibt die ursprünglichste Form, die Vertrauen annehmen kann.<sup>160</sup> Voraussetzung dafür, dass eine Person einer anderen vertraut, ist deren wahrgenommene Kompetenz, Integrität und das Wohlwollen,<sup>161</sup> alles Eigenschaften der zu vertrauenden Person, weshalb in der Literatur auch von ‚characteristic-based trust‘ gesprochen

---

<sup>154</sup> BEUC (2020), S. 4.

<sup>155</sup> Beckert (20002).

<sup>156</sup> Bachmann/Inkpen (2011).

<sup>157</sup> Luhmann (1979).

<sup>158</sup> Möllering (2006).

<sup>159</sup> Shapiro (1987).

<sup>160</sup> Luhmann (1979).

<sup>161</sup> Currall (1992); Sako (1992).

wird.<sup>162</sup> Vertrauen ist dabei keine spontane Entscheidung, sondern muss verdient werden.<sup>163</sup> Bevor eine Beziehung etabliert, also z. B. ein Vertrag geschlossen wird, muss es Vertrauensgeber:innen möglich sein, eine erste Einschätzung der Kompetenz, Integrität und des Wohlwollens der anderen Partei geben zu können. Typischerweise startet eine persönliche Vertrauensbeziehung mit weniger umfangreichen Transaktionen, die nur ein geringes Maß an Vertrauen erfordern und damit auch nur ein geringes Risiko aufweisen. Bei Erfolg werden diese Transaktionen sukzessive ausgeweitet.<sup>164</sup>

Arbeits- und damit Aufgabenteilung zwischen den Mitgliedern einer Gesellschaft schafft komplexe Strukturen von Abhängigkeitsbeziehungen, die nicht in persönliche Beziehungsstrukturen eingebettet sind. Für diese Beziehungsstrukturen spielt institutionelles Vertrauen eine entscheidende Rolle.<sup>165</sup> Unter Institutionen werden Verhaltensregeln, deren Einhaltung in der Gesellschaft auf breiter Akzeptanz beruhen, verstanden.<sup>166</sup> Dazu gehören nicht nur das geschriebene Recht, sondern auch bestimmte Routinen und Praktiken, aber auch soziale und ethische Normen, die außerhalb des geltenden Rechts dem individuellen Handeln Beschränkungen auferlegen und deren Verletzung Sanktionen zur Folge hat. Zum Beispiel wickeln Verbraucher:innen Finanzdienstleistungen mit unterschiedlichen Finanzunternehmen ab. Zwar existiert auch hier grundsätzlich die Möglichkeit, persönliche Vertrauensbeziehungen mit einzelnen Mitarbeiter:innen aufzubauen, allerdings werden deren Entscheidungskompetenzen als auch deren Anreizstruktur eng durch die unternehmerische Governance- Struktur geprägt, die sich wiederum in Regeln manifestiert, die zu befolgen von der Unternehmensleitung erwartet wird.<sup>167</sup>

Informelle ebenso wie formelle Regeln haben für die Vertrauensbildung eine große Bedeutung, gerade, wenn sie über einen längeren Zeithorizont praktiziert werden und damit ein stabiles und bekanntes Umfeld schaffen (,familiarity‘ im Luhmannschen Sinne).<sup>168</sup> Wohlbemerkt stellen derartige Institutionen kein Substitut für Vertrauen dar, eben weil sie nicht in der Lage sind, in der jeweiligen spezifischen Situation absolute Sicherheit über das Verhalten des Vertragspartners zu schaffen. Sie sind aber in der Lage, das Risiko, das Vertrauensgeber:innen eingehen, zu senken. Bestätigt wird dies durch empirische Forschungsarbeiten.<sup>169</sup> Diese Beschränkung des Risikos geschieht durch den Sanktionsmechanismus, der allen Regeln innewohnt und mit dem eine ,Non-Compliance‘ bestraft wird, nicht allein aufgrund von Gerichtsverfahren, sondern auch der Verlust von Reputation spielt eine Rolle.<sup>170</sup> Insofern übernehmen Institutionen die Rolle einer dritten Partei mit der Funktion, Vertrauensmissbrauch zu verhindern. Deshalb werden Institutionen als ,guardians of trust‘ bezeichnet.<sup>171</sup>

---

<sup>162</sup> Shapiro (1987).

<sup>163</sup> Jalava (2006).

<sup>164</sup> Sako (1992).

<sup>165</sup> Zucker (1986).

<sup>166</sup> Giddens (1984).

<sup>167</sup> Zucker (1986).

<sup>168</sup> Bachmann/Inkpen (2011).

<sup>169</sup> S. z. B. Arrighetti u. a. (1997).

<sup>170</sup> Bachmann/Zaheer (2006).

<sup>171</sup> Shapiro (1987).

Allerdings entfalten Institutionen ihre vertrauensfördernde Wirkung nur, wenn auch ihnen selbst eine Vertrauenswürdigkeit verliehen wird.<sup>172</sup> In diesem Zusammenhang wird in der einschlägigen Literatur auch von gesellschaftlichem Vertrauen gesprochen („societal trust“).<sup>173</sup> Insofern sind zwei Dimensionen des institutionellen Vertrauens zu beachten: erstens Vertrauen in die Institutionen an sich und zweitens deren Bedeutung für die Bildung von Vertrauen in sozialen und ökonomischen Interaktionsprozessen.

Beim technologischen Vertrauen rückt der Fokus eher auf die Funktionalität von Techniken. Es bestand lange Konsens unter Vertrauensforscher:innen darüber, dass die Möglichkeit und Neigung zu opportunistischem Verhalten des Vertrauensnehmers eine konstitutive Bedingung für Vertrauen darstellt.<sup>174</sup> Auf der Grundlage der Einsicht, dass einer Technologie grundsätzlich die Möglichkeit und Neigung zu opportunistischem Verhalten fehlt, richten Arbeiten, die sich mit technologischem Vertrauen befassen, den Blick auf die eigentlich zentrale Eigenschaft von Vertrauensbeziehungen, nämlich die Vulnerabilität des Vertrauensgebers. Diese Vulnerabilität setzt aber die Möglichkeit von opportunistischem Verhalten durch den Vertrauensgeber nicht zwingend voraus, vielmehr spielt die Abhängigkeit vom Funktionieren der Technologie die entscheidende Rolle.<sup>175</sup> Welche Unterschiede es zwischen dem Vertrauen in Personen und dem Vertrauen in Technologie gibt, verdeutlicht am Beispiel von IT, wird in einer Studie<sup>176</sup> anhand des Vertrauensbildungsprozesses verdeutlicht. Unterschieden wird zwischen anfänglichem Vertrauen, also Vertrauen vor Nutzung der Technologie und wissensbasiertem Vertrauen, das durch wiederholte Nutzung entsteht.<sup>177</sup> Sie verweisen dabei auf zahlreiche Studien,<sup>178</sup> die belegen, dass es bei der Bildung von technologischem Vertrauen vor allem um Wissenslücken im Hinblick auf die Nutzung von neuen Technologien geht.

Technologisches Vertrauen wird mit Hilfe von drei Komponenten operationalisiert: Erstens einer grundsätzlichen Einstellung zu Technologie, einem institutionellen Vertrauen in Technologie und Vertrauen in eine ganz bestimmte Technologie. Damit stellen die Studien heraus, dass auch im Falle von technologischem Vertrauen Institutionen eine wichtige Rolle spielen, und zwar in dem Sinne, dass eine grundsätzliche Bereitschaft, Technologie zu vertrauen, institutionelles Vertrauen beeinflusst und über diesen Weg das Vertrauen in eine bestimmte Technologie fördert.

Kritisch einzuschätzen ist allerdings die Auffassung, die Möglichkeit von opportunistischem Verhalten spiele bei technologischem Vertrauen keine Rolle.<sup>179</sup> Tatsächlich zeigen Studien, dass Menschen auf Computer genauso reagieren wie auf Personen.<sup>180</sup> Zudem sind sich Verbraucher:innen durchaus bewusst, dass sie Informationen ins Netz geben, über deren Nutzung sie in der Regel keine Kontrolle haben. Und schließlich ist an die immer zahlreicher werdenden Betrugsfälle zu erinnern. Die Nutzung von Informationstechnologien erhöht also aus Sicht von

---

<sup>172</sup> Child/Möllering (2003).

<sup>173</sup> Barber (1983).

<sup>174</sup> Aufbauend auf Luhmann (1979).

<sup>175</sup> McKnight u. a. (2011).

<sup>176</sup> McKnight u. a. (2011).

<sup>177</sup> McKnight u. a. (2011).

<sup>178</sup> Pavlou (2003); Lippert (2007); Thatcher u. a. (2010).

<sup>179</sup> McKnight u. a. (2011).

<sup>180</sup> Nass/Moon (2000).

**Digital Abgehängt**

Verbraucher:innen durchaus die Unsicherheit über die Vertrauenswürdigkeit derjenigen, an die sie bestimmte Aufgaben, z. B. Zahlungsvorgänge delegieren. Welche Rolle dies für die Akzeptanz bzw. Nichtakzeptanz von digitalen Bezahlmethoden spielt, ist Gegenstand des folgenden Abschnitts.

Die Entwicklung unterschiedlicher Formen des digitalen Zahlungsverkehrs wird sowohl von einem Zurückdrängen des personellen und dem Anwachsen notwendigen institutionellen Vertrauens begleitet als auch von einem steigenden Anteil eines erforderlichen technologischen Vertrauens. Auch die breite Verwendung von Bargeld basiert auf einem dichten Geflecht von Institutionen, denen vertraut werden muss und die ihrerseits ein Vertrauen in die Eignung von Geldscheinen und Münzen fördern. Anders als beim digitalen Zahlungsverkehr sind diese Institutionen etabliert und haben sich im Hinblick auf eine zuverlässige Bargeldversorgung als stabil erwiesen. Das erforderliche Vertrauen wurde also bereits verdient. Der bargeldlose Zahlungsverkehr zeichnet sich im Unterschied zur Zahlung mit Geldscheinen und Münzen dadurch aus, dass anstelle der Zentralbank ausschließlich private Finanzdienstleister als Vertrauensnehmer agieren und dabei in zunehmendem Maße persönliche Beziehungen entfallen. Zahlungsaufträge werden an ein Gegenüber vergeben, das man in der Regel nicht kennt.

Überlässt man dennoch diesem Gegenüber die Erledigung eines Zahlungsauftrags, so setzt dies ein Vertrauen voraus, das notwendigerweise stark auf Institutionen aufbaut, die einen Schutz vor Missbrauch intendieren und darin in den Augen der Auftraggeber:innen auch vertrauenswürdig sind. Beispiele sind gesetzliche Regulierungen bezüglich Transparenz und Haftung bei Fehlbuchungen und Verlust der Bank- oder Kreditkarte, aber auch Selbstregulierungen in Form von Verhaltenskodizes. Die Vertrauenswürdigkeit dieses institutionellen Umfelds zeigt sich dabei in der Art und Weise, wie die einzelnen Regelungen umgesetzt werden. Defizite in der praktischen Umsetzung können schnell zu einem Vertrauensverlust in gesetzliche Regulierungen sowie in Selbstregulierungen durch die Finanzanbieter führen, wie die Finanzkrise gezeigt hat. Dass dies auch den Zahlungsverkehr erreichen kann, zeigt die Entstehung von Bitcoin als unmittelbare Reaktion darauf. Ein funktionierender bargeldloser Zahlungsverkehr setzt somit voraus, dass es gesetzliche (formelle) bzw. informelle Regeln gibt, die in der Praxis auch umgesetzt werden und die effektiv sind. Ein dadurch verdientes institutionelles Vertrauen ermöglicht eine breite Akzeptanz von bargeldlosen Zahlungen, da Sender wie Empfänger allenfalls ein tragbares Restrisiko mit bargeldloser Zahlung verbinden.

Der Übergang zum digitalen Zahlungsverkehr stellt für Verbraucher:innen allerdings eine zusätzliche Herausforderung in Bezug auf eine steigende Komplexität dar. Bargeldloser Zahlungsverkehr war zunächst sehr überschaubar. Außer der Überweisung per Formular und der Bezahlung mit Scheck und Karte gab es keine Alternativen. Dagegen ändern sich die Bezahlalternativen nahezu ständig und die Komplexität zeigt sich in unterschiedlichen Funktionsweisen der Apps (mobile Bezahlssysteme) oder Kartenlesegeräte ebenso wie in den Anwendungsvorschriften. Vor allem aber rückt der Bezug zum (vertrauten) Finanzdienstleister immer mehr in den Hintergrund, wodurch ein wahrgenommenes Risiko bezüglich der Sicherheit des Zahlungsvorgangs erhöht werden dürfte. Weitere Unsicherheiten gesellen sich dazu: Man gibt Informationen ins Netz und weiß nicht, wo diese letztendlich landen. Wer garantiert, dass eine Zahlung auch korrekt ankommt, dass das Konto nicht gehackt wird, wer garantiert Cybersicherheit?

Cyberkriminalität zu Lasten von Verbraucher:innen hat laut Beschwerdestatistik der Verbraucherzentralen 2023 stark zugenommen. So verwenden Kriminelle verschiedene Methoden

wie Phishing-Mails, Spoofing-Anrufe<sup>181</sup> und Links zu gefälschten Webseiten, um an die Bankverbindung und Zahlungskarten von Verbraucher:innen zu kommen. So verdoppelten sich 2023 im Vergleich zum Vorjahr die Verbraucherbeschwerden zu Cyberkriminalität und Finanzdienstleistungen in den Verbraucherzentralen. Dabei wenden sich Verbraucher:innen in der Regel nur dann an die Verbraucherzentralen, wenn ihre Bank oder Sparkasse Schäden zunächst nicht reguliert und die Geschädigten auf dem Verlust sitzen bleiben.<sup>182</sup> Auch eine Studie des Digitalverbands bitkom<sup>183</sup> bestätigt die Entwicklung. 67 Prozent der Befragten wurden im Jahr 2023 Opfer von Cyberkriminalität, 13 Prozent wurden Opfer von Betrug beim Online-Banking oder ihre Kontodaten wurden ausgespäht. Im vorherigen Jahr waren noch 75 Prozent von Cyberkriminalität betroffen gewesen.<sup>184</sup>

Auch erste empirische Erkenntnisse unterstützen die Barriere des mangelnden Vertrauens in digitale Zahlungsmethoden. Gefragt wurden 851 potenzielle Nutzer:innen von mobilen Bezahlsystemen in Australien danach, was sie am meisten davon abhält, diese Systeme tatsächlich zu nutzen. Ein Mangel an anfänglichem Vertrauen stellte sich als wichtigste Hürde heraus. Zugleich verweisen die Resultate auf eine positive Korrelation zwischen wahrgenommener Qualität der bereitgestellten Informationen, wahrgenommener Service-Qualität und wahrgenommener Systemstabilität und anfänglichem Vertrauen in mobile Bezahlsysteme. Ein anfängliches Vertrauen in mobile Bezahlsysteme fördere zudem die wahrgenommene Anwenderfreundlichkeit und Vorteilhaftigkeit. Auch verweisen zahlreiche Studien auf der Grundlage von empirischen Analysen auf die Notwendigkeit von institutionenbasiertem Vertrauen für die Nutzung mobiler Bezahlsysteme. Vor allem komme einem effektiven Rechtsrahmen, einer effektiven Regulierung und einer funktionierenden digitalen Infrastruktur dabei eine hohe Bedeutung zu.

Tatsächlich zählen zunehmende Betrugsfälle im Netz zu den wichtigsten Gründen, die das Vertrauen der Verbraucher:innen im digitalen Zahlungsverkehr negativ beeinflussen.<sup>185</sup> Phishing und andere Betrugsformen haben sich zu ernsthaften Bedrohungen für die Sicherheit persönlicher Daten und damit auch für das Guthaben auf dem Zahlungskonto vieler Verbraucher:innen entwickelt. Kriminelle nutzen raffinierte Taktiken, um Zahlungsdienstnutzer:innen, also die Bankkund:innen, in die Falle zu locken – sei es durch Diebstahl von Zahlungskarten, gefälschte E-Mails, täuschend echte Webseiten oder die Vortäuschung von Anrufen durch Bankmitarbeiter:innen. Schon durch einen kleinen Moment der Unachtsamkeit können hier teils beträchtliche Schadenssummen entstehen. Die Täter sind hierbei selten zu ermitteln, sodass ein Erstattungsanspruch gegen die Bank für die meisten Betroffenen als einzige Möglichkeit der Schadensbeseitigung bleibt. Je nachdem, wie die Umstände des konkreten Einzelfalls gelagert sind, kann dem Anspruch gegen die Bank auf Wiedergutschrift des verlorenen Betrages ein eigener Anspruch der Bank gegen Bankkund:innen aufgrund von grober Fahrlässigkeit entgegenstehen. Diese Beispiele weisen einmal mehr auf die Notwendigkeit funktionierender, d. h. schützender

---

<sup>181</sup> Telefonanrufe, bei denen der Anrufer absichtlich eine falsche Telefonnummer oder Identität auf dem Display des Empfängers anzeigt.

<sup>182</sup> Verbraucherzentrale Bundesverband e.V. (09.05.2024), S. 5.

<sup>183</sup> Befragt wurden unter 1.018 Personen in Deutschland ab 16 Jahren, die das Internet nutzen.

<sup>184</sup> Bitkom Research (2024), o.S.

<sup>185</sup> Ozili (2020), S. 8.

Institutionen hin. Gerade rechtlichen Regelungen kommt hierbei Bedeutung zu, allerdings nur dann, wenn sie klar und in sich konsistent sind.

Studien zeigen zudem, dass Vertrauen in Institutionen des digitalen Zahlungssystems bei vulnerablen Verbrauchergruppen niedriger ist. So deuten Ergebnisse einer Studie aus den Niederlanden darauf hin, dass Befragte mit geringen digitalen Kenntnissen oder Personen, die finanzielle Schwierigkeiten haben, ein unterdurchschnittliches Maß an Vertrauen sowohl in das Zahlungssystem als auch in die eigene Bank haben. Ebenso findet die Studie, dass blinde oder sehbehinderte Personen und Personen mit eingeschränkter oder fehlender Handfunktion weniger Vertrauen in das Zahlungssystem haben als Personen, die nicht zu einer dieser Gruppen gehören.<sup>186</sup>

Zusammenfassend kann festgehalten werden, dass mangelndes Vertrauen in digitale Bezahlssysteme ein Hemmnis darstellt, sie auch zu nutzen. Dies trifft insbesondere auf Gesellschaften mit einer hohen Abneigung gegen Unsicherheit zu. Eine damit zusammenhängende Vermeidung, digitale Bezahlssysteme zu nutzen, führt dann auch dazu, im Zuge des technologischen Fortschritts auf diesem Gebiet digital abgehängt zu werden. Gleichzeitig zeigen die zitierten Studien aber auch, dass Institutionen, also sanktionsbehaftete Regelwerke mit der Intention, Unsicherheit in der virtuellen Welt zu senken, vertrauensfördernd wirken. Dabei gilt es, das Ausmaß der „Angst vor dem Neuen“ hinsichtlich der Eingriffsstärke und Sanktionsheftigkeit zu berücksichtigen.

Die vertrauensbildende Funktion kann die Regulierung zu Betrugsfällen allerdings nur eingeschränkt einnehmen. Obwohl die rechtliche Ausgangslage hierbei auf den ersten Blick recht klar zu sein scheint, ist sie im Detail jedoch in Abgrenzungsfragen des Einzelfalls oftmals schwierig zu handhaben. Ein Erstattungsanspruch von Zahlungsdienstnutzer:innen gegen die Bank ergibt sich aus § 675u S. 2 BGB. Demnach ist der Zahlungsdienstleister, also die Bank, im Fall eines nicht autorisierten Zahlungsvorgangs verpflichtet, Bankkund:innen den Zahlungsbetrag unverzüglich zu erstatten bzw. das Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte. Wie oben erläutert, ist ein Zahlungsvorgang nur dann autorisiert, wenn Bankkund:innen diesem zugestimmt haben (§ 675j Abs. 1 S. 1 BGB). In Betrugsfällen des digitalen Zahlungsverkehrs liegt keine wirksame Autorisierung durch die Bankkund:innen vor, sodass ein Anspruch auf Wiedergutschrift gegen die Bank aus § 675u Satz 2 BGB grundsätzlich in Betracht käme.

Vielfach kann die Bank dem Anspruch von Bankkund:innen auf Wiedergutschrift jedoch ihren eigenen Schadensersatzanspruch in gleicher Höhe aus § 675v Abs. 3 BGB entgegenhalten. Voraussetzung für den entgegengesetzten Anspruch der Bank aus § 675v Abs. 3 BGB ist, dass die Bankkund:innen entweder

- in betrügerischer Absicht gehandelt haben, oder aber
- den Schaden durch eine vorsätzliche oder grob fahrlässige Verletzung
- einer oder mehrerer der in § 675l Abs. 1 BGB geregelten Sorgfaltspflichten oder
- vereinbarter Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments herbeigeführt haben.

---

<sup>186</sup> Broekhoff u. a. (2024), S. 104.

Relevant ist meist die grob fahrlässige Verletzung von Sorgfaltspflichten (§ 675l BGB). Wie oben erläutert, verpflichtet die Vorschrift die Zahlungsdienstnutzer:innen dazu, alle zumutbaren Vorkehrungen zu treffen, um das Zahlungsinstrument und die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen sowie den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Zahlungsinstruments unverzüglich anzuzeigen, nachdem sie hiervon Kenntnis erlangen (§ 675l Abs. 1 BGB). Für die Zahlungsvorgänge nach einer Anzeige tragen die Zahlungsdienstnutzer:innen kein Haftungsrisiko mehr (§ 675v Abs. 5 S. 1 BGB).

In der Rechtsprechung wird die grob fahrlässige Verletzung der Sorgfaltspflichten regelmäßig bejaht. Vor dem Hintergrund, dass die Identifizierung von unfairen Praktiken immer schwieriger wird, ist diese Rechtsprechung zu kritisieren. Eine entsprechende Studie des vzbv zeigt, dass es Verbraucher:innen kaum möglich ist, betrügerische Angriffe zu identifizieren. So äußerten 57 Prozent der Befragten einen Betrugsverdacht bei betrügerischen Fallkonstellationen, allerdings auch bei 38 Prozent der Fallkonstellationen ohne betrügerisches Anbieterverhalten.<sup>187</sup> In der Rechtsprechung haben sich zwei unterschiedliche Fallgruppen herauskristallisiert: Die Speicherung der Karten-PIN auf einem Zettel, der zusammen mit der Zahlungskarte aufbewahrt wird, und die Weitergabe der PushTAN an unbefugte Dritte.<sup>188</sup>

In der ersten Fallgruppe handelt es sich um Fälle, in denen nach dem Verlust oder Diebstahl einer Bankkarte unter Verwendung der Originalkarte und der richtigen PIN durch unbefugte Dritte Geld abgehoben wird. In diesen Fällen gehen Gerichte davon aus, dass der typische Geschehensablauf nach der Lebenserfahrung darauf schließen lässt (der Beweis des ersten Anscheins oder Anscheinsbeweis), dass die PIN in pflichtwidriger Weise zusammen mit der Karte aufbewahrt wurde.<sup>189</sup> Zur Erschütterung dieses Anscheinsbeweises ist es erforderlich, dass die Bankkund:innen erfolgreich einen atypischen Geschehensverlauf glaubhaft machen können, durch den die Betrüger Kenntnis von der PIN erlangen konnten. Hierzu müssen konkrete Tatsachen dargelegt werden, die die ernsthafte Möglichkeit eines atypischen Geschehensverlaufs, wie etwa einer Sicherheitslücke oder eines professionellen Ausspähens wenigstens nahelegen.<sup>190</sup>

In der Praxis berufen sich die Gerichte dabei auf ein BGH-Urteil aus 2011.<sup>191</sup> Diesem Urteil lag ein Fall aus 2009 zugrunde, bei dem die Zahlungskarte entwendet und damit unter der Verwendung der PIN mehrmals Geld abgehoben wurde. Es steht außer Zweifel, dass sich die durch die Betrüger eingesetzte Technik mittlerweile erheblich weiterentwickelt hat. Obwohl die Banken die Technik, womit die Zahlungskarten ausgestattet sind (Chipkartentechnik), als sicher einstufen, ist es zweifelhaft, ob sie in der Lage ist, Geldabhebung ohne PIN vollkommen zu verhindern. In der Praxis treten immer mehr Fälle auf, bei denen es den Betrügern auch ohne Kenntnis der PIN möglich ist, bei bloßem Besitz der Zahlungskarte Geld abzuheben. Ob sie dafür die PIN technisch auslesen oder den Geldautomaten z. B. durch das Aufspielen einer Malware manipulieren, ist zwar nicht bekannt,

---

<sup>187</sup> Verbraucherzentrale Bundesverband e.V. (09.05.2024), S. 1.

<sup>188</sup> Die letztere Fallgruppe wird bereits im Erwägungsgrund 72 der PSD2 erwähnt.

<sup>189</sup> OLG Dresden, Urt. v. 13.03.2024 – 5 U 589/23, BKR 2024, 826; BGH, Urt. v. 29.11.2011 – XI ZR 370/10, MMR 2012, 225.

<sup>190</sup> OLG Dresden, Urt. v. 13.03.2024 – 5 U 589/23, BKR 2024, 826 (Leitsatz).

<sup>191</sup> BGH, Urt. v. 29.11.2011 – XI ZR 370/10, VuR 2012, 105.

aber nach den rasanten technischen Entwicklungen seit dem BGH-Urteil aus 2011 doch plausibel.<sup>192</sup>

Die zweite Fallgruppe, die Gerichte immer wieder beschäftigt, ist der PushTAN-Betrug. Dabei rufen Betrüger die Bankkund:innen an und geben sich als Mitarbeiter:innen ihrer Bank aus. In der Regel sind die Betrüger hierbei bereits mithilfe von Phishing oder Hacking in den Besitz der Online-Banking-Zugangsdaten der Betroffenen gelangt. Im Laufe des Telefongesprächs fordern die vermeintlichen Bankmitarbeiter:innen die Bankkund:innen dann zur mündlichen Weitergabe von Sicherheitsmerkmalen wie etwa TANs auf, um Überweisungen zu tätigen. Leisten die Bankkund:innen dem Folge, gehen die Gerichte in der Regel von einer grob fahrlässigen Pflichtverletzung seitens der Bankkund:innen aus.<sup>193</sup> Das gilt auch, wenn unter Anleitung der Anrufer:innen etwa eine PushTAN bestätigt wird.<sup>194</sup> Begründet wird dies einerseits damit, dass es sich hierbei um eine bekannte Betrugsmasche handle, vor der seit vielen Jahren in Medien und durch die Banken selbst gewarnt werde. Andererseits wird angeführt, dass die fernmündliche Weitergabe solcher Sicherheitsmerkmale oder auch die Bestätigung einer PushTAN, aus deren Text eindeutig etwa der Transfer von Geld auf ein fremdes Konto hervorgehe, in grob fahrlässiger Weise pflichtwidrig sei.<sup>195</sup> Abweichend hiervon wird nur in Ausnahmefällen zugunsten der Bankkund:innen entschieden, wenn etwa der Freigabetext der PushTAN so uneindeutig formuliert ist, dass für die Bankkund:innen nicht ersichtlich ist, was genau damit freigegeben wird.<sup>196</sup>

In der Praxis bleibt in Betrugsfällen vor allem die unverzügliche Erstattungspflicht des Zahlungsdienstleisters außer Acht. Die Zahlungsdienstleister sind dazu verpflichtet, den Betrag, der Gegenstand eines nicht autorisierten Zahlungsvorgangs war, unverzüglich zu erstatten (§ 675u S. 2 BGB). Die Erstattung muss spätestens am nächsten Geschäftstag nach Anzeige der Zahlungsdienstnutzer:innen oder anderweitiger Kenntniserlangung des Zahlungsdienstleisters erfolgen (§ 675u S. 3). Die einzige Ausnahme zu dieser Pflicht besteht beim betrügerischen Verhalten von Zahlungsdienstnutzer:innen<sup>197</sup> und nur dann, wenn der Zahlungsdienstleister die berechtigten Gründe für seinen Verdacht einer zuständigen Behörde schriftlich mitgeteilt hat.<sup>198</sup> Anstatt den Betrag des nicht autorisierten Zahlungsvorgangs unverzüglich zu erstatten, machen die Banken unverzüglich geltend, der/die Zahlungsdienstnutzer:in habe ihre Sorgfaltspflicht aus § 675l BGB grob fahrlässig verletzt.

Zum Teil können die Bankkund:innen in Verdachtsfällen ihre Bank überhaupt nicht oder nicht schnell genug erreichen oder die Banken reagieren zu langsam auf eine Anzeige.<sup>199</sup> Gemäß § 675m Abs. 1 Nr. 3 BGB (Art. 70 Abs. 1 lit. d PSD2) haben die Zahlungsdienstleister sicherzustellen, dass die Zahlungsdienstnutzer:innen durch geeignete Mittel jederzeit die Möglichkeit haben, die

---

<sup>192</sup> Fohrer (2024), S. 8.

<sup>193</sup> OLG Bremen, Beschl. v. 15.04.2024 – 1 U 47/23, BKR 2024, 729; OLG Köln, Beschl. v. 19.10.2023 – 13 U 42/23, GRUR-RS 2023, 33010; LG Lübeck, Urt. v. 03.01.2024 – 3 O 83/23, BKR 2024, 494.

<sup>194</sup> OLG Frankfurt, Urt. v. 06.12.2023 – 3 U 3/23, MMR 2024, 497.

<sup>195</sup> OLG Köln, Beschl. v. 19.10.2023 – 13 U 42/23, GRUR-RS 2023, 33010.

<sup>196</sup> LG Köln, Urt. v. 08.01.2024 – 22 O 43/23, BKR 2024, 339.

<sup>197</sup> Erwägungsgrund 71 PSD2.

<sup>198</sup> Beispielsweise Staatsanwaltschaft, Polizei oder die BaFin im Rahmen des ZAG, s. Zetzsche, in: Säcker u. a. (2023), BGB § 675u Rn. 43.

<sup>199</sup> Verein für Verbraucherrechte, Pressemitteilung vom 12. November 2024, Verbraucher müssen bei ihren Bankkonten vor kriminellen Handlungen besser geschützt werden.

unverzögliche Anzeige eines Verlusts, Diebstahls, der missbräuchlichen Verwendung oder der sonstigen nicht autorisierten Nutzung eines Zahlungsinstruments vorzunehmen. Kommt der Zahlungsdienstleister dieser Pflicht nicht nach, sind die Zahlungsdienstnutzer:innen lediglich von ihrer Haftung nach § 675v Abs. 1 BGB befreit. § 675v Abs. 1 BGB sieht vor, dass die Zahlungsdienstnutzer:innen bis zum Betrag von 50 Euro haften, falls die nicht autorisierten Zahlungsvorgänge auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Zahlungsinstruments beruhen. Insofern sind die Zahlungsdienstnutzer:innen von ihrer Ersatzpflicht im Falle einer Schadensverursachung durch grob fahrlässige Verletzung ihrer Schutzpflichten (§ 675v Abs. 3 Nr. 2 BGB) nicht befreit. Doch wenn die Zahlungsdienstnutzer:innen ihre Bank nicht schnell erreichen können bzw. wenn die Bank nicht schnell genug auf die Anzeige reagiert und die Kontosperrung oder die Kontaktaufnahme mit der Empfängerbank nicht schnell genug erfolgt, erhöht sich die Schadenssumme erheblich und zusammen mit dem Vorwurf der groben Fahrlässigkeit bleiben die Bankkund:innen auf dem Schaden sitzen.

Gemäß § 675z S. 1 BGB sind die Ansprüche von Zahlungsdienstnutzer:innen gegen die Bank im Falle eines nicht autorisierten Zahlungsvorgangs in §§ 675 u. f. BGB abschließend geregelt. Dies hat zur Folge, dass die Zahlungsdienstnutzer:innen keinen Schadensersatz in Verbindung mit einer Verletzung der Schutzpflicht geltend machen können (§§ 280 Abs. 1 i. V. m. 241 Abs. 2 BGB).<sup>200</sup> Eine solche Schutzpflicht<sup>201</sup> könnte sich aus Art. 2 SKA-DVO ergeben.<sup>202</sup> Dementsprechend verfügen die Zahlungsdienstleister über Transaktionsüberwachungsmechanismen, die auf der Analyse von Zahlungsvorgängen der Zahlungsdienstnutzer:innen basieren und ihnen die Erkennung nicht autorisierter oder betrügerischer Zahlungsvorgänge ermöglichen (Art. 2 Abs. 1 SKA-DVO). Diese Überwachungsmechanismen müssen u. a. den Betrag eines jeden Zahlungsvorgangs und die bekannten Betrugsszenarien bei der Erbringung von Zahlungsdienstleistungen einbeziehen (Art. 2 Abs. 2 SKA-DVO). Die Überwachungsmechanismen ermöglichen die Transaktionsrisikoanalyse gem. Art. 18 SKA-DVO und darauf basierend den Verzicht auf eine starke Kundenauthentifizierung bei niedrigem Risiko.

Gleichwohl kann die Verletzung der Schutzpflichten das Mitverschulden (§ 254 BGB) der Bank begründen. Dazu gehören etwa die unzureichende Beobachtung neuerlicher Betrugsmethoden, mangelnde Reaktionen auf neue Gefährdungslagen, eine mangelnde allgemeine Systemsicherheit oder die unzulängliche Aktualisierung eingesetzter Systeme.<sup>203</sup> Die Bank trifft auch ein Verschulden, wenn etwa betrügerische Abbuchungen über das vereinbarte Verfügungslimit hinaus oder trotz der

---

<sup>200</sup> Zetzsche, in: Säcker u. a. (2023), BGB § 675z Rn. 5; s. dagegen Zahrt (2024b), S. 594 ff.

<sup>201</sup> Zusätzlich zu den in § 675m BGB explizit genannten Schutzpflichten. Zu diesen Pflichten gehört unter anderem, dass die Bank im Rahmen ihrer Möglichkeiten dafür Sorge zu tragen hat, dass die personalisierten Sicherheitsmerkmale des Zahlungsinstruments ausschließlich dem/der Kund:in zugänglich sind. Daneben trifft die Bank etwa die Pflicht, den Kund:innen nicht unaufgefordert Zahlungsinstrumente zuzusenden, sicherzustellen, dass die Kund:innen die Möglichkeit haben, sicherheitsrelevante Vorfälle kostenfrei anzuzeigen und jede Nutzung des Zahlungsinstruments nach einer solchen Anzeige zu verhindern.

<sup>202</sup> Ob aufsichtsrechtliche Pflichten eine Pflicht zum Schutz der Kund:innen begründen können, wird in der Literatur und in der Rechtsprechung größtenteils verneint, s. z. B. OLG Bremen, Beschluss v. 30.08.2024 – 1 U 32/24, BeckRS 2024, 29116 und Beschluss v. 15.04.2024 – 1 U 47/23, BeckRS 2024, 11361; LG Heilbronn, Urteil vom 27.08.2027 – Bm 6 O 103/24, BeckRS 2024, 31545; Zahrt (2024b), S. 598. Lediglich in einem Urteil hat das Kammergericht Berlin daraus die Pflicht abgeleitet, „auffällige Zahlungsaufträge zu erkennen, um auf diese Weise frühzeitig die Ausführung verdächtiger Zahlungen zu verhindern“, s. KG, Beschluss vom 4.9.2024 – 4 U 79/23, Rn. 28, BeckRS 2024, 33664. In der Literatur wird auch die Auffassung vertreten, dass die aufsichtsrechtlichen Pflichten bezüglich des Zahlungsverkehrs auf das Zivilrecht ausstrahlen, s. Linardatos (2021), S. 675. Zudem wird hervorgehoben, dass ein auf den Transaktionsüberwachungsmechanismen basierender Eingriff seitens der Bank einen Verstoß gegen das Verbot automatisierter Entscheidungen i. S. v. Art. 22 DSGVO darstellen würde, s. Zahrt (2024b), S. 599.

<sup>203</sup> Maihold, in: Ellenberger/Bunte (2022), § 33 Rn. 380.

Fehlerhaftigkeit des Authentifizierungsverfahrens ausgeführt werden.<sup>204</sup> In Ausnahmefällen kommt auch eine allgemeine Warn- und Hinweispflicht der Bank in Betracht.<sup>205</sup> Eine solche Pflicht ist dann anzunehmen, wenn der Bank bekannt ist oder im Einzelfall bekannt sein musste, dass die Ausführung eines Zahlungsvorgangs zur Schädigung von Zahlungsdienstnutzer:innen führt.<sup>206</sup> Dies ist insbesondere dann der Fall, wenn die Bank „auf Grund massiver Anhaltspunkte den Verdacht hegt, dass ein Kunde bei der Teilnahme am bargeldlosen Zahlungsverkehr durch eine Straftat einen anderen schädigen will.“<sup>207</sup> Da es den Banken möglich ist, durch Transaktionsüberwachungsmechanismen nicht autorisierte oder betrügerische Zahlungsvorgänge zu erkennen (Art. 2 Abs. 1 SKA-DVO), sind die Banken verpflichtet, die Interessen der Zahlungsdienstnutzer:innen zu schützen und sie vor einem eventuellen Betrugsfall zu warnen bzw. auf einen eventuellen Betrugsfall hinzuweisen. Unterlässt die Bank eine solche Warnung oder einen solchen Hinweis, was in der Praxis regelmäßig der Fall ist, begründet dies das Mitverschulden der Bank. Doch in der Praxis bleibt das Mitverschulden der Bank regelmäßig außer Acht.

### **Mangelnde Bereitschaft der Anbieter**

Verbraucherschutzrechtliche Regelungen bedeuten für die Kreditgeber Handlungsanweisungen bzw. Handlungsverbote, die das Streben der Finanzanbieter nach möglichst hohem betriebswirtschaftlichem Erfolg regelmäßig restringieren. Lassen gesetzliche Regelungen den Finanzanbietern Handlungsspielräume, so wird ihnen damit ein Anreiz gesetzt, diese zugunsten des betriebswirtschaftlichen Erfolges zu nutzen. Ein hoher Wettbewerb und höhere andere unvermeidbare Kosten könnten dann dazu führen, dass die Gesetzesabsicht nicht umgesetzt wird, wobei dies durchaus im gesetzlich zulässigen Rahmen bleibt.

Im Bereich des Zahlungsverkehrs zeigt sich eine solche fehlende Bereitschaft bei der Umsetzung der Regulierung deutlich beim Angebot des Basiskontos. Voraussetzung für die Teilnahme am digitalen Zahlungsverkehr ist ein Zahlungskonto, welches gesetzlich jedem zusteht, in der Praxis jedoch nicht jedem zugänglich ist. Da ein Zahlungskonto eine notwendige Bedingung für die Inanspruchnahme vieler Dienstleistungen ist, sollte der Zugang zu einem sogenannten Basiskonto gesetzlich sichergestellt werden.<sup>208</sup> Das Recht auf ein Zahlungskonto durch das Basiskonto wird vor allem für vulnerable Personengruppen nicht flächendeckend umgesetzt. Beispielsweise wird potenziellen Kund:innen das Basiskonto als Zahlungskonto selten proaktiv angeboten. In einer durch das *iff* durchgeführten Mystery Shopping-Erhebung wurde in ca. 50 Prozent der Fälle in der Filiale kein Basiskonto aktiv angeboten.<sup>209</sup>

## **2.4 Regulatorische Barrieren**

Neben der vertrauensbildenden Funktion kann Regulierung jedoch auch eine Barriere im Zugang zum Zahlungssystem darstellen. Das ist dann der Fall, wenn sie aufgrund strenger Anwendung zugangsfördernde Funktionen einschränkt, wie im Folgenden am Beispiel der Regulierung der

---

<sup>204</sup> Maihold, in: Ellenberger/Bunte (2022), § 33 Rn. 381 ff.

<sup>205</sup> Maihold, in: Ellenberger/Bunte (2022), § 33 Rn. 384.

<sup>206</sup> Vgl. BGH, Urt. v. 17.11.1975 – II ZR 70/74, BeckRS 1975, 31115150; Urt. v. 20.6.1963 – II ZR 185/61, NJW 1963, 1872.

<sup>207</sup> BGH, Urt. v. 6.5.2008 – XI ZR 56/07, NJW 2008, 2245.

<sup>208</sup> §§ 31 ff. ZKG, die Art. 16 ff. ZKRL in deutsches Recht umsetzt.

<sup>209</sup> Finance Watch (2024), S. 13.

Prävention von Geldwäsche und Terrorismusfinanzierung gezeigt wird. Das Geldwäschegesetz hat das Ziel, Geldwäsche und Terrorismusfinanzierung zu verhindern, indem Finanzströme stärker kontrolliert werden. Durch die Maßnahmen sollen Geldströme transparenter gemacht werden indem u. a. durch die eindeutige Identifikation von Geschäftspartner:innen sichergestellt wird, dass Transaktionen nicht anonym durchgeführt werden können.

Eine strenge Anwendung der notwendigen Kundenidentifizierung kann den Zugang zum Zahlungsverkehr erschweren. Wenn beispielsweise die Banken ihre Vertragspartner:innen identifizieren, um die Erfordernisse des GwG zu erfüllen, sollen dabei unterschiedliche Verfahren die Identifizierung von Personen ermöglichen, z. B. das Videoidentifizierungsverfahren oder PostIdent-Verfahren.<sup>210</sup> Für ein Videoidentifizierungsverfahren muss der Ausweis über holographische Merkmale verfügen.<sup>211</sup> Personengruppen, die beispielsweise aufgrund einer Behinderung das Haus nicht verlassen und sich daher mit einem neuen Lichtbildausweis mit holographischen Merkmalen nicht zu identifizieren vermögen, können somit am Zugang zum digitalen Zahlungsverkehr gehindert werden.<sup>212</sup> In diesem Fall kann die Bank zur Erfüllung ihrer Identifizierungspflicht (§ 10 Abs. 1 Nr. 1 GwG) andere hierfür geeignete Personen oder Unternehmen beauftragen (§ 17 Abs. 5-9 GwG). In diesem Zusammenhang ist die Deutsche Post AG mit dem PostIdent-Verfahren durch die BaFin als geeignetes Unternehmen bzw. als zulässiges Verfahren anerkannt.<sup>213</sup> Im Rahmen des PostIdent-Verfahrens kann die Identität von Personen nicht nur in der Filiale, sondern auch zu Hause bzw. in Pflegeheimen durch Postbot:innen entsprechend gesetzlicher Bestimmungen geprüft werden. Der Einsatz dieses Verfahrens hängt aber davon ab, ob die Bank die Post damit beauftragt.

Ein weiteres Beispiel stellen Fälle dar, in denen Menschen mit Einschränkungen keine Unterstützung durch andere Personen in Anspruch nehmen dürfen. Beispielsweise ist die Ausweisnummer auf persönlichen Ausweisdokumenten nicht mit dem Finger spürbar. Wenn sich daher eine sehbehinderte Person z. B. vor der Kontoeröffnung in einem Video-Identifizierungsverfahren identifizieren und einen Teil der Ausweisnummer vorlesen soll, ist sie dazu nicht in der Lage. Sobald eine andere Person zur Unterstützung dabei ist, darf das Verfahren nicht weitergeführt werden und wird daher unterbrochen. Damit sind sehbehinderte Menschendarauf angewiesen, sich ihre Ausweisnummer vor dem Video-Identifizierungsverfahren von einer sehenden Person vorlesen zu lassen, sodass sie diese in einer ihnen zugänglichen Art und Weise notieren können.<sup>214</sup>

Auch beim Zugang zum Basiskonto entsteht durch die strengen Anforderungen an die Kundenidentifizierung für vulnerable Personengruppen eine Barriere. In der Praxis fehlen Migrant:innen häufig die von vielen Banken für ein Basiskonto geforderten amtlichen Ausweisdokumente.<sup>215</sup> Obdachlosen wiederum fehlt eine persönliche Wohnadresse, die im

---

<sup>210</sup> BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, S. 40 ff., 76 ff.

<sup>211</sup> B.V und B.VI BaFin-Rundschreiben 3/2017 (GW) zum Videoidentifizierungsverfahren.

<sup>212</sup> Damar (08.12.2021), S. 8 ff.; European Parliament (März 2024), S. 51.

<sup>213</sup> BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, S. 73 f.

<sup>214</sup> Interview mit Herrn Markus Ertl vom Deutschen Blinden- und Sehbehindertenverband e.V.

<sup>215</sup> Khan (2021), S. 3; Finance Watch (2024), S. 16.

Rahmen der Geldwäscheprävention gefordert werden muss (§§ 11 Abs. 4, 12 Abs. 1 GwG).<sup>216</sup> Der Anspruch auf ein Basiskonto besteht ausdrücklich auch für wohnungslose Personen. Sie können alternativ eine andere postalische Adresse angeben wie etwa die eines Familienmitglieds, Freundes, einer Beratungsstelle oder ein Postfach (§ 11 Abs. 4 Nr. 1 lit. (e) GwG).<sup>217</sup> Die Anwendung dieser Vorschrift ist allerdings in der Praxis äußerst problematisch, da die Anbieter regelmäßig auf einer Meldebescheinigung bestehen.

### 3. Zwischenfazit

Die oben angeführten Ausführungen zeigen, dass Barrieren zum digitalen Verkehr alle Verbraucher:innen betreffen, vulnerable Verbrauchergruppen wie einkommensschwache und Personen mit Einschränkungen jedoch im Besonderen von diesen Barrieren betroffen sind. Praktische Barrieren umfassen vor allem die Ressourcen, die für die Nutzung des digitalen Zahlungsverkehrs nötig sind. Dies umfasst den Zugang zum Internet, das Vorhandensein eines Endgerätes sowie die motorischen und kognitiven Fähigkeiten, das Endgerät samt Zahlungsfunktionen zu bedienen. Kritisch hervorgehoben sind hier die Kostenbarrieren sowie die mangelnde Umsetzung eines barrierefreien Zugangs zum Zahlungsverkehr. Bei der Barriere der mangelnden Kompetenz geht es für die Banken darum, mit der fehlenden digitalen Kompetenz, gerade der Generationen, die nicht in einer digitalen Welt aufgewachsen sind, umzugehen und diese darin zu unterstützen. Die dritte identifizierte Barriere besteht in der fehlenden Bereitschaft sowohl auf Seiten der Verbraucher:innen, die sich auf Grund von mangelndem Vertrauen in die Digitalisierung von dieser fernhalten möchten, als auch auf Seiten der Anbieter, die aus betriebswirtschaftlichen Zielsetzungen zugangsfördernde Regulierung nicht umsetzen. Schließlich wurde die regulatorische Barriere identifiziert, die vorliegt, wenn bestehende Regulierungen den Zugang zum digitalen Zahlungsverkehr einschränken.

---

<sup>216</sup> FEANTSA (Januar 2022), S. 10; Finance Watch (2024), S. 16.

<sup>217</sup> Bundesanstalt für Finanzdienstleistungsaufsicht (2017), o.S.

## IV. Implikationen für die Stärkung der Teilhabe am Zahlungsverkehr

Online- und Mobile-Banking ermöglicht es Nutzer:innen, Bankgeschäfte von zu Hause oder unterwegs zu erledigen, was eine hohe Flexibilität und Bequemlichkeit ermöglicht. Überweisungen, Daueraufträge, Kontoübersicht und viele andere Bankdienste sind rund um die Uhr verfügbar, was Online- und Mobile-Banking zu einer bevorzugten Option für technikaffine und mobile Nutzer macht. Für den Zugang zu digitalem Zahlungsverkehr wie beispielsweise Online-Shopping, internationale Transaktionen oder mobile Zahlungen sind Online- und Mobile-Banking essenziell, da sie eine sofortige und unkomplizierte Durchführung dieser Zahlungen ermöglichen. Ein großer Vorteil des digitalen Zahlungsverkehrs ist die Minimierung der Notwendigkeit, Bargeld zu verwenden, da die Zahlungen direkt und digital abgewickelt werden können. Hier zeigt sich die wachsende Bedeutung von digitalen Zahlungsmethoden wie Kreditkarten, E-Wallets oder mobilen Bezahlmethoden. Zudem erleichtern das Online- und Mobile-Banking das Verwalten von Finanzen wie das Einsehen von Kontoauszügen oder das Planen von Zahlungen.

Jedoch kann die Nutzbarkeit des Online- und Mobile-Bankings für bestimmte Nutzergruppen wie ältere Menschen oder diejenigen ohne regelmäßigen Internetzugang eingeschränkt sein. Auch die Notwendigkeit, grundlegende digitale Fähigkeiten zu besitzen, stellt eine Hürde für manche dar. Um eine breite Nutzung von digitalen Bezahlmethoden zu erreichen, muss zudem bei den potenziellen Nutzer:innen ein Vertrauen herrschen, das sowohl die technische Funktionsfähigkeit als auch die Zuverlässigkeit und Sicherheit der in Anspruch genommenen Zahlungsdienstleistungen umfasst. Ein zentrales Problem ist dabei die Cybersicherheit: Online- und Mobile-Banking können ein Ziel für Hacker und Betrüger sein, wogegen die Sicherheitsvorkehrungen wie starke Kundenauthentifizierung und Passwörter nicht immer den ausreichenden Schutz anbieten können. Und selbst eine Regulierung durch gesetzliche Regelungen bietet keinen ausreichenden Schutz, da es an einer effektiven und ausreichenden Umsetzung mangelt. In einigen Fällen kann die Regulierung selbst für eine Zugangseinschränkung verantwortlich sein.

Eine perfekte Bezahlmethode ermöglicht es, fällige Zahlungen fristgerecht ohne nennenswerte Hürden zu ermöglichen, dabei kostengünstig und sicher zu sein und das Private zu schützen. Die obigen Ausführungen zeigen, dass weder Bargeld noch digitale Zahlungsmethoden diesbezüglich perfekt sind. Zudem wird deutlich, dass oftmals keine wirkliche Wahlfreiheit zwischen den unterschiedlichen Bezahlmethoden existiert. Verbraucher:innen werden dabei immer häufiger vor die Notwendigkeit gestellt, eine digitale Bezahlmethode zu nutzen, um gewünschte Transaktionen durchführen zu können. Tatsächlich bieten digitale Bezahlmethoden den Verbraucher:innen ja auch Vorteile, die zunehmend erkannt werden.

Die Zugangsbarrieren zu Bargeld sind eher praktischer Natur und hängen sowohl mit der abnehmenden Zahl an Bankfilialen (vor allem in der Fläche) zusammen als auch mit begrenzten Möglichkeiten des Einzelhandels, entstehende Lücken zu füllen. Eine weitere Barriere hat mit der steigenden Digitalisierung des Zahlungsverkehrs zu tun, durch die Banken ihre Kunden kostengünstig Zugang zum digitalen Zahlungsmittel ermöglichen und die gleichzeitig damit einhergeht, dass die Akzeptanz von Bargeld aufgrund der kostenintensiveren Bargeldbereitstellung im Handel schwindet.

Es gilt, die beschriebenen Barrieren zu überwinden. Angesprochen sind dabei aber nicht nur digitale Bezahlmethoden. Vielmehr sollte nicht nur im Interesse einer Wahlfreiheit für Verbraucher:innen, sondern auch im Interesse der einzel- wie gesamtwirtschaftlichen finanziellen Stabilität dem Zugang und der Nutzung von Bargeld weiterhin Bedeutung zukommen. Was Erstgenanntes anbelangt, so sei auf die Fähigkeit von Bargeld verwiesen, Budgetbeschränkungen rechtzeitig zu erkennen, was auch ein wichtiger Beitrag zur Vermeidung von Überschuldung ist. Im Hinblick auf Letztgenanntes sei auf das steigende Risiko von Black-Out-Situationen verwiesen.

Im Folgenden werden aus dem Status Quo Implikationen abgeleitet, auf welche Weise bestehende Barrieren abgebaut werden können und auch sollen. Der Orientierungsmaßstab ist dabei die fortschreitende Digitalisierung des Zahlungsverkehrs, an der möglichst viele Verbraucher:innen teilhaben können, ohne gleichzeitig in einer situativ nicht gerechtfertigten Weise daran teilnehmen zu müssen.

In Bezug auf das damit verbundene Ziel der Wahlfreiheit sei an dieser Stelle auf die Kampagne “Keep me Posted” aus Großbritannien verwiesen, die sich für das Recht der Verbraucher:innen einsetzt, selbst wählen zu können, wie sie auf Finanzdienstleistungen zugreifen möchten. Die Kampagne hat dabei insbesondere die Bedürfnisse von vulnerablen und älteren Verbraucher:innen im Blick. Sie wendet sich gezielt an Unternehmen, Regulierungsbehörden und politische Entscheidungsträger, um auf die Notwendigkeit der Wahlfreiheit aufmerksam zu machen. Die Kampagne fordert, dass Verbraucher:innen weiterhin die Möglichkeit haben müssen, wichtige Dokumente wie Rechnungen, Kontoauszüge oder Vertragsinformationen kostenlos in Papierform zu erhalten, wenn sie dies wünschen. Unternehmen sollen dafür klar und transparent über die verfügbaren Kommunikationswege informieren, damit Verbraucher:innen auch aktiv darüber informiert werden, dass sie papierbasierte Alternativen nutzen können. Ein zentrales Anliegen der Kampagne ist zudem die Abschaffung von Zusatzgebühren für papierbasierte Kommunikation. Verbraucher:innen sollen keine finanziellen Nachteile erleiden, wenn sie sich dafür entscheiden, Dokumente oder Rechnungen in Papierform zu erhalten, anstatt auf digitale Alternativen umzusteigen.<sup>218</sup>

## 1. Abbau von praktischen Barrieren

Der Abbau von praktischen Barrieren stellt eine notwendige Bedingung für den Zugang zum Zahlungsverkehr dar. Ohne deren Abbau sind nicht alle Bezahlmethoden gleichermaßen erreichbar und kann somit eine Wahlfreiheit nicht ausgeübt werden.

### 1.1 Infrastrukturelle Barrieren abbauen

Der unbeschränkte Zugang zum Bargeld muss erhalten bleiben, denn es verfügt nicht jeder über einen WLAN-Zugang, kann sich nicht jeder die Anschaffung der notwendigen Hardware leisten. Die Sicherstellung der gleichmäßigen Versorgung der Bürger:innen und vor allem solcher, die mit besonderen Barrieren beim Zugang zu verschiedenen Zahlungsmitteln und bei deren Nutzung konfrontiert sind, wird auch im öffentlichen Interesse als Staatsaufgabe angesehen.<sup>219</sup> Da die Bereitstellung von Bargeld auch auf Anbieterseite mit Kosten verbunden ist, die sie – anders als

---

<sup>218</sup> Financial Services User Group (31.12.2023), 25 f.

<sup>219</sup> Knobloch u. a. (19.11.2012), S. 47.

beim digitalen Zahlungsverkehr – nicht so einfach auf die Verbraucher:innen überwälzen können, sind regulierende Maßnahmen und/oder Anreize erforderlich, um diese Aufgabe zu erfüllen.

Zahlungsdienstleister haben die Pflicht, sicherzustellen, dass sich ihre Kund:innen mit genügend Bargeld als gesetzlichem Zahlungsmittel versorgen können. Beim Zugang zum Bargeld ist vor allem zu beachten, dass es sich dabei um die Erfüllung von vertraglichen Geldschulden durch das gesetzliche Zahlungsmittel handelt. Den Anspruch der Zahlungsdienstnutzer:innen auf ihr Kontoguthaben haben die Zahlungsdienstleister, wenn gewünscht, durch Barzahlung zu erfüllen. Insofern ist es an erster Stelle die Pflicht der Zahlungsdienstleister, dass ihre Kund:innen weiterhin ausreichenden Zugang zum Bargeld haben, sodass die Erfüllung vertraglicher Pflichten der Zahlungsdienstleister faktisch weiterhin möglich bleibt. Allerdings sind Banken derzeit gesetzlich nicht verpflichtet, in bestimmten Abständen Geldautomaten bereitzustellen.

Es gibt auch auf EU-Ebene bisher keine konkreten Vorschriften, wie diese Pflicht der Bargeldversorgung umgesetzt werden soll. Dies soll sich jedoch mit dem künftigen BargeldVO ändern. Aufgrund der Wichtigkeit des Bargelds und des Zugangs zum Bargeld hat die EU vor, die Mitgliedstaaten zu verpflichten, in allen Regionen ihres Hoheitsgebiets, einschließlich städtischer und nichtstädtischer Gebiete, für einen hinreichenden und wirksamen Zugang zu Bargeld zu sorgen (Art. 8 Abs. 1 S. 1 BargeldVO-Vorschlag). Dazu sollen die Mitgliedstaaten aufgrund von der Kommission zu definierenden einheitlichen Indikatoren die Lage dauerhaft überwachen und bewerten. Diese Indikatoren könnten Faktoren umfassen, die sich auf den Zugang zu Bargeld auswirken, z. B. die Dichte an Bargeldzugangspunkten im Verhältnis zur Bevölkerung, Abhebungs- und Einlagebedingungen, einschließlich Gebühren, das Vorhandensein verschiedener Netze mit unterschiedlichen Zugangsmodalitäten für die Kund:innen, Unterschiede zwischen städtischen und ländlichen Gebieten und sozioökonomische Unterschiede sowie Zugangsprobleme für bestimmte Bevölkerungsgruppen.<sup>220</sup>

Der Verordnungsvorschlag sieht vor, dass Mitgliedstaaten zukünftig Maßnahmen ergreifen müssen, sollte kein hinreichender und wirksamer Zugang zu Bargeld in ihrem Hoheitsgebiet gewährleistet sein (Art. 8 Abs. 3 BargeldVO-Vorschlag). Diese können u. a. folgende Maßnahmen umfassen:

- Anforderungen an Zahlungsdienstleister zur Aufrechterhaltung der Bargelddienste in einer ausreichenden Zahl ihrer Filialen, wobei eine ausreichende geografische Breite abzudecken ist,
- Anforderungen an ausschließlich online tätige Kreditinstitute zur Benennung zugelassener Händler oder zur Aufrechterhaltung einer hinreichenden Dichte an Geldautomaten, wobei im Verhältnis zur Bevölkerung für eine gute geografische Streuung zu sorgen ist,
- Zusammenlegung von Geldautomaten,
- Empfehlungen an Nichtkreditinstitute wie unabhängige Geldautomatenbetreiber, Einzelhändler oder Postämter, um diese dazu zu bewegen, die von Banken erbrachten Bargelddienstleistungen zu ergänzen.<sup>221</sup>

---

<sup>220</sup> Erwägungsgrund 7 BargeldVO-Vorschlag.

<sup>221</sup> Erwägungsgrund 7 BargeldVO-Vorschlag. Die Empfehlungen bleiben hier leider auf allgemeiner Ebene.

**Box 1: Fallbeispiel zur Bargeldversorgung**

In der praktischen Umsetzung der durch den BargeldVO-Vorschlag vorgesehenen Maßnahmen sind an erster Stelle die Kreditinstitute in die Pflicht zu nehmen. Ein Beispiel zur Umsetzung der Verordnung ins nationale Recht bietet die Regulierung im englischen Recht. Die englische Financial Conduct Authority (FCA) hat im Juli 2024 eine Regulierung über den Zugang zum Bargeld (FCA 2024/26) verabschiedet, die am 18. September 2024 in Kraft getreten ist.<sup>222</sup> Zudem ist seit Oktober 2022 eine Regelung bezüglich Filialschließungen (FG 22/6) in Kraft.<sup>223</sup> Entsprechend diesen Instrumenten sind die Kreditinstitute verpflichtet, die Auswirkungen von Schließungen von Filialen und Geldautomaten beim Zugang zu den finanziellen Dienstleistungen zu bewerten. Sollte die Bewertung zum Ergebnis kommen, dass der Zugang zu den finanziellen Dienstleistungen beeinträchtigt wird, müssen die Kreditinstitute eine Alternative anbieten und zwar vor der Schließung. Wenn bestehende Alternativen, z. B. die Filiale einer anderen Bank oder ein Banking-Hub, ausreichende Versorgung mit den Dienstleistungen und dem Bargeld anbieten, muss die filialschließende Bank ihre Kund:innen beim Wechsel zur anderen Bank unterstützen. Wenn bestehende Alternativen nicht verfügbar sind, muss die Bank prüfen, welche alternativen Angebote vernünftigerweise bereitgestellt werden könnten, um den Verlust von Dienstleistungen auszugleichen. Dazu gehören u. a. Bereitstellung mobiler Banking-Hubs, temporärer „Pop-up“-Filialen in der Gemeinschaft oder Bargeldlieferdienste, Beauftragung eines gebührenfreien Geldautomaten, Unterstützung der Kund:innen bei der Nutzung digitaler und telefonischer Kanäle, soweit sie dazu in der Lage sind (Banken dürfen nicht davon ausgehen, dass alle Kund:innen in der Lage sind, einen bestimmten alternativen Kanal zu nutzen), Entwicklung weiterer innovativer Lösungen, um den Verlust von Dienstleistungen auszugleichen.

Des Weiteren sind sie verpflichtet, ihre Kund:innen über die geplante Schließung und Alternativen zu informieren sowie Unterstützung für den Übergang anzubieten. Im Rahmen dieser Regulierungen findet auch eine allgemeine Bewertung der Bargeldversorgung statt. Durch diese Bewertung wird festgestellt, wo Menschen und Geschäfte ansässig sind und ob eine Lücke in der Bargeldversorgung besteht. Sollte die Bewertung eine lokale Versorgungslücke feststellen, sind die (ausgewählten 14 großen) Kreditinstitute verpflichtet, ohne unangemessene Verzögerung die erforderlichen Bargelddienstleistungen zu erbringen.

Die Schließung der Versorgungslücke erfordert auch, dass die zur Verfügung gestellten Geldautomaten an leicht zugänglichen Stellen erreichbar sowie funktionsfähig sind und der Nachfrage entsprechend Bargeld bereitstellen. Lediglich für die Dichte von Bargeldabhebungsmöglichkeiten zu sorgen, ist für die Gewährleistung des Zugangs nicht ausreichend. In diesem Zusammenhang ist das Beispiel aus Belgien sehr einleuchtend.<sup>224</sup> Die belgischen Banken haben vor einigen Jahren eine selbstverpflichtende Vereinbarung getroffen, wonach sie für die Dichte von Geldautomaten zu sorgen hatten. Allerdings waren die Geldautomaten entweder an nicht zentralen Stellen (z. B. in einer Seitenstraße im Wohngebiet anstatt am Bahnhof oder in der Nähe von Einkaufszentren) platziert oder sie waren regelmäßig leer oder nicht funktionsfähig. Daher müssten Abhilfemaßnahmen nicht nur für die Dichte der

<sup>222</sup> Abrufbar auf <https://www.fca.org.uk/publication/policy/ps24-8.pdf>, Letzter Zugriff: 7. November 2024.

<sup>223</sup> Abrufbar auf: <https://www.fca.org.uk/publication/finalised-guidance/fg22-6.pdf>, Letzter Zugriff: 7. November 2024.

<sup>224</sup> Erwähnt auf der 1st European Conference of the International Association of Consumer Law am 17.-18. September 2024 in Girton College, Cambridge (Vereinigtes Königreich).

Geldautomaten oder Bargeldabhebungsmöglichkeiten Sorge tragen, sondern auch für den tatsächlichen Zugang zum Bargeld.

Interessant ist in Bezug auf die Bargeldversorgung auch das Angebot der Bargeldlieferungen. Bargeldlieferungen werden von Sparkassen und anderen Banken zu unterschiedlichen Konditionen angeboten. So variieren Kosten und Höhe sowie Stückelungsmöglichkeiten der Bargeldlieferungen. Bargeldlieferungen werden als Kompensation für den Rückgang von Filialen und Bankautomaten angesehen und sollen sich an Verbrauchergruppen richten, die aufgrund ihres Alters oder ihrer Funktionseinschränkung nicht in der Lage sind, selbstständig Bargeld an einem Geldautomaten abzuheben.<sup>225</sup> Inwiefern dieser Service bekannt ist und genutzt wird, ist nicht bekannt.

Gerade, wenn Zugangslücken bei der Bargeldversorgung bestehen, sollten Abhebemöglichkeiten ermittelt und kommuniziert werden. Die Financial Services User Group der EU-Kommission fordert entsprechend, dass diese Informationen über alternative Möglichkeiten des Zugangs, einschließlich der technischen Ausstattung wie sprechende Geldautomaten, sowohl von den Finanzinstituten als auch von lokalen und regionalen Unterstützungsgruppen veröffentlicht werden.<sup>226</sup> Diese öffentliche Kommunikation zur Bargeldversorgung samt Informationen über alternative Möglichkeiten des Zugangs könnte auch ein Anreiz für die Finanzinstitute sein, bessere Zahlen hierzu zu präsentieren, um Kund:innen an sich zu binden.<sup>227</sup>

Um den Zugang zum Bargeld weiter zu verbessern, hat der europäische Gesetzgeber vor, Einzelhändlern aufsichtsrechtlich zu ermöglichen, unabhängig vom Kauf Bargeldbereitstellungsdienste anzubieten. Insofern werden die Einzelhändler ohne Beantragung einer Zulassung als Zahlungsdienstleister bzw. ohne Auftreten als Vertreter eines Zahlungsinstituts (Erwägungsgrund 10 PSR-E) Bargeldabhebungsdienste anbieten können, wenn der zur Verfügung gestellte Betrag pro Abhebung 50,- EUR nicht übersteigt (Art. 37 PSD3-E). Allerdings darf diese Lösung lediglich unterstützend zur Anwendung kommen und sich nicht zur Hauptquelle für die Bargeldversorgung entwickeln.

Eine der wichtigsten praktischen Hürden bei der Teilnahme am Zahlungsverkehr stellen die physikalischen Barrieren dar. Um die digitale Teilhabe von Menschen mit langfristigen körperlichen, seelischen, geistigen oder Sinnesbeeinträchtigungen am digitalen Zahlungsverkehr zu erleichtern bzw. zu ermöglichen, stellen das Barrierefreiheitsstärkungsgesetz (BFSG) und die Verordnung zum Barrierefreiheitsstärkungsgesetz (BFSGV) bestimmte Anforderungen an Zahlungsdienstleistungen. Diese umfassen alle für die Führung eines Zahlungskontos erforderlichen Vorgänge sowie mit einem Zahlungskonto verbundenen Dienste (§ 2 Nr. 24 lit. c und d BFSG), wie z. B. Ausführung von Zahlungsvorgängen mittels einer Zahlungskarte und Überweisungen. Nach dem Inkrafttreten des BFSG und der BFSGV am 28. Juni 2025 werden alle Dienstleister verpflichtet sein, u. a. alle mit der Dienstleistung in Verbindung stehenden Informationen über mehr als einen sensorischen Kanal bereitzustellen, in verständlicher und wahrnehmbarer Weise darzustellen sowie, falls vorhanden, alle ihre Websites, Online- und Mobile-Apps barrierefrei bedienbar zu gestalten (§ 12 BFSGV). Sie müssen zudem die Interoperabilität mit assistiven Technologien gewährleisten (§ 13 BFSGV). D. h.

---

<sup>225</sup> Financial Services User Group (31.12.2023), S. 15.

<sup>226</sup> Financial Services User Group (31.12.2023), S. 7.

<sup>227</sup> Ozili (2020), S. 3 Die bestehenden Websites dazu beinhalten leider keine Informationen über alternative Möglichkeiten des Zugangs, s. <https://www.girocard.eu/fuer-mich/meine-karte/geldautomatenfinder/>, Letzter Abruf: 26. November 2024, oder <https://geldautomaten-suche.org/>, Letzter Abruf: 26. November 2024.

sie müssen sicherstellen, dass ihre Systeme und Anwendungen mit assistiven Technologien wie Screenreadern oder speziellen Eingabegeräten kompatibel sind, um die Zugänglichkeit für Menschen mit Behinderungen zu ermöglichen. Gesondert für die Bankdienstleistungen, darunter auch für die Zahlungsdienstleistungen, wird zudem vorgeschrieben, dass die Identifizierungsmethoden, Authentifizierungsmethoden, elektronischen Signaturen und Sicherheitsfunktionen barrierefrei zu gestalten sind (§ 17 Abs. 1 BFSGV). Nicht zuletzt ist zu gewährleisten, dass die Informationen zur Funktionsweise der Bankdienstleistung verständlich sind, ohne dass ihr Schwierigkeitsgrad das Sprachniveau B2 überschreitet (§ 17 Abs. 2 BFSGV). Da Art. 22 Abs. 1 DigEUR-Vorschlag die Barrierefreiheit des digitalen Euro vorschreibt, gelten alle Voraussetzungen zur Barrierefreiheit auch für den digitalen Euro.

Die Barrierefreiheit von Geldautomaten, die nach dem 28. Juni 2025 in Verkehr gebracht werden, wird durch das BFSG vorgeschrieben.<sup>228</sup> Insofern müssen sie u. a. mit Sprachausgabetechnologie ausgestattet sein, die Benutzung von Einzel-Kopfhörern ermöglichen, die Nutzer:innen über mehr als einen sensorischen Kanal darauf hinweisen, wenn eine zeitlich begrenzte Eingabe erforderlich ist, sowie die Verlängerung der gegebenen Zeit ermöglichen. Allerdings erlaubt die BFRL die Weiterverwendung von Geldautomaten, die vor dem 28. Juni 2025 eingesetzt werden, bis zum Ende ihrer wirtschaftlichen Nutzungsdauer, aber nicht länger als 20 Jahre nach ihrer Ingebrauchnahme (Art. 32 Abs. 2 BFRL). Immerhin hat das BFSG diese Frist auf 15 Jahre gekürzt (§ 38 Abs. 2 BFSG). Daher dürfen die nicht barrierefreien Geldautomaten, die in Deutschland vor dem 28. Juni 2025 eingesetzt werden, bis zum 28. Juni 2040 weiterverwendet werden, solange dies auch der wirtschaftlichen Nutzungsdauer des Geldautomaten entspricht. Leider hat der deutsche Gesetzgeber die Gelegenheit verpasst, die Barrierefreiheit aller Geldautomaten schneller zu sichern.

Sozial- und Behindertenverbände kritisieren das BFSG als nicht weitreichend genug, da es beispielsweise bauliche Aspekte vernachlässigt. Laut der Sozial- und Behindertenverbände adressiere das BFSG nur digitale Produkte und Dienstleistungen und auch nur in Teilen die der Privatwirtschaft.<sup>229</sup> Zudem seien die langen Übergangsfristen nicht nachvollziehbar.<sup>230</sup> Die Kritik betrifft auch die fehlende Regulierung über den Ort und die Beschaffenheit von Geldautomaten, die bei der Barrierefreiheit eine ausschlaggebende Rolle spielen. So sollten Geldautomaten an Orten mit guten Parkmöglichkeiten für Rollstuhlfahrer aufgestellt und in verschiedenen Höhen bereitgestellt werden, um auch für kleinere Menschen und Rollstuhlfahrer verfügbar zu sein.<sup>231</sup> Auch die Lichtverhältnisse des Standorts des Geldautomaten sind wichtig, da Blendung oder unterschiedliche Lichtverhältnisse die Lesefähigkeit beeinträchtigen können. Menschen ohne nutzbare Sehkraft benötigen taktile oder akustische Eingaben.<sup>232</sup> Ferner müsse die Art und Weise der durch Geldautomaten vermittelten Kommunikation barrierefrei sein. Dies umfasst die Schriftgröße und den Kontrast, aber auch die genutzten Begrifflichkeiten und die verfügbare Sprache. So sollten „einfache Sprache“ und unterschiedliche Sprachen verfügbar sein. Auch die

---

<sup>228</sup> Art. 4 Abs. 2 i. V. m. Art. 2 Abs. 1 lit. b und Anhang I Abschnitt I Nr. 2 lit. o BFRL; §§ 3 i. V. m. 1 Abs. 2 Nr. 2 BFSG und § 7 BFSGV.

<sup>229</sup> Deutscher Bundestag (2021).

<sup>230</sup> Ebd., u. a. Aktion Mensch (2021)

<sup>231</sup> De Nederlandsche Bank (2023), S. 38.

<sup>232</sup> Financial Services User Group (31.12.2023), S. 21.

Verwendung von Piktogrammen und Fotos wird diesbezüglich empfohlen, um Kommunikation nicht von Alphabetisierung und Sprache abhängig zu machen.<sup>233</sup>

Entsprechend relevant ist hier auch, dass die Barrierefreiheit der starken Kundenauthentifizierung künftig in Art. 88 PSR-E gesondert geregelt wird. Dementsprechend müssen die Verfahren zur starken Kundenauthentifizierung nicht nur die Barrierefreiheitsanforderungen der BFRL erfüllen, sondern müssen darüber hinaus sicherstellen, dass allen Zahlungsdienstnutzer:innen, einschließlich Menschen mit Behinderungen, älteren Menschen, Menschen mit geringen digitalen Kompetenzen und Menschen, die keinen Zugang zu digitalen Wegen oder Zahlungsinstrumenten haben, mindestens ein auf ihre besondere Situation abgestimmtes Mittel zur Verfügung steht, um eine starke Kundenauthentifizierung durchführen zu können. Das EP hat diese Pflicht dahingehend ergänzt, dass die starke Kundenauthentifizierung kostenlos zur Verfügung zu stellen ist (Art. 88 Abs. 2 PSR-E, EP-Bericht). Zudem dürfen die Zahlungsdienstleister die Leistungsfähigkeit der starken Kundenauthentifizierung nicht von der ausschließlichen Verwendung eines einzigen Authentifizierungsverfahrens bzw. eines Smartphones oder sonstigen intelligenten Gerätes abhängig machen. Die Zahlungsdienstleister sind verpflichtet, mehr als ein Mittel für die Durchführung der starken Kundenauthentifizierung zu entwickeln, um den verschiedenen spezifischen Situationen all ihrer Kund:innen gerecht zu werden, insbesondere derjenigen mit Behinderungen, geringen digitalen Kompetenzen, älteren Personen und Personen, die keinen Zugang zu digitalen Kanälen oder Zahlungsinstrumenten haben.

Bei der Umsetzung dieser möglichen künftigen Regelungen braucht es die Bereitstellung von mehreren alternativen Anwendungsmöglichkeiten, um die digitale Identitätsfeststellung sowie die Nutzung von Anwendungen des digitalen Zahlungsverkehrs tatsächlich barrierefrei zu gestalten. Bei digital unkundigen Personen und kognitiv eingeschränkten Personen braucht es beispielsweise einfache, intuitive Anwendungen in einfacher Sprache, sodass sie in der Lage sind, zu beurteilen, welche Transaktion sie freigeben. Auch hier könnten unterschiedliche Bedürfnisse bedacht werden wie z. B. durch das Angebot einfacher Sprache in verschiedenen Fremdsprachen.<sup>234</sup>

## 1.2 Akzeptanz von Bargeld: Nutzungsmöglichkeiten erhöhen

Neben dem Zugang zu Bargeld ist auch die breite Nutzungsmöglichkeit von Bargeld im Handel für einen inklusiven Zahlungsverkehr wichtig. Ist diese Nutzung von Bargeld nicht gegeben, werden Personen ohne Zugang zum digitalen Zahlungsverkehr von der wirtschaftlichen Teilhabe ausgeschlossen. Vor dem Hintergrund, dass die Möglichkeit der Bargeldzahlung von Verbraucher:innen präferiert wird, wird der Rückgang von Bargeldakzeptanz vor allem kritisch gesehen. Bargeld schützt die Privatsphäre, der Zugang ist verhältnismäßig voraussetzungsfrei und damit inklusiv und resilient. Diesbezüglich ist hier vor allem der Bargeld-VO-Vorschlag wichtig, der auf diese Barriere in Bezug auf Bargeld eingehen möchte.

Durch den BargeldVO-Vorschlag wird die Verpflichtung zur Annahme von Euro-Banknoten und -Münzen geregelt. Sollte der Vorschlag in seiner derzeitigen Fassung verabschiedet werden, wird klargestellt, dass das Bargeld zum vollen Nennwert mit schuldbefreiender Wirkung angenommen werden muss (Art. 4 BargeldVO-Vorschlag). Die Annahmepflicht gilt nicht für den Onlinehandel, da

---

<sup>233</sup> De Nederlandsche Bank (2023), S. 38.

<sup>234</sup> BEUC (o.J.), S. 6.

die Zahlungen für Waren oder Dienstleistungen, die im Fernabsatz (einschließlich Online-Käufen) erworben werden, nicht in den Anwendungsbereich der künftigen Verordnung fallen werden (Art. 2 Abs. 2 BargeldVO-Vorschlag). Zudem werden Zahlungsempfänger aus legitimen und vorübergehenden Gründen eine Bargeldzahlung ablehnen dürfen, z. B. wenn sie kein ausreichendes Wechselgeld haben (Art. 5 Abs. 1 lit. a, Abs. 2 BargeldVO-Vorschlag).

Art. 5 Abs. 1 lit. b BargeldVO-Vorschlag lässt weiterhin vertragliche Vereinbarungen über Zahlungsmodalitäten zu. Wie oben erläutert, basiert die Verweigerung der Bargeldannahme im Einzelhandel überwiegend auf den AGB, die eine bargeldlose Zahlung vorschreiben. Insofern wird die Ausnahme im BargeldVO-Vorschlag die Probleme in der Praxis nicht verhindern können. Aus diesem Grund verlangen Verbraucherschutzorganisationen, diese Ausnahme entweder zu löschen oder zu konkretisieren.<sup>235</sup>

Diese Ausnahme im Bargeld-VO ist mit Bezug auf Vereinbarungen durch AGB zu streichen. Denn diese breite Ausnahme würde zur Folge haben, dass sich in der Praxis nichts ändert. Eine Ausnahme sollte lediglich auf beidseitig explizit ausgehandelte Vereinbarungen beschränkt sein und eine Vereinbarung durch AGB ausschließen. Da allerdings die Bargeldakzeptanz im Einzelhandel stark von den Kosten der Bargeldversorgung abhängt, sollte man gleichzeitig dem Einzelhandel einen entsprechenden Anreiz anbieten.

Ein kostengünstigeres Bargeldhandling kann Anreize für den Handel schaffen, Bargeld als Zahlungsmittel zu akzeptieren. So ermöglichen es beispielsweise sogenannte Smart Safes und Bargeldrecycler im Einzelhandel, den Aufwand des Bargeldhandlings in Geschäften zu reduzieren, indem die Frequenz der Bargeldabholung durch Wertdienstleister reduziert werden kann. Bargeldrecycler, in denen Bargeldannahme und Bargeldausgabe automatisiert werden können und Bargeld direkt auf Echtheit geprüft wird, tragen dazu bei, dass auch eine bessere Übersicht über den Bargeldbestand besteht und damit kein unnötiges Wechselgeld beschafft wird.<sup>236</sup> Eine weitere Möglichkeit, die Kosten für das Bargeldhandling im Einzelhandel zu reduzieren, ist die Abschaffung von 1- und 2-Cent-Münzen, da die Herstellung der Münzen teurer ist als ihr Nennwert.<sup>237</sup> In diesem Fall müssten Preise auf 5-Cent Beträge gerundet werden.<sup>238</sup>

### 1.3 Kosten für Verbraucher:innen gering halten

Die für den Zahlungsverkehr aufzuwendenden Kosten sind eine weitere praktische Barriere für die Teilhabe am Zahlungsverkehr. Personengruppen mit einem höheren Risiko, digital abgehängt zu sein, gehören häufig auch zu den Einkommensschwächeren und sind deshalb mit einem größeren Aufwand dafür konfrontiert, am Zahlungsverkehr teilzunehmen. Sind diese zusätzlichen Kosten Voraussetzung für die Teilnahme am Zahlungsverkehr, können sie schnell zum Ausschluss führen. Wohlbemerkt können sowohl mit der Bargeldabhebung als auch mit der Nutzung des digitalen Zahlungsverkehrs Kosten verbunden sein.

---

<sup>235</sup> Philipp Wendt, Verbraucherzentrale Hessen, Vortrag „Bargeld unter Druck?“ auf dem Hessischen Verbrauchertag: „Portemonnaie, Smartphone oder Iris-Scan? Wie bezahlen wir in der Zukunft?“ am 6. November 2024, VZBV (16.02.2024); Verbraucherzentrale Bundesverband e.V. (2023), S. 6 f.

<sup>236</sup> Ehrenberg-Silies u. a. (Januar 2024), S. 81.

<sup>237</sup> Beil/Hohmann (2014), S. 4.

<sup>238</sup> Ehrenberg-Silies u. a. (Januar 2024), S. 84.

Das Bargeld wird nicht nur durch Zahlungsdienstleister bereitgestellt, sondern auch durch Bargeldautomatenbetreiber.<sup>239</sup> Sie unterliegen lediglich der Transparenzpflicht (Art. 3 lit. (o) PSD2). Hinsichtlich dieser Transparenzpflicht sieht der PSR-E keine Änderungen vor (Art. 7 PSR-E). Das Europäische Parlament (EP) hat diese Pflicht auch im PSD3-E ergänzt (Art. 38 Abs. 4a PSD3-E, EP-Bericht). Insofern würden weiterhin die Verbraucher:innen diese Kosten tragen, sollten sie keine gebührenfreie Bargeldabhebungsoptionen in der Nähe haben.

Zur Überwindung dieser Kostenbarriere sollte es ein Finanzierungskonzept geben, das die Übernahme der Kosten für die Bargeldabhebung durch die Banken regelt. Da die Bereitstellung des Bargelds für ihre Kund:innen im Rahmen des Zahlungsdienstervertrags eine Verpflichtung der Banken ist und da die Kund:innen bereits Kontogebühren zahlen, dürften die Kosten für die Bereitstellung des Bargelds über Geldautomaten von anderen, von den Banken unabhängigen Betreibern, nicht von den Verbraucher:innen getragen werden.

Beim Zugang zum digitalen Zahlungsverkehr stellen auch Kosten für den Kontozugang eine Zugangsbarriere dar. Besonders kritisch sind hier die Kosten für den Zugang zu einem Basiskonto zu betrachten. Gemäß Art. 18 Abs. 1 ZKRL ist das Basiskonto entweder kostenlos oder gegen ein angemessenes Entgelt anzubieten. In der Umsetzung dieser Vorschrift hat es der deutsche Gesetzgeber bevorzugt, dass Basiskonten gegen ein angemessenes Entgelt zur Verfügung gestellt werden (§ 41 Abs. 1, 2 ZKG). Doch in der Praxis werden insbesondere für die einkommensarmen Verbraucher:innen zu hohe Entgelte verlangt. Obwohl der BGH mittlerweile der Praxis, den Zugang zum Basiskonto durch zu hohe, prohibitiv wirkende Entgelte zu verhindern, eine Abfuhr erteilt hat,<sup>240</sup> sind die reduzierten Entgelte für viele Verbrauchergruppen weiterhin zu hoch.<sup>241</sup> Wie oben dargestellt belaufen sich Kosten je nach Finanzinstitut zwischen 58,80 € und 143,40 € pro Jahr. Laut einer Studie des vzbv bietet Deutschland dadurch im europäischen Vergleich das teuerste Basiskonto an.<sup>242</sup> Solche Kosten sind nicht, wie in der ZKRL und im ZKG gefordert, angemessen und sollten entsprechend deutlich reduziert werden, um den Zugang auch für einkommensschwächere Personengruppen zu realisieren.<sup>243</sup> Als weitere Maßnahmen kommen Preisdeckelung und/oder die Verknüpfung mit einem Referenzindex, wie z. B. dem Verbraucherpreisindex, in Frage.<sup>244</sup> Nicht zuletzt sollte das Basiskonto für vulnerable Verbrauchergruppen kostenlos sein.<sup>245</sup>

Ein Problem bezüglich der Kosten der Bargeldabhebung entsteht auch bei den Bargeldbereitstellungsdiensten im Einzelhandel. Der Verbraucherschutz kritisiert zu Recht, dass die Bargeldabhebung im Einzelhandel zumeist mit bedeckten Kosten verbunden ist, also die Verbraucher:innen zunächst etwas in dem Geschäft (zumeist für einen Mindestbetrag) kaufen müssten, um überhaupt an der Kasse Bargeld abheben zu können (Cashback). Die Gebühren, die für Cashback von den Banken erhoben werden, werden derzeit vielmehr durch die Einzelhändler getragen. Für die Einzelhändler ist es allerdings möglich, diese Gebühren auf die Verbraucher:innen

---

<sup>239</sup> Zu Gebühren, die durch Zahlungsdienstleister erhoben werden, s. oben II.2.2.

<sup>240</sup> BGH, Urt. v. 30.6.2020 – XI ZR 119/19 (juris).

<sup>241</sup> Finance Watch (2024), S. 10.

<sup>242</sup> Verbraucherzentrale Bundesverband e.V. (2024).

<sup>243</sup> FEANTSA (Januar 2022), S. 9.

<sup>244</sup> Verbraucherzentrale Bundesverband e.V. (2024).

<sup>245</sup> Finance Watch (2024), 11 f.

abzuwälzen. Sollten sie von dieser Möglichkeit Gebrauch machen, unterliegen sie dabei der Transparenzpflicht, d. h. die Entgelte für die Bargeldabhebung müssen den Verbraucher:innen offengelegt werden (Art. 38 Abs. 4a PSD3-E, EP-Bericht).

Die für den digitalen Zahlungsverkehr aufzuwendenden Kosten müssen für die Sozialleistungsempfänger:innen tragbar sein. Das ist eine Herausforderung vor allem für Menschen mit Behinderungen, die häufig zusätzliche Geräte oder Applikationen brauchen, um die Möglichkeiten des digitalen Zahlungsverkehrs nutzen zu können, weil sie sehr oft von Sozialleistungen abhängen. Der Leistungsumfang reicht zur Abdeckung dieser zusätzlichen Kosten aber häufig nicht aus. Für die digitale Grundausstattung braucht es somit zunächst eine bedarfsgerechte Anhebung und regelmäßige Anpassung des Regelsatzes, die sowohl Anschaffungs- und Wartungskosten als auch laufende Verbrauchsausgaben (entsprechende Internetverbindung, Software-Updates etc.) zur Sicherstellung digitaler Teilhabe angemessen berücksichtigen. Überdies existiert ein spezifischer Bedarf an digitaler Teilhabe für Menschen mit einer wesentlichen Behinderung i. S. v. § 99 SGB IX. Die in § 84 Abs. 1 SGB IX dargestellten Regelungen für entsprechende Ausgleichszahlungen kommen wegen der engen Voraussetzung des erforderlichen Ausgleichens einer durch die Behinderung bestehenden Einschränkung nur für besondere Fallgestaltungen zur Anwendung. Die Fachverbände für Menschen mit Behinderung schlagen daher die folgende Änderung von § 84 Abs. 1 SGB IX vor: „Die Leistungen umfassen Hilfsmittel, die erforderlich sind, um eine durch die Behinderung bestehende Einschränkung einer gleichberechtigten Teilhabe am Leben in der Gemeinschaft mittelbar oder unmittelbar auszugleichen. Die Leistungen umfassen auch barrierefreie Computer sowie andere Ausstattungen zur digitalen Teilhabe.“ Aus Sicht der Fachverbände für Menschen mit Behinderung könnte der behinderungsbedingte Mehrbedarf für erhöhte Kosten bei der digitalen Ausstattung auch über die Einführung eines besonderen Mehrbedarfs für die Kosten der digitalen Ausstattung im Recht der Grundsicherung/Hilfe zum Lebensunterhalt (Ergänzung des § 30 SGB XII bzw. § 21 SGB II) geregelt werden.<sup>246</sup>

## 2. Umgang mit fehlender Kompetenz

### 2.1 Finanzielle und digitale Kompetenzen aufbauen

Eine hybride Zahlungsrealität stellt neue Anforderungen an die finanzielle Bildung, denn sie muss neben Bargeld auch digitale Zahlungsmittel berücksichtigen. Der digitale Zahlungsverkehr bietet viele Annehmlichkeiten, macht den Umgang mit Geld jedoch abstrakter und anfälliger für Fehlentscheidungen. Ohne gezielte Maßnahmen zur Aufklärung und Regulierung kann er den Weg in die Überschuldung ebnen. Ein bewusster Umgang mit digitalen Zahlungsmethoden ist entscheidend, um die finanzielle Kontrolle zu behalten. So verweist die Stellungnahme der Sozialverbände zum Thema Bargeld auf folgendes Beispiel:

*„Menschen, die sich in der unbaren Bezahlwelt verschuldet haben, müssen für die Fallstricke unbarer Zahlungsmittel sensibilisiert und dazu befähigt werden, sich in einer hybriden Bezahlwelt risikoarm zu bewegen. Da immer mehr*

---

<sup>246</sup> Die Fachverbände für Menschen mit Behinderung (26.10.2021), 7 f.

*Menschen digitale Kanäle nutzen, muss Überschuldungsprävention hybrid ausgerichtet sein.*<sup>247</sup>

Anwendungen des digitalen Zahlungsverkehrs sollten Funktionen der Ausgabenkontrolle beinhalten. Während früher vor allem gelehrt wurde, dass ausschließlich Bargeld lehre, den Überblick zu behalten, kann diese Sichtweise ausdifferenziert werden.<sup>248</sup> So ermöglichen einige Banking-Apps es bereits, die Kontobewegungen zu analysieren und dadurch einen Überblick über die Ausgabenstruktur zu haben. So kann ein guter Überblick über vergangene Ausgaben geschaffen werden. Insofern schafft der digitale Zahlungsverkehr zumindest ex-post eine Ausgabenkontrolle. Finanzielle Bildungsangebote müssen auf diese Möglichkeit nicht nur hinweisen, sondern auch die Notwendigkeit begründen, Tools zur Ausgabenkontrolle zu nutzen.

Da der Zahlungsverkehr immer mehr digital stattfindet, muss digitale Kompetenz als Teil der finanziellen Kompetenz gefördert werden. Dies wird auch von der OECD so gesehen, denn sie hat in ihrem Vorschlag für die deutsche Finanzbildungsstrategie eben diesen Aufbau von digitaler Finanzkompetenz betont und Empfehlungen, die auf eine sichere Nutzung digitaler Finanzdienstleistungen gerichtet sind, formuliert.<sup>249</sup>

## **2.2 Unterstützungsmöglichkeiten: Kompetenzen verbessern und Kapazitäten aufbauen**

Vor allem beim digitalen Zahlungsverkehr sind zusätzliche Kompetenzen sowohl bei Anbieter:innen als auch Nutzer:innen notwendig, um den inklusiven Zugang zu gewährleisten. So ist im BargeldVO-Vorschlag vermerkt, dass die Mitgliedstaaten dabei unterstützt werden, „ihre politischen Bemühungen zur Förderung der digitalen finanziellen Inklusion fortzusetzen, beispielsweise durch Maßnahmen zur Verbesserung der Finanzkompetenz und insbesondere der digitalen Finanzkompetenz im Rahmen der allgemeinen und beruflichen Bildungssysteme [...]“.<sup>250</sup> Im Folgenden wird zunächst auf die Implikationen auf Anbieterseite und anschließend auf die Implikationen für die Nutzer:innenseite eingegangen.

Voraussetzung für den Zugang zum digitalen Zahlungsverkehr ist der Zugang zu einem Zahlungskonto und entsprechend die Umsetzung des gesetzlich verankerten Rechts auf ein Basiskonto. Hierfür müssen Banken ein klares Verständnis über die Anforderungen des ZKG haben. So sollten Bankmitarbeiter:innen mit Kundenkontakt vollständige Kenntnisse über die gesetzliche Regulierung haben und somit bei Anspruch allen Kund:innen, unabhängig von ihrer finanziellen Situation, die Möglichkeit der Eröffnung eines Basiskontos anbieten.<sup>251</sup>

Um Zugangsbarrieren in Bezug auf fehlende Kompetenz auf Verbraucherseite zu beheben, bedarf es persönlicher Unterstützung bei der Nutzung von digitalen Bezahlmethoden durch die Anbieter. Hierfür braucht es physische Anlaufstellen, die weiterhin niedrigschwellig telefonisch, aber auch persönlich und schriftlich erreichbar sind. So verpflichtet beispielsweise § 12 BFSGV die Banken,

---

<sup>247</sup> Themenpapier BdZ-DG (2024a), S. 2.

<sup>248</sup> Das zeigt auch das Beispiel der Zahlungskarte, denn hier haben Menschen ja gar nicht die Möglichkeit, ihr gesamtes Geld abzugeben und sie ausschließlich in Form von Bargeld zu nutzen.

<sup>249</sup> OECD (2024), 24f.

<sup>250</sup> Erwägungsgrund 14 BargeldVO-Vorschlag.

<sup>251</sup> FEANTSA (Januar 2022), S. 8.

Unterstützungsdienste wie Help-Desk, Call-Center und Schulungsdienste barrierefrei anzubieten. Je nach den Bedürfnissen der Kund:innen sind dabei unterschiedliche Kommunikationswege erforderlich. Wichtig dabei ist eine Erreichbarkeit rund um die Uhr, wodurch unnötige Wartezeiten zu vermeiden sind. Zweifelsohne kann Bankkund:innen besser geholfen werden, wenn sie sofort jemanden erreichen können.<sup>252</sup> Dafür bedarf es allerdings bei den Finanzdienstleistern ausreichender Kapazitäten.

Neben der Kapazitätsfrage, ist der Zugang zur Unterstützung auch eine Frage der Kompetenzen der Bankmitarbeiter:innen. Neben Geduld und Einfühlungsvermögen der Bankmitarbeiter:innen beim Umgang mit verschiedenen, insbesondere unterstützungsbedürftigen Personengruppen, ist hierfür auch unterschiedliches (Erfahrungs-) Wissen unabdingbar.<sup>253</sup> Bankkund:innen kann besser geholfen werden, wenn sie mit jemandem sprechen können, der Erfahrung mit der Zielgruppe und den Hindernissen hat, auf die sie stoßen, und der auch ihre Sprache (oder Gebärdensprache) spricht.<sup>254</sup>

Für die finanzielle Eingliederung ausgegrenzter Personengruppen mit komplexen Herausforderungen kann auch über spezialisierte Beauftragte nachgedacht werden. Diese sollten hochqualifiziert sein und die Besonderheiten der ausgegrenzten Personengruppe kennen sowie Kenntnisse über informelle finanzielle Netzwerke in der jeweiligen Gemeinschaft haben. Zudem sollten diese spezialisierten Beauftragten Bedürfnisse dieser Personengruppen analysieren und an Anbieter und Politik kommunizieren, um eine Verbesserung des Zugangs zum digitalen Zahlungsverkehr durch eine Weiterentwicklung der personellen Kompetenzen und der technischen Ausstattung zu bewirken.<sup>255</sup>

Umfassende Unterstützung für alle Verbrauchergruppen wird durch den DigEUR-Vorschlag vorgesehen. Sowohl Zahlungsdienstleister als auch öffentliche Stellen (z. B. lokale oder regionale Behörden oder Postämter) haben Menschen mit Behinderungen, funktionalen Einschränkungen oder begrenzten digitalen Fähigkeiten sowie älteren Menschen Unterstützung bei der digitalen Inklusion an Ort und Stelle anzubieten (Art. 14 Abs. 3 lit. b, Abs. 4 DigEUR-Vorschlag). Diese Unterstützung umfasst bei der digitalen Inklusion eine spezielle Hilfe beim Onboarding eines Kontos für den digitalen Euro und der Nutzung aller grundlegenden Zahlungsdienste im Zusammenhang mit dem digitalen Euro.

Dieser Ansatz für den digitalen Euro ist auf den digitalen Zahlungsverkehr zu erweitern. Der praktische Bedarf an umfassender Unterstützung geht über den digitalen Euro hinaus und macht sich insbesondere durch die Filienschließungen bemerkbar. Zunehmend fehlt es an Anlaufstellen und Ansprechpartner:innen. Aus diesem Grund wäre eine ähnliche Unterstützungspflicht im PSR-E für alle Verbrauchergruppen wünschenswert.

Zudem sind die Banken in Verantwortung zu nehmen, ihre Mitarbeiter:innen zielgruppenorientiert zu sensibilisieren. Ein gutes Beispiel in dieser Hinsicht liefern die niederländischen Banken. Die vier größten niederländischen Banken haben eine Sensibilisierungskampagne unter ihren eigenen

---

<sup>252</sup> De Nederlandsche Bank (2023), S. 8.

<sup>253</sup> De Nederlandsche Bank (2023), S. 8. BAGSO (2022), S. 41

<sup>254</sup> De Nederlandsche Bank (2023), S. 8.

<sup>255</sup> Ozili (2020), S. 12.

Mitarbeiter:innen gestartet. Dafür haben sie Videos entwickelt, die zeigen, auf welche Hürden Menschen unterschiedlicher Zielgruppen beim (digitalen) Banking stoßen und wie die Bankmitarbeiter:innen zielgruppenorientiert Unterstützung leisten können.<sup>256</sup>

Eine Schulungspflicht sieht Art. 84 Abs. 2 PSR-E für Betrugsfälle vor. Dementsprechend organisieren die Zahlungsdienstleister für ihre Mitarbeiter:innen, die im Bereich der Konzeption und Aufrechterhaltung von Zahlungsdiensten und deren Angebot an die Kund:innen tätig sind, mindestens jährlich Schulungsprogramme zu den Risiken und Trends in Sachen Zahlungsbetrug und stellen sicher, dass ihre Mitarbeiter:innen angemessen ausgebildet sind, um ihre Aufgaben und Verantwortlichkeiten zur Minderung und Steuerung von Zahlungsbetrugsrisiken wahrnehmen zu können.

Diese Schulungspflicht ist auf den Zahlungsverkehr im Allgemeinen und mit Bezug auf die Kundenorientierung zu erweitern. Die im Art. 84 Abs. 2 PSR-E vorgesehene Schulungspflicht ist zwar zum Zwecke der Betrugsprävention sehr zu begrüßen, allerdings geht der Bedarf in der Praxis über die Betrugsprävention hinaus und umfasst den Zahlungsverkehr im Allgemeinen. Zudem stellen die Bedürfnisse unterschiedlicher Kundengruppen eine Herausforderung für Bankmitarbeiter:innen dar. Zur Entwicklung und Verbesserung ihrer Fähigkeiten, zielgruppenorientierte Unterstützung im Zahlungsverkehr leisten zu können, sollten die Bankmitarbeiter:innen auch zielgruppenspezifisch geschult werden.

Nicht zuletzt ist die Sensibilisierung der Verbraucher:innen bei der Bewältigung einiger Hürden von Bedeutung. Eine solche Maßnahme sieht beispielsweise Art. 84 Abs. 1 PSR-E vor. Dementsprechend sieht die vorgeschlagene Vorschrift vor, dass die Banken ihren Kund:innen klare Hinweise geben, wie sie Betrugsversuche erkennen können, und welche Maßnahmen und Vorkehrungen sie treffen müssen, um keinen betrügerischen Handlungen zum Opfer zu fallen. Darüber hinaus sollen die Banken ihre Kund:innen auf allen geeigneten Wegen und durch die Medien warnen, wenn neue Formen von Zahlungsbetrug aufkommen, wobei sie den Bedürfnissen ihrer schutzbedürftigsten Kundengruppen Rechnung tragen.

Auch diese Maßnahme ist themenübergreifend anzubieten. Zweifellos ist die Sensibilisierung von Verbraucher:innen von ausschlaggebender Bedeutung. Allerdings geht der Bedarf, digitale Kompetenzen aufzubauen und zu verbessern, über Betrugsfälle hinaus. Derzeit werden solche Bildungs- und Schulungsangebote durch Sozialverbände angeboten, wie z. B. durch die Bundesarbeitsgemeinschaft der Seniorenorganisationen (BAGSO).<sup>257</sup> Am Beispiel der durch die Sozialverbände geleisteten Arbeit sollten vielmehr die Banken solche Bildungs- und Schulungsangebote übernehmen oder sie finanzieren. Da die Bankwirtschaft mittlerweile größtenteils auf eine Digitalisierung ihrer Angebote abstellt, darf sie ihre Kund:innen nicht sich selbst überlassen.<sup>258</sup> An erster Stelle ist es ihre Pflicht, ihre Kund:innen mitzunehmen, und zwar auch diejenigen, die aus unterschiedlichen Gründen nicht mithalten können.

---

<sup>256</sup> S. Auftakt der Sensibilisierungskampagne „1op6“ für Bankmitarbeiter:innen, abrufbar auf: [https://toegankelijkbankieren.nl/?mailpoet\\_router&endpoint=view\\_in\\_browser&action=view&data=WzlwLCIzODRiYjM4MGIxMjgiLDQ0NiwiYzU5OTNiZGQwOGRkZGQxMWNiYzU2N2MxMGEwZDhkMzUiLDE2LDBd](https://toegankelijkbankieren.nl/?mailpoet_router&endpoint=view_in_browser&action=view&data=WzlwLCIzODRiYjM4MGIxMjgiLDQ0NiwiYzU5OTNiZGQwOGRkZGQxMWNiYzU2N2MxMGEwZDhkMzUiLDE2LDBd), Letzter Abruf: 20. November 2024.

<sup>257</sup> Interview mit Frau Alexandra Ziegler, BAGSO.

<sup>258</sup> Fohrer (2024).

### 3. Fehlende Bereitschaft adressieren

Um die Barriere der fehlenden Bereitschaft zu adressieren, muss zum einen Anonymität beim Zahlungsverkehr ermöglicht werden und zum anderen Vertrauen in die Digitalisierung des Zahlungssystems gestärkt werden. Im Folgenden werden entsprechende regulatorische Implikationen herausgearbeitet.

#### 3.1 Anonymität bzw. Schutz der Privatsphäre ermöglichen

Die Verarbeitung personenbezogener Daten im Rahmen der Zahlungsdienste ist auf das Notwendigste zu beschränken. In dieser Hinsicht sind die Vorschriften der DSGVO maßgeblich. Der PSR-E, EP-Bericht stellt dies in Art. 1 Abs. 3a PSR-E klar. Allerdings sieht die künftige Verordnung zum Zwecke der Betrugsprävention Transaktionsüberwachungsmechanismen vor,<sup>259</sup> die u. a. die vorherigen Zahlungsvorgänge, Online-Zugriffe auf Zahlungskonten sowie die über die EBA IT-Plattform ausgetauschten Daten zum Betrug und beobachtete Betrugsmuster umfassen. Allerdings dürfen diese Daten nicht länger als erforderlich gespeichert werden und sind spätestens nach Beendigung der Kundenbeziehung zu löschen (Art. 83 Abs. 2 Unterabs. 2 PSR-E). Das EP hat diese Frist auf zehn Jahre nach Beendigung der Kundenbeziehung verlängert (Art. 83 Abs. 2 Unterabs. 4 PSR-E, EP-Bericht). Nicht zuletzt darf der Datenaustausch weder zur Beendigung der Kundenbeziehung noch zur Beeinträchtigung des künftigen Onboardings durch einen anderen Zahlungsdienstleister führen (Art. 83 Abs. 6 PSR-E). Das EP hat klargestellt, dass diese Regel nicht gilt, wenn die Beteiligung an betrügerischen Aktivitäten von Kontoinhaber:innen durch die zuständigen Behörden bestätigt wurde.

Ferner gestattet der PSR-E eine Ausnahme vom Verbot der Verarbeitung sensibler Daten. Gemäß Art. 9 Abs. 1 DSGVO ist die Verarbeitung sensibler Daten, beispielsweise Gesundheitsdaten und Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, grundsätzlich untersagt. Durch die Ergänzung des EP wird klargestellt, dass dieses Verbot auch für Zahlungsdienste gilt (Art. 1 Abs. 3a PSR-E, EP-Bericht). Allerdings sieht Art. 80 Abs. 1 PSR-E eine Ausnahme bei der Verarbeitung sensibler Daten vor, und zwar „im öffentlichen Interesse eines gut funktionierenden Zahlungsdienstebinnenmarkts“, soweit dies für die Erbringung von Zahlungsdiensten und für die Erfüllung der Verpflichtungen im Rahmen der Verordnung notwendig ist. Zur Bewahrung der Grundrechte und -freiheiten natürlicher Personen müssen die Zahlungsdienstleister bei der Verarbeitung sensibler Daten angemessene Vorkehrungen treffen, u. a. dafür, die Grundsätze der Zweckbindung, der Datenminimierung und der Speicherbegrenzung einzuhalten und u. a. modernste Sicherheits- und Datenschutzvorkehrungen zu treffen wie z. B. Pseudonymisierung oder Verschlüsselung. Somit konstatiert der PSR-E eine Ausnahme zum Verbot der Verarbeitung sensibler Daten im Rahmen des Art. 9 Abs. 2 lit. (j) DSGVO.

Die Erwägungsgründe der künftigen Verordnung beinhalten keine einschlägige Erläuterung dazu, aus welchem Grund die Verarbeitung sensibler Daten im öffentlichen Interesse eines gut funktionierenden Zahlungsdienstebinnenmarkts erforderlich sein könnten.<sup>260</sup> Art. 9 Abs. 2 DSGVO erlaubt die Verarbeitung sensibler Daten in bestimmten Fällen unter strengen Voraussetzungen. Da

---

<sup>259</sup> S. unten IV.3.2

<sup>260</sup> S. Erwägungsgrund 98 PSR-E.

die Verarbeitung sensibler Daten mit erheblichen Risiken für natürliche Personen einhergehen, sollten die neu einzuführenden Ausnahmen zu dem Verbot des Art. 9 Abs. 1 DSGVO sehr gut begründet werden. Da es an einer stichhaltigen Begründung für die Ausnahme des Art. 80 Abs. 1 PSR-E fehlt, sollte diese Vorschrift ersatzlos gestrichen werden.

Nicht zuletzt ist die Anonymität für den digitalen Euro von Bedeutung. Der digitale Euro wird sowohl für Online- als auch für Offline-Zahlungsvorgänge zur Verfügung stehen (Art. 23 Abs. 1 DigEUR-Vorschlag). Die begrenzten Transaktionsdaten aufgrund der Offline-Zahlungsvorgänge werden weder von den Zahlungsdienstleistern noch von der EZB bzw. den nationalen Zentralbanken aufbewahrt (Art. 37 Abs. 2 DigEUR-Vorschlag). Bei der Abwicklung von Offline-Transaktionen mit dem digitalen Euro wird die Verarbeitung personenbezogener Daten durch Zahlungsdienstleister auf die Aufladung- und Auszahlungsdaten beschränkt und lediglich zum Zwecke der Geldwäscheprävention im beschränkten Rahmen zulässig sein (Art. 37 Abs. 3, 4 DigEUR-Vorschlag). Ob diese Vorschriften so auch umgesetzt werden, kann an dieser Stelle nicht beurteilt werden. Gelingt es, dann wäre der digitale Euro eine echte Alternative zu herkömmlichen Online-Bezahlsystemen, welche die Skepsis der Verbraucher:innen zerstreuen und das fehlende Vertrauen herstellen könnte.

### 3.2 Vertrauen stärken durch Betrugsprävention

Um das Vertrauen der Verbraucher:innen in den digitalen Zahlungsverkehr zu erhöhen,<sup>261</sup> sieht der PSR-E zahlreiche Maßnahmen zur Betrugsprävention vor. Die EU-Verordnungen sind unmittelbar anwendbar und ihre Vorschriften dürfen als Anspruchsgrundlage dienen. Die intendierten unmittelbar anwendbaren Rechtsvorschriften verbieten aufgrund eines Vorrangs des Europarechts nationale Alleingänge. Insofern wird die künftige PSR-E die Rechtsverhältnisse zwischen Zahlungsdienstleistern und -nutzer:innen vereinheitlichen, und noch existierende abweichende nationale Vorschriften werden nach dem Inkrafttreten der Verordnung nicht mehr anwendbar sein.

Gleichwohl erlaubt die künftige Verordnung den Mitgliedstaaten, in bestimmten Fällen günstigere Ansprüche für Zahlungsdienstnutzer:innen zu schaffen (Art. 107 Abs. 1 PSR-E). Dazu gehören die Haftung des Zahlungsdienstleisters für eine fehlerhafte Anwendung beim Abgleichservice (Art. 57 PSR-E) und die Haftung des Zahlungsdienstleisters in Fällen von Identitätsbetrug (Art. 59 PSR-E). Nicht zuletzt erlaubt Art. 107 Abs. 1 PSR-E strengere Betrugsbekämpfungsmaßnahmen, die über die durch die Verordnung festgelegten Maßnahmen hinausgehen.

Im Folgenden werden die durch den Vorschlag vorgesehenen Maßnahmen erläutert und die eventuell bestehenden Schutzlücken herausgearbeitet. Dabei wird an entsprechenden Stellen ausgeführt, welche günstigeren Ansprüche i. S. v. Art. 107 AEUV der deutsche Gesetzgeber für Zahlungsdienstnutzer:innen vorsehen könnte.

#### Transparenz

Das Verhalten der Banken in Betrugsfällen fließt derzeit in die Entscheidungsfindung der Verbraucher:innen bei der Wahl einer Bank möglicherweise nicht ein, obwohl es einen erheblichen Einfluss auf das Vertrauen in den Finanzsektor haben könnte. Viele Verbraucher:innen konzentrieren sich bei der Wahl ihrer Bank hauptsächlich an Kriterien wie hohe Sicherheit beim

---

<sup>261</sup> Zahrte (2024a), S. 136.

Online-Banking, kostenloses Girokonto und eine hohe Dichte von Geldautomaten. Sicherheit hat also grundsätzlich eine Relevanz; die Frage, wie eine Bank aber dann auf Betrugsfälle reagiert, bleibt oft unbeachtet. Dabei könnte das Vertrauen in die Sicherheitsmaßnahmen einer Bank und ihre Transparenz im Umgang mit Betrug das Verhalten und die Wahrnehmung der Kundschaft erheblich beeinflussen. Ein solcher Fokus könnte langfristig nicht nur die Kundenzufriedenheit, sondern auch die Reputation der Bank stärken.<sup>262</sup> Nach geltendem Recht haben die Zahlungsdienstleister gemäß § 54 Abs. 5 ZAG (Art. 96 Abs. 6 PSD2) der BaFin mindestens einmal jährlich statistische Daten zu Betrugsfällen in Verbindung mit den unterschiedlichen Zahlungsmitteln vorzulegen. Die Bundesanstalt hat der Europäischen Bankenaufsichtsbehörde (EBA) und der EZB die vorgelegten Daten in aggregierter Form zur Verfügung zu stellen. Art. 82 PSR-E ändert an dieser Pflicht zur Berichtserstattung nichts (Art. 82 Abs. 1 PSR-E). Das EP hat allerdings diese Vorschrift durch den Umfang der zu berichtenden Daten ergänzt (Art. 82 Abs. 1 Unterabs. 2 PSR-E, EP-Bericht). Des Weiteren hat das EP die Pflicht der EBA und der EZB, die statistischen Daten mindestens einmal jährlich zu veröffentlichen, ausdrücklich geregelt (Art. 82 Abs. 1a PSR-E, EP-Bericht).

Zur Unterstützung von informierten Entscheidungen der Verbraucher:innen sollten diese statistischen Informationen zu Betrugsfällen und zum Verhalten der Bank bezüglich der Erstattungsansprüche von Verbraucher:innen auf nationaler Ebene bankspezifisch offengelegt werden. Der durch das EP hinzugefügte Art. 82 Abs. 1 Unterabs. 2 PSR-E (EP-Bericht) sieht vor, dass die statistischen Daten die Anzahl und die Höhe der erstatteten betrügerischen Transaktionen sowie die Gründe für die Verweigerung der Erstattung, etwa die betrügerische Absicht oder das grob fahrlässige Verhalten der Verbraucher:innen, umfassen muss. Nach der teleologischen Auslegung sollte die Vorschrift auch die Anzahl der Fälle umfassen, in denen der Erstattungsanspruch verweigert wurde, und nicht lediglich die Gründe der Verweigerung. Zudem sollten die Zahlen nicht nur als europäische Statistiken veröffentlicht werden, sondern auch auf nationaler Ebene. Nicht zuletzt sollte die nationale Veröffentlichung bankspezifisch erfolgen, sodass die Verbraucher:innen (sowie unterstützend die Verbraucherschutzorganisationen) diese Informationen, also die Anzahl der Betrugsfälle und das Verhalten der jeweiligen Bank, in die Entscheidungsfindung einfließen lassen können. Man könnte argumentieren, dass bankspezifische Informationen die Betrüger dazu ermuntern, bestimmte Banken ins Visier zu nehmen, und dadurch Sicherheitsrisiken für die Banken entstehen würden. Allerdings sind die Banken, nicht zuletzt durch die DORA,<sup>263</sup> verpflichtet, die technologische Sicherheit ihrer operativen Systeme zu gewährleisten. Der Zweck dabei besteht nicht nur in der Widerstandsfähigkeit des europäischen Finanzsektors, sondern auch in der wirksamen und reibungslosen Erbringung der Finanzdienstleistungen auch in Stresssituationen sowie in der Gewährung des Verbrauchervertrauens.<sup>264</sup> Man könnte auch argumentieren, dass Betrugsfälle außerhalb des Einflusses der Bank liegen und daher die Veröffentlichung der statistischen Daten für die Banken unfair wären. Doch, wie unten noch zu sehen ist, müssen die Banken bestimmte präventive Maßnahmen einsetzen. Zudem liegt es vollkommen im Ermessen der Bank, wie sie auf die Ansprüche der Verbraucher:innen reagieren.

---

<sup>262</sup> Statista/YouGov (2020); im Rahmen der Studie wurden 2.076 Personen in Deutschland befragt.

<sup>263</sup> Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABL. 2022 L 333/1 (DORA).

<sup>264</sup> Erwägungsgrund 6 DORA.

Genau diese Information ist für die Entscheidungsfindung von Verbraucher:innen von erheblicher Bedeutung.

Durch die Veröffentlichung der statistischen Informationen zu Betrugsfällen würde nicht nur ein Anreiz für sichere Zahlungssysteme und Wettbewerb geschaffen, sondern auch das Engagement der Banken ihren Kund:innen gegenüber gefördert. Sollte das im PSR-E vorgesehene Haftungsregime in Betrugsfällen unverändert bleiben,<sup>265</sup> könnten dieser Anreiz und das Engagement auch durch die Aufnahme der oben genannten bankspezifischen Informationen in die vorvertraglichen Informationspflichten (Art. 20 PSR-E) erzielt werden. Derzeit haben die Zahlungsdienstleister mit Bezug auf Betrugsfälle lediglich diejenigen Informationen vorvertraglich mitzuteilen, die die Schutz- und Anzeigepflichten der Zahlungsdienstnutzer:innen betreffen, wie z. B. die Vorkehrungen, die die Zahlungsdienstnutzer:innen für die sichere Aufbewahrung eines Zahlungsinstruments zu treffen haben oder wie und innerhalb welcher Frist sie dem Zahlungsdienstleister nicht autorisierte oder fehlerhaft ausgelöste oder ausgeführte Zahlungsvorgänge anzeigen müssen.<sup>266</sup>

### **Ausgabenobergrenzen**

Als eine allgemeine Maßnahme zum Schutz vor Betrug kommen in der künftigen europäischen Gesetzgebung Ausgabenobergrenzen in Betracht. Diese sind bereits für Echtzeitüberweisungen vorgesehen, falls die Zahlungsdienstnutzer:innen wünschen, einen per Echtzeitüberweisung versendbaren Höchstbetrag festzulegen (Art. 5a Abs. 6 SEPA-VO). Sie können entweder pro Tag oder pro Zahlungsvorgang festgelegt und jederzeit geändert werden. Sollte ein Zahlungsauftrag für eine Echtzeitüberweisung den festgelegten Höchstbetrag überschreiten, ist der Zahlungsdienstleister verpflichtet, den Zahlungsauftrag nicht auszuführen und dies den Zahlungsdienstnutzer:innen mitzuteilen. Die Mitteilung hat auch die Information zu enthalten, wie der Höchstbetrag geändert werden kann. In gleicher Weise sieht Art. 51 Abs. 1 PSR-E vor, dass eine vertragliche Vereinbarung zu angemessenen und verhältnismäßigen Ausgabenobergrenzen möglich ist. Zudem sind sie standardmäßig auf einem niedrigen Niveau festzulegen.

Die Erfahrungen aus der Praxis zeigen allerdings, dass die Ausgabenobergrenzen keine effektive Maßnahme zum Schutz vor Betrug darstellen. Sollten diese bereits festgelegt worden sein, erhöhen die Betrüger als Erstes diese Obergrenze oder geben einfach mehrere Zahlungsvorgänge im Betrag der Höchstgrenze in Auftrag, nachdem sie ihr eigenes Endgerät mit dem Online-Banking verknüpft haben. Aus diesem Grund sollte es den Vertragsparteien möglich sein, eine Änderung der Ausgabenobergrenzen erst nach einer bestimmten Frist, z. B. erst nach 24 Stunden, umzusetzen. Innerhalb dieses Zeitraums sollten die Nutzer:innen die Möglichkeit haben, die Änderung der Ausgabenobergrenze zu widerrufen.

### **Empfängerüberprüfung**

Eine weitere Maßnahme zur Verringerung des Betrugsrisikos stellt die Empfängerüberprüfung dar.<sup>267</sup> Dies ist bereits in Art. 5c SEPA-VO für alle Überweisungen vorgeschrieben. Im Euroraum gilt diese

---

<sup>265</sup> Dazu unten mehr, s. 0.

<sup>266</sup> Art. 52 Nr. 5 lit. a und e PSD2, Art. 248 § 4 Abs. 1 Nr. 5 lit. a und e EGBGB i.V.m. § 675d Abs. 1 BGB.

<sup>267</sup> Erwägungsgrund 70 PSR-E.

Pflicht ab dem 9. Oktober 2025, für die in der EU ansässigen Zahlungsdienstleister ab 9. Juli 2027 (Art. 5c Abs. 9 SEPA-VO). Dementsprechend gleicht der Zahlungsdienstleister vor der Autorisierung des Zahlungsauftrags den Kundenidentifikator<sup>268</sup> mit den Namen von Zahlungsempfänger:innen ab. Bei fehlender Übereinstimmung unterrichtet der Zahlungsdienstleister die Kund:innen hierüber und teilt auch mit, dass die Autorisierung des Zahlungsvorgangs dazu führen könnte, dass die Gelder auf Zahlungskonten überwiesen werden, deren Inhaber:innen nicht die angegebenen Zahlungsempfänger:innen sind.<sup>269</sup>

Die gleiche Maßnahme ist ebenfalls in Art. 50 Abs. 1 PSR-E vorgesehen. Gemäß Art. 50 Abs. 8 PSR-E wird die Empfängerbestätigung bei Echtzeitüberweisungen der SEPA-VO und bei sonstigen Überweisungen der künftigen ZDVO unterliegen. Gemäß Art. 50 Abs. 1 PSR-E hat der Zahlungsdienstleister die Empfängerüberprüfung kostenlos anzubieten. Anders als die SEPA-VO sieht Art. 50 Abs. 4 PSR-E allerdings vor, dass die Zahlungsdienstleister allen Zahlungsdienstnutzer:innen die Möglichkeit anbieten, auf die Empfängerüberprüfung zu verzichten. Gemäß Art. 5c Abs. 6 SEPA-VO besteht die Verzichtmöglichkeit dagegen lediglich für Zahlungsdienstnutzer, die keine Verbraucher:innen sind, und wenn sie mehrere Echtzeitüberweisungsaufträge als Bündel einreichen.

Eine Empfängerbestätigung sollte bei Zahlungsaufträgen von Verbraucher:innen zumindest für Überweisungen im SEPA-Raum ohne eine Verzichtmöglichkeit zu gestalten sein. Dadurch wird nicht nur dem Schutz vor Betrug Rechnung getragen, sondern auch eine eventuell unterschiedliche Regelung zwischen Echtzeitüberweisungen und normalen Überweisungen verhindert. Die Empfängerbestätigung ohne Verzichtmöglichkeit kann sogar auf alle Überweisungen an diejenigen Länder erweitert werden, die Teil des IBAN-Systems sind.<sup>270</sup> Zudem ist sicherzustellen, dass die Verbraucher:innen in der Praxis nicht zum Verzicht verleitet werden, wie etwa durch vorgeklickte Boxen. Wie noch unten verdeutlicht werden wird, schließt ein Verzicht dann auch eine Haftung des Zahlungsdienstleisters für den Fall einer unsorgfältig durchgeführten Empfängerüberprüfung aus.

## Transaktionsüberwachung

Um betrügerische Transaktionen besser zu verhindern und aufzudecken, wird die Pflicht der Zahlungsdienstleister, über Transaktionsüberwachungsmechanismen zu verfügen, im PSR-E geregelt. Derzeit wird diese Pflicht lediglich in der SKA-DVO geregelt und bezieht sich ausdrücklich auf die starke Kundenauthentifizierung. Wie oben erläutert, ist dies derzeit beim Mitverschulden der Banken relevant. Durch die künftige ZDVO wird diese Pflicht ausdrücklich mit Betrugsprävention in Verbindung gebracht. Gemäß Art. 83 Abs. 1 lit. c PSR-E müssen die Zahlungsdienstleister über Transaktionsüberwachungsmechanismen verfügen, die ihnen die Möglichkeit geben, potenziell betrügerische Zahlungsvorgänge zu verhindern und aufzudecken. Das EP hat die Vorschrift dahingehend revidiert, dass die Aufdeckung und Verhinderung von betrügerischen

---

<sup>268</sup> Im SEPA-Raum ist dies die internationale Bankkontonummer (IBAN), s. Nr. 1 lit. a. Anhang SEPA-VO; s. auch Omlor (2024), S. 3479.

<sup>269</sup> Mehr dazu s. Omlor (2024), S. 3483 f.

<sup>270</sup> Gemäß Art. 50 Abs. 1 PSR-E ist die Überprüfung anhand des Kundenidentifikators durchzuführen. Art. 3 Nr. 39 PSR-E definiert den Kundenidentifikator als „eine Kombination aus Buchstaben, Zahlen oder Symbolen, die der Zahlungsdienstleister dem Zahlungsdienstnutzer mitteilt und die der Zahlungsdienstnutzer angeben muss, damit ein anderer am Zahlungsvorgang beteiligter Zahlungsdienstnutzer oder das Zahlungskonto dieses anderen Zahlungsdienstnutzers bei einem Zahlungsvorgang zweifelsfrei ermittelt werden kann.“ Im EP-Bericht wird klargestellt, dass der Kundenidentifikator nicht die IBAN sein muss (Erwägungsgrund 70, Art. 3 Nr. 39 PSR-E, EP-Bericht). Aus diesem Grund beauftragt Art. 3 Unterabs. 2 PSR-E, EP-Bericht die EBA, eine Liste der Methoden festzulegen, die als Kundenidentifikator verwendet werden können.

Zahlungsvorgängen nicht mehr als „Möglichkeit“ dargestellt wird. Zudem hat das EP die Pflicht, betrügerische Zahlungsvorgänge zu verhindern, aufzudecken und so weit möglich aufzulösen, hinzugefügt (Art. 83 Abs. 1 lit. c PSR-E, EP-Bericht). Diese Mechanismen stützen sich auf die Analyse früherer Zahlungsvorgänge und Online-Zugriffe auf Zahlungskonten sowie auf die ausgetauschten Daten zum Betrug und beobachtete Betrugsmuster. Zu diesem Zweck werden u. a. Informationen über Zahlungsdienstnutzer:innen einschließlich umgebungs- und verhaltensbezogener Merkmale, die für die Zahlungsdienstnutzer:innen im Rahmen einer normalen Verwendung der personalisierten Sicherheitsmerkmale typisch sind, und Informationen über Zahlungskonten einschließlich Zahlungsvorgangshistorien verwendet (Art. 83 Abs. 2 PSR-E).

Auf der Grundlage dieser Transaktionsüberwachung, stellt der PSR-E zahlreiche konkrete Maßnahmen zur Verfügung, die die Zahlungsdienstleister treffen können, um die Zahlungsdienstnutzer:innen zu schützen. Das Ziel des europäischen Gesetzgebers, dass die Zahlungsdienstleister für jegliche durch Betrug verursachten finanziellen Verluste der Zahlungsdienstnutzer:innen aufkommen, wenn sie nicht über die geeigneten Mechanismen zur Verhinderung von Betrug verfügen, bzw. diese nicht einsetzen, kommt im EP-Bericht ganz klar zum Ausdruck.<sup>271</sup> Teleologisch sollten die Zahlungsdienstleister auch dann für die durch Betrug verursachten finanziellen Verluste der Zahlungsdienstnutzer:innen aufkommen, wenn sie über solche Mechanismen verfügen, aber diese bei der Betrugsprävention nicht bzw. nicht ordnungsgemäß einsetzen.

Die erste Möglichkeit, die Zahlungsdienstleister haben, ist die Blockierung des Zahlungsauftrags. Diese Maßnahme wurde nicht durch die Kommission, sondern durch das EP vorgeschlagen. Gemäß Art. 83 Abs. 2 Unterabs. 2 PSR-E, EP-Bericht, haben Zahlungsdienstleister das Recht, die Ausführung des Zahlungsauftrags zu blockieren oder die entsprechenden Beträge zu sperren und wiedereinzuziehen, wenn die Transaktionsüberwachungsmechanismen stichhaltige Anhaltspunkte für den Verdacht auf eine betrügerische Transaktion liefern oder wenn Zahlungsdienstnutzer:innen dem Zahlungsdienstleister einen Polizeibericht übermitteln.

Diese Maßnahme ist allerdings dem Ermessen des Zahlungsdienstleisters überlassen. Nach ihrem klaren Wortlaut begründet die Vorschrift keine Pflicht zur Blockierung für die Zahlungsdienstleister. Um einen umfassenden Schutz für die Zahlungsdienstnutzer:innen herzustellen, sollte ein Ermessen durch eine Pflicht ersetzt und diese zugleich, wie eigentlich intendiert,<sup>272</sup> mit einer Regelung zur Haftung des Zahlungsdienstleisters bzw. zur Haftungsbefreiung für die Zahlungsdienstnutzer:innen gekoppelt werden, falls der Zahlungsdienstleister dieser Pflicht nicht nachkommt.<sup>273</sup>

Eine weitere Maßnahme stellt die Sperrung des Zahlungsinstruments dar. Gemäß Art. 51 Abs. 2 PSR-E kann sich der Zahlungsdienstleister das Recht vorbehalten, ein Zahlungsinstrument zu sperren, wenn der Rahmenvertrag eine dahingehende Vereinbarung enthält und wenn objektive Gründe im Zusammenhang mit der Sicherheit des Zahlungsinstruments dies rechtfertigen oder wenn der Verdacht auf eine nicht autorisierte oder betrügerische Nutzung des Zahlungsinstruments besteht. Eine Sperrung des Zahlungsinstrumentes ist ferner möglich, wenn damit eine Kreditlinie in

---

<sup>271</sup> Erwägungsgrund 100 PSR-E, EP-Bericht.

<sup>272</sup> S. Erwägungsgrund 103b PSR-E, EP-Bericht.

<sup>273</sup> S. dazu unten den Unterabschnitt „Haftung des Zahlungsdienstleisters“.

Zusammenhang steht und ein erheblich erhöhtes Risiko besteht, dass der Zahler seiner Zahlungspflicht nicht nachkommen kann. Dabei handelt es sich allerdings vielmehr um eine Option für den Zahlungsdienstleister als um eine Pflicht. Das EP hat daher die Vorschrift dahingehend geändert, dass die Sperrung des Instruments nicht mehr dem Ermessen des Zahlungsdienstleisters überlassen ist und es keiner gesonderten Vereinbarung im Rahmenvertrag bedarf. Insofern handelt es sich im PSR-E, EP-Bericht um eine ausdrückliche Pflicht. In beiden Versionen des Vorschlags ist die Rechtsvorschrift allerdings nicht ausdrücklich mit der Transaktionsüberwachung verknüpft. Um Klarheit zu schaffen, sollte in der Vorschrift Erwähnung finden, dass der Verdacht einer nicht autorisierten oder betrügerischen Nutzung des Zahlungsinstruments aus den Transaktionsüberwachungsmechanismen hergeleitet werden kann.

Aus den Transaktionsüberwachungsmechanismen folgen Handlungsmöglichkeiten mit Bezug auf Betrugsprävention auch für die Zahlungsdienstleister der Zahlungsempfänger:innen. Nach dem durch das EP hinzugefügten Art. 69 Abs. 2a PSR-E (EP-Bericht) kann der Zahlungsdienstleister der Zahlungsempfänger:innen die sofortige Bereitstellung des Geldbetrags auf dem Zahlungskonto der Zahlungsempfänger:innen verweigern, wenn die Transaktionsüberwachung einen hinreichenden Verdacht auf einen betrügerischen Zahlungsvorgang begründet. Erfolgt eine solche Verweigerung, lässt sich der Zahlungsdienstleister von den Zahlungsempfänger:innen unverzüglich über den vermuteten betrügerischen Zahlungsvorgang aufklären und macht die Mittel je nach Ergebnis entweder verfügbar oder sendet sie an den kontoführenden Zahlungsdienstleister der Zahler:innen zurück.

Nach dem eindeutigen Wortlaut der Vorschrift sind allerdings Zahlungsdienstleister von Zahlungsempfänger:innen nicht verpflichtet, diese Maßnahme durchzuführen. Dies kann in der Praxis zur Folge haben, dass es den Betrügern weiterhin ermöglicht wird, die ihren Konten gutgeschriebenen Beträge schnellstmöglich auf ein anderes, womöglich außerhalb der EU liegendes Konto zu überweisen. Aus diesem Grund sollte es für die Zahlungsdienstleister der Zahlungsempfänger:innen verpflichtend sein, die Gutschrift auf das Konto zu blockieren, wenn ein hinreichender Verdacht auf einen Betrugsfall vorliegt, bzw. wenn ihnen gemeldet wurde, dieses Konto sei an betrügerischen Vorgängen beteiligt. Da die Mitgliedstaaten über die Verordnung hinausgehende Betrugsbekämpfungsmaßnahmen treffen können (Art. 107 Abs. 1 PSR-E), wäre es möglich, diese Pflicht auch im deutschen Recht zu verankern.

Das EP hat zudem eine weitere Vorschrift hinzugefügt, die den Zahlungsdienstleister verpflichtet, Überweisungen auf solche Konten zu sperren, die ihm als betrügerisch gemeldet wurden oder die an nachweislich betrügerischen Vorgängen beteiligt waren. Der PSR-E sieht vor, dass die Zahlungsdienstleister bestimmte Informationen austauschen, um am Betrug beteiligte Kundenidentifikatoren<sup>274</sup> identifizieren zu können (Art. 83 Abs. 3 ff. PSR-E). Liegen aufgrund eines solchen Austauschs dem Zahlungsdienstleister konkrete Informationen vor, dass ein Kundenidentifikator für betrügerische Zwecke verwendet wird, ist der Zahlungsdienstleister verpflichtet, Überweisungen an diesen Kundenidentifikator zu sperren (Art. 83 Abs. 5a PSR-E, EP-Bericht).

---

<sup>274</sup> Für den Begriff s. oben Fn. 270 und 268.

## Widerrufsfrist

Betrugspräventiv und somit vertrauensfördernd, kann auch eine länger bestehende Widerrufsfrist sein. Eine schnelle Abwicklung von Zahlungsvorgängen ist Segen und Fluch zugleich. So begünstigt eine schnelle Abwicklung auch Betrugsfälle. Eine Widerrufsfrist im Zahlungsverkehr bietet auch aus diesem Grund zusätzliche Sicherheit. Ebenso schützt sie vor unabsichtlichen Fehlern und verschafft Zeit, verdächtige Aktivitäten zu überprüfen und gegebenenfalls einzugreifen.

Beim Online-Banking ist ein Widerruf des Zahlungsauftrags gemäß der PSD2 und PSR-E nicht möglich. Wie die PSD2 ermöglicht der PSR-E den Widerruf der Autorisierung eines Zahlungsauftrags (Art. 49 Abs. 7 PSR-E).<sup>275</sup> Allerdings kann die Autorisierung nicht mehr widerrufen werden, nachdem der Zahlungsauftrag beim Zahlungsdienstleister eingeht (Art. 66 Abs. 1 PSR-E).<sup>276</sup> Beim Online-Banking ist dies regelmäßig der Zeitpunkt, an dem der Zahlungsauftrag beim Online-Banking-Server des Zahlungsdienstleisters eingeht. Aus diesem Grund können die Zahlungsaufträge, die über Online-Banking erteilt werden, nicht mehr widerrufen werden und müssen somit innerhalb der gesetzlichen Frist ausgeführt werden. Es wäre allerdings rechtsmissbräuchlich, wenn der Zahlungsdienstleister darauf besteht, den Zahlungsauftrag auszuführen, obwohl er mit seiner Ausführung noch nicht begonnen hat. Zudem wäre es auch rechtsmissbräuchlich, wenn der Zahlungsdienstleister die Rücknahme verweigern würde, obwohl sie keinen großen Betriebsaufwand auslösen würde.<sup>277</sup>

Gleichwohl steht es im Rahmen der Privatautonomie den Vertragsparteien frei, abweichende Vereinbarungen zum Widerruf von Zahlungsaufträgen zu treffen (Art. 66 Abs. 5 PSR-E).<sup>278</sup> Insofern können Zahlungsdienstleister und Zahlungsdienstnutzer:innen wirksam vereinbaren, dass der Widerruf der Zahlungsaufträge einer längeren als gesetzlichen Fristen unterliegen werden. Eine solche Vereinbarung würde auch für den Zeitraum getroffen werden, nachdem der Zahlungsdienstleister mit der Ausführung des Zahlungsvorgangs begonnen, aber der Zahlungsbetrag noch nicht dem Konto des/der Zahlungsempfänger:in gutgeschrieben wurde.<sup>279</sup>

Längere Widerrufsfristen könnten die Verbraucher:innen dazu befähigen, betrügerische Zahlungsaufträge zurück abzuwickeln. Wenn beispielsweise Zahlungsdienstnutzer:innen, die mit dem Online-Banking noch nicht vertraut sind, die Widerrufs-, und somit die Ausführungsfrist von Zahlungsaufträgen um 2 oder 3 Tage verlängern könnten, hätten sie in einem Betrugsfall die Möglichkeit, alle betrügerischen Zahlungsvorgänge zu widerrufen. In der Praxis kommen allerdings solche Vereinbarungen so gut wie nie vor. Aus diesem Grund sollte die Verlängerung der Widerrufsfrist proaktiv angeboten und eine dahingehende Verpflichtung der Zahlungsdienstleister in die künftige ZDVO aufgenommen werden. Da die Mitgliedstaaten über die Verordnung hinausgehende Betrugsbekämpfungsmaßnahmen treffen können (Art. 107 Abs. 1 PSR-E), wäre es möglich, diese Pflicht auch im deutschen Recht zu verankern.

---

<sup>275</sup> Art. 63 Abs. 3 PSD2; § 675p BGB.

<sup>276</sup> Art. 80 PSD2; § 675n Abs. 1 S. 1 BGB.

<sup>277</sup> Jungmann, in: Säcker u. a. (2023), BGB § 675p Rn. 54.

<sup>278</sup> Art. 80 Abs. 5 PSD2; § 675p Abs. 4 BGB.

<sup>279</sup> Vgl. BGH, Urt. v. 16.6.2015 – XI ZR 243/13, NJW 2015, 3093; Jungmann, in: Säcker u. a. (2023), BGB § 675p Rn. 52.

## Management in Betrugsfällen

### Anzeige beim Zahlungsdienstleister

Um die Meldung von Betrugsfällen bei den Zahlungsdienstleistern sicherzustellen, verpflichtet der PSR-E wie die PSD2 diese dazu, den Verbraucher:innen geeignete Mittel für die Anzeige bei ihnen zur Verfügung zu stellen (Art. 53 Abs. 1 lit. c PSR-E). Es ist zu begrüßen, dass das EP diese Pflicht dahingehend ergänzt, dass die Zahlungsdienstleister einen kostenlosen Kommunikationskanal zur Verfügung zu stellen verpflichtet sind (Art. 53 Abs. 1 lit. c PSR-E, EP-Bericht).<sup>280</sup> Den Zahlungsdienstnutzer:innen soll es möglich sein, über diesen Kommunikationskanal u. a. einen betrügerischen Zahlungsvorgang zu melden. Zusätzlich zur PSD2 schreibt Art. 53 Abs. 1 lit. c PSR-E, EP-Bericht vor, dass der Kommunikationskanal auch menschliche Unterstützung ermöglichen soll, sodass die Zahlungsdienstnutzer:innen qualifizierte Beratung erhalten können, wenn sie den Verdacht hegen, Opfer eines Betrugsangriffs zu sein.<sup>281</sup> Zudem fordert das EP, die Vorschrift zu erweitern und die Zahlungsdienstleister zu verpflichten, sichere Kommunikationskanäle zu nutzen und grundsätzlich davon abzusehen, Links und Dokumente per E-Mail zu übermitteln (Art. 53 Abs. 1 lit. ea PSR-E EP-Bericht). Erfüllen die Zahlungsdienstleister diese Pflichten nicht, würden die Zahlungsdienstnutzer:innen keine daraus entstehenden Verluste tragen.<sup>282</sup>

### Unverzügliche Erstattung

Die Pflicht zur unverzüglichen Erstattung des Zahlungsdienstleisters erfährt durch den PSR-E keine Änderung. Nach dem PSR-E sind die Zahlungsdienstleister dazu verpflichtet, den Betrag, der Gegenstand eines nicht autorisierten Zahlungsvorgangs war, unverzüglich zu erstatten (Art. 56 Abs. 1 PSR-E). Die Erstattung muss spätestens am nächsten Geschäftstag nach der Anzeige von Zahlungsdienstnutzer:innen oder anderweitiger Kenntniserlangung des Zahlungsdienstleisters erfolgen. Lediglich im Falle eines objektiv begründeten Verdachts, Zahlungsdienstnutzer:innen hätten einen Betrug begangen, kann der Zahlungsdienstleister von einer unverzüglichen Erstattung absehen. Die Nichterfüllung der Pflicht zur unverzüglichen Erstattung ist mit der schriftlichen Mitteilung an die zuständige nationale Behörde gekoppelt.

Anders als die PSD2 sieht der PSR-E für die Erfüllung dieser Pflicht und die schriftliche Mitteilung an die Behörde eine Frist von zehn Geschäftstagen vor. Gemäß Art. 56 Abs. 2 PSR-E hat der Zahlungsdienstleister innerhalb von vierzehn Geschäftstagen nach Feststellung oder Erhalt der Anzeige zum nicht autorisierten Zahlungsvorgang

- den Zahlungsdienstnutzer:innen den Betrag des nicht autorisierten Zahlungsvorgangs zu erstatten, oder
- den Zahlungsdienstnutzer:innen eine Begründung zu liefern, warum er die Erstattung ablehnt.

Das EP fordert, die Frist auf vierzehn Tage zu verlängern und die Pflicht, Zahlungsdienstnutzer:innen eine Begründung zu liefern, warum die Erstattung abgelehnt wird, um die nationale Behörde zu ergänzen (Art. 56 Abs. 2 PSR-E, EP-Bericht). Insofern werden die Zahlungsdienstleister künftig lediglich in Fällen, in denen sie einen objektiv begründeten Verdacht haben, die

---

<sup>280</sup> Art. 70 Abs. 1 lit. d PSD2; § 675m Abs. 1 Nr. 3 BGB.

<sup>281</sup> Erwägungsgrund 76a PSR-E, EP-Bericht.

<sup>282</sup> Dazu unten den Unterabschnitt „Haftung des Zahlungsdienstleisters“.

Zahlungsdienstnutzer:innen hätten einen Betrug begangen, die unverzügliche Erstattung ablehnen können. Allerdings stellt die Vorschrift nicht ausdrücklich sicher, ob die Zahlungsdienstleister diesem Erstattungsanspruch die grob fahrlässige Verletzung der Sorgfaltspflichten durch Zahlungsdienstnutzer:innen entgegenhalten dürfen. In dieser Hinsicht wäre in der künftigen Vorschrift eine dahingehende Aufklärung erforderlich, dass die Zahlungsdienstleister zunächst ihre Erstattungspflicht erfüllen müssen, bevor sie ihren eigenen Erstattungsanspruch aufgrund der grob fahrlässigen Verletzung der Sorgfaltspflichten geltend machen können.

### **Haftung des Zahlungsdienstleisters**

Bekanntlich ist die Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge das wichtigste und das meistdiskutierte Instrument, um das Vertrauen der Zahlungsdienstnutzer:innen am digitalen Zahlungsverkehr zu erhöhen. Die Zahlungsdienstleister sind die ersten Parteien, an die sich die Zahlungsdienstnutzer:innen wenden und Hilfe sowie Unterstützung suchen, wenn sie Opfer von Betrugsfällen werden. Die Banken als Zahlungsdienstleister werfen allerdings den Zahlungsdienstnutzer:innen zu schnell grobe Fahrlässigkeit vor. Dies hat nicht nur zur Folge, dass die Zahlungsdienstnutzer:innen auf dem Schaden sitzen bleiben, sondern auch, dass ihr Vertrauen in ihre Bank sowie in digitale Zahlungssysteme verloren geht.

Der PSR-E sieht ein etwas kompliziertes Haftungsregime vor, das leider nicht in der Lage ist, aktuelle Probleme mehrheitlich zu lösen und das Vertrauen in den digitalen Zahlungsverkehr zu erhöhen. Das Haftungsregime des PSR-Es basiert wiederum auf einer allgemeinen Vorschrift zum Erstattungsanspruch der Zahlungsdienstnutzer:innen. Zusätzlich dazu wird durch eine Sonderbestimmung der Fall des Identitätsbetrugs mit Bezug zum Zahlungsdienstleister geregelt. Nicht zuletzt sind zahlreiche Betrugspräventionsmaßnahmen vorgesehen. Zum Teil erzeugen diese Maßnahmen allenfalls einen Papiertiger, da es doch dem Ermessen der Bank überlassen wird, im Sinne der gesetzlichen Regelungen aktiv zu werden oder nicht, wobei sie im Unterlassungsfall mit keinen zivilrechtlichen Folgen rechnen müssen.

Wie das geltende Recht sieht Art. 56 Abs. 1 PSR-E die Pflicht des Zahlungsdienstleisters vor, den Betrag des nicht autorisierten Zahlungsvorgangs zu erstatten. Gemäß dieser Vorschrift können Zahlungsdienstleister von dieser Erstattung nur dann absehen, wenn sie aus berechtigten Gründen den Verdacht hegen, die Zahlungsdienstnutzer:innen hätten Betrug begangen. Sie haben zehn Tage Zeit, um entweder den Betrag des nicht autorisierten Zahlungsvorgangs zu erstatten oder den begründeten Betrugsverdacht bei der zuständigen nationalen Behörde zu melden (Art. 56 Abs. 2 PSR-E). Die Frist in dem EP-Bericht beträgt vierzehn Tage (Art. 56 Abs. 2 PSR-E, EP-Bericht).

Allerdings steckt der Teufel im Detail. Das EP hat in seiner Position die Definition der Autorisierung neu hinzugefügt (Art. 3 Nr. 34a PSR-E, EP-Bericht). Dementsprechend ist die Autorisierung als „eine Genehmigung, die in einem Verfahren erteilt wird, bei dem der Zahlungsdienstnutzer einen bestimmten Vorgang freiwillig und in voller Kenntnis aller relevanten Fakten authentifiziert“ definiert (subjektive Definition). Dagegen ist, gemäß Art. 49 Abs. 1 PSR-E ein Zahlungsvorgang nur dann autorisiert, „wenn der Zahler seine Erlaubnis zur Ausführung des Zahlungsvorgangs erteilt hat.“ (objektive Definition). Insofern setzt die Definition in Art. 49 Abs. 1 PSR-E „die volle Kenntnis aller relevanten Fakten“ für eine Autorisierung nicht voraus. Dieser Unterschied in Begrifflichkeiten könnte eine Auslegung zu Lasten der Zahlungsdienstnutzer:innen zur Folge haben. Da Art. 49 Abs. 1 PSR-E die speziellere Norm ist, könnte man für die Haftung des Zahlungsdienstleisters lediglich auf die bloße Erlaubnis zur Ausführung des Zahlungsvorgangs abstellen. So könnten alle Zahlungsvorgänge, in denen die Zahlungsdienstnutzer:innen betrügerisch zur Autorisierung verleitet

**Digital Abgehängt**

werden, als „autorisiert“ gelten, da der Begriff in Art. 49 Abs. 1 PSR-E „die volle Kenntnis aller relevanten Fakten“ für eine Autorisierung nicht voraussetzt. Folglich läge ein autorisierter Zahlungsvorgang vor, der einen Erstattungsanspruch nicht auslösen würde. Aus diesem Grund ist nachträglich zu empfehlen, die Begrifflichkeiten in den Art. 3 Nr. 34a PSR-E, EP-Bericht und Art. 49 Abs. 1 PSR-E zu vereinheitlichen und den Begriff der Autorisierung in Art. 3 Nr. 34a PSR-E, EP-Bericht zu bevorzugen.<sup>283</sup>

Die Haftung der Zahlungsdienstnutzer:innen für eine grob fahrlässige Verletzung der Sorgfaltspflichten bleibt unverändert (Art. 60 Abs. 1 Unterabs. 3 PSR-E). Wie das geltende Recht schreibt Art. 60 Abs. 1 Unterabs. 3 PSR-E vor, dass die Zahlungsdienstnutzer:innen alle mit nicht autorisierten Zahlungsvorgängen zusammenhängenden Verluste tragen, wenn diese Verluste durch betrügerisches Handeln oder durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer der Sorgfaltspflichten der Zahlungsdienstnutzer:innen entstehen. Verletzt aber der Zahlungsdienstleister seine Pflicht, eine starke Kundenauthentifizierung zu verlangen, trägt er die finanziellen Verluste der Zahlungsdienstnutzer:innen. Allerdings haften die Zahlungsdienstnutzer:innen für den Schaden, falls sie betrügerisch gehandelt haben, selbst wenn keine starke Kundenauthentifizierung verlangt wurde (Art. 60 Abs. 2 PSR-E). Gleiches gilt, wenn der Zahlungsdienstleister eine Ausnahme von der Durchführung der starken Kundenauthentifizierung anwendet.

Die Beurteilung, wann eine grob fahrlässige Pflichtverletzung vorliegt, ist und bleibt die Sache des nationalen Rechts. Dass der Erwägungsgrund 82 des Vorschlags für eine verbraucherfreundlichere Auslegung der „grob fahrlässigen Pflichtverletzung“ plädiert und es im EP-Bericht dafür Beispiele gibt,<sup>284</sup> und wiederum im EP-Bericht die EBA zur Entwicklung von Leitlinien in Bezug auf den Begriff „grob fahrlässig“ verpflichtet (Art. 59 Abs. 5c PSR-E, EP-Bericht),<sup>285</sup> ändert daran nichts. Da die deutsche Rechtsprechung bisher die technischen Entwicklungen und die raffinierten Methoden der Betrüger größtenteils unberücksichtigt gelassen hat, ist keine Änderung in der deutschen Rechtsprechung zu erwarten, sollte keine grundsätzliche Änderung im Haftungsregime erfolgen. Da Art. 56 Abs. 1 und 60 Abs. 1 Unterabs. 3 PSR-E die geltende Rechtslage nicht ändern, werden sich die Banken weiterhin auf grob fahrlässige Verletzung der Sorgfaltspflichten ihrer Kund:innen berufen. Eine Veränderung im Bankenverhalten bei Betrugsfällen ist somit nicht zu erwarten.

Allerdings sieht Art. 60 Abs. 1 Unterabs. 4 PSR-E eine Möglichkeit zur Einschränkung der Haftung der Zahlungsdienstnutzer:innen vor. Gemäß dieser Vorschrift können die zuständigen nationalen Behörden oder die Zahlungsdienstleister die Haftung der Zahlungsdienstnutzer:innen für eine grob fahrlässige Verletzung der Sorgfaltspflichten einschränken, wobei sie insbesondere der Art der personalisierten Sicherheitsmerkmale sowie den besonderen Umständen Rechnung tragen, unter denen der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstrumentes stattgefunden hat. Diese Vorschrift stellt größtenteils eine Wiederholung des Art. 74 Abs. 1

---

<sup>283</sup> Vgl. auch Erwägungsgrund 79a PSR-E, EP-Bericht.

<sup>284</sup> Folgende Beispiele werden durch den Erwägungsgrund 82 PSR-E, EP-Bericht als grob fahrlässige Verletzung der Sorgfaltspflichten angegeben: Die Ausführung einer Zahlung an einen Betrüger ohne berechtigte Gründe für die Annahme, dass es sich bei dem Empfänger der betreffenden Zahlung um einen rechtmäßigen Zahlungsempfänger handelt, die Aufbewahrung der zur Autorisierung eines Zahlungsvorgangs verwendeten Sicherheitsmerkmale neben dem Zahlungsinstrument in einem Format, das für Dritte offen und leicht auffindbar ist, die Verteilung einer Bank dazu, eine aufgrund einer Betrugswarnung veranlasste Sperrung aufzuheben, auf Anweisung eines unbekanntem Dritten oder die Weitergabe eines entsperreten Smartphones an einen Dritten.

<sup>285</sup> S. hierzu Erwägungsgrund 82a PSR-E, EP-Bericht.

Unterabs. 5 PSD2 dar, der in der deutschen Praxis keine große Bedeutung entfaltet hat. Aus diesem Grund ist es zweifelhaft, ob diese Vorschrift eine angemessene Lösung für die Probleme in der Praxis anbietet.

Eine der wichtigsten neuen Vorschriften des PSR-Es regelt Identitätsbetrugsfälle. Gemäß Art. 59 Abs. 1 PSR-E sind die Zahlungsdienstleister verpflichtet, den Betrag des betrügerischen Zahlungsvorgangs<sup>286</sup> zu erstatten, falls

- Zahlungsdienstnutzer:innen, bei denen es sich um Verbraucher:innen handelt, von Dritten manipuliert wurden, die sich unter Verwendung des Namens oder der E-Mail-Adresse oder der Telefonnummer des Zahlungsdienstleisters der Verbraucher:innen als Mitarbeiter:innen dieses Zahlungsdienstleisters ausgaben, und diese Manipulation anschließend betrügerische Zahlungsvorgänge zur Folge hatte, und
- die Verbraucher:innen den Betrug unverzüglich polizeilich gemeldet und den Zahlungsdienstleister angezeigt haben.

Das EP hat die Vorschrift dahingehend revidiert, dass der Identitätsbetrug auch die Fälle umfasst, wenn der Dritte den Namen, die E-Mail-Adresse oder die Telefonnummer einer anderen entsprechenden öffentlichen oder privaten Einrichtung verwendet und sich als Mitarbeiter dieser Einrichtung ausgibt (Art. 59 Abs. 1 PSR-E, EP-Bericht). Jedenfalls scheint die Vorschrift auf dem ersten Blick einen großen Fortschritt darin gemacht zu haben, das Vertrauen der Verbraucher:innen in digitale Zahlungssysteme zu erhöhen, denn ein nicht kleiner Teil der Betrugsfälle in Deutschland ist mit solchen Manipulationen verbunden, in denen die Betrüger den Namen oder die E-Mail-Adresse oder Telefonnummer des Zahlungsdienstleisters verwenden.

Allerdings gilt diese Regelung u. a. dann nicht, wenn Verbraucher:innen grob fahrlässig gehandelt haben. Art. 59 Abs. 3 PSR-E sieht vor, dass die Regelung keine Anwendung findet, wenn Verbraucher:innen betrügerisch oder grob fahrlässig gehandelt haben oder sich weigern, bei der Untersuchung des Zahlungsdienstleisters zu kooperieren bzw. sachdienliche Angaben zu den Umständen des Betruges zu machen. Für den Fall, dass tatsächlich betrügerisches bzw. nicht kooperatives Verhalten vorliegt, mag diese Ausnahmeregelung durchaus sinnvoll sein. Dagegen untergräbt die Ausnahme zum grob fahrlässigen Verhalten den Schutz bei den Identitätsbetrugsfällen. Derzeit müssen die Verbraucher:innen den gesamten Schaden aus Identitätsbetrugsfällen alleine tragen, weil ihnen grobe Fahrlässigkeit zugeschrieben wird. Insofern bietet die Regelung des PSR-Es zu Identitätsbetrugsfällen keine echte Lösung.<sup>287</sup> Die durch das EP vorgesehenen EBA-Leitlinien in Bezug auf den Begriff „grob fahrlässig“ (Art. 59 Abs. 5c PSR-E, EP-Bericht) würden daran nichts ändern, da die Beurteilung, wann grobe Fahrlässigkeit vorliegt, Angelegenheit des nationalen Rechts ist. Anders als die deutsche Rechtsprechung, hat beispielsweise der französische Kassationshof in einem aktuellen Urteil entschieden, dass keine grobe Fahrlässigkeit der Verbraucher:innen vorliegt, wenn sie mit der Telefonnummer des Zahlungsdienstleisters kontaktiert werden und glauben, mit einem/einer Mitarbeiter:in der Bank in Kontakt zu stehen. Denn in diesen Fällen verschafft der Anruf von der „Bank“ Vertrauen und verringert somit die Wachsamkeit von Verbraucher:innen. Der Verbraucher wurde in diesem Fall

---

<sup>286</sup> Die vorgeschlagene Vorschrift spricht von dem „autorisierten betrügerischen Zahlungsvorgang“, s. hierzu vorherige Erklärungen in diesem Unterabschnitt und Erwägungsgrund 79 PSR-E, EP-Bericht.

<sup>287</sup> S. auch Zahrte (2024a), S. 141.

unter der Telefonnummer seiner Bank kontaktiert und über einen Hackerangriff auf sein Konto informiert.<sup>288</sup>

Die Regelung zum Identitätsbetrug scheint durch die Pflicht der Zahlungsdienstleister unterstützt zu sein, sichere Kommunikationskanäle zu nutzen. Nach dem durch das EP hinzugefügten Art. 53 Abs. 1 lit. ea PSR-E (EP-Bericht) müssen die Zahlungsdienstleister sichere Kommunikationskanäle nutzen und grundsätzlich davon absehen, Links und Dokumente per E-Mail zu übermitteln. Verletzt der Zahlungsdienstleister diese Pflicht, tragen die Zahlungsdienstnutzer:innen keine sich daraus ergebenden finanziellen Verluste, es sei denn, sie haben selbst betrügerisch gehandelt (Art. 53 Abs. 2a PSR-E, EP-Bericht). Im Vorschlag sucht man vergeblich, was unter einem sicheren Kommunikationskanal für Zahlungsdienstnutzer:innen zu verstehen ist. Zudem sieht die durch das EP hinzugefügte Regelung keine echte Pflicht vor, sichere Kommunikationskanäle zu nutzen, da die Zahlungsdienstleister lediglich „grundsätzlich“ davon absehen müssen, Links und Dokumente per E-Mail zu übermitteln. Insofern könnten die Zahlungsdienstleister immer einwenden, dass sie mit ihren Kund:innen nur in Ausnahmefällen per E-Mail kommunizieren.

Zusätzlich zu diesen Vorschriften würden auch zahlreiche Sonderbestimmungen des PSR-Es zur Anwendung kommen, beispielsweise die Sperrung des Zahlungsinstruments. Wie oben erläutert, kann der Zahlungsdienstleister ein Zahlungsinstrument sperren (Kommissionsvorschlag) bzw. ist er dazu verpflichtet (EP-Bericht), wenn objektive Gründe bzw. Risiken im Zusammenhang mit der Sicherheit des Zahlungsinstruments dies rechtfertigen oder wenn der Verdacht einer nicht autorisierten oder betrügerischen Nutzung des Zahlungsinstruments besteht. Das EP hat diese Pflicht mit einer ausdrücklichen Sanktion verknüpft: Erfolgt eine solche Sperrung trotz hinreichender Gründe für den Verdacht von Betrug nicht, so kommen die Zahlungsdienstnutzer:innen nicht für die finanziellen Folgen auf, es sei denn, sie haben betrügerisch gehandelt (Art. 51 Abs. 2 PSR-E, EP-Bericht). Insofern haften die Zahlungsdienstnutzer:innen nicht, wenn der Zahlungsdienstleister es versäumt hat, das Zahlungsinstrument beim Verdacht eines betrügerischen Zahlungsvorgangs zu sperren.

Zudem hat das EP den Zahlungsdienstleistern die Möglichkeit eingeräumt, bei verdächtigen Transaktionen den Zahlungsauftrag zu blockieren (Art. 83 Abs. 2 Unterabs. 2 PSR-E, EP-Bericht). Die Entscheidung, eine verdächtige Zahlung zu blockieren, bleibt allerdings den Zahlungsdienstleistern selbst überlassen. Der PSR-E sieht keine Sanktionen vor, falls ein Anbieter eine potenziell betrügerische Zahlung nicht blockiert, obwohl Überwachungssysteme Anzeichen für Betrug erkennen. Dies stellt eine wichtige Schutzlücke für die Zahlungsdienstnutzer:innen dar. Es ist nachträglich zu empfehlen, die Blockierung des Zahlungsauftrags in Fällen von verdächtigen Transaktionen verpflichtend vorzuschreiben und die Zahlungsdienstnutzer:innen von ihrer Haftung zu befreien, falls die Bank dieser Pflicht nicht nachkommt.

Der PSR-E nimmt den Zahlungsdienstleister für die fehlerhafte Anwendung der Empfängerbestätigung in die Verantwortung. Gemäß Art. 57 Abs. 1 PSR-E werden den Zahlungsdienstnutzer:innen keine durch autorisierte Überweisungen entstandenen finanziellen Verluste angelastet, wenn der Zahlungsdienstleister es versäumt, die Zahlungsdienstnutzer:innen bei einer festgestellten Unstimmigkeit zwischen Kundenidentifikator und Namen der

---

<sup>288</sup> Cour de Cassation, Urt. V. 23. Oktober 2024, Nr. 23-16.267, ECLI:FR:CCASS:2024:CO00586, abrufbar auf: <https://www.courdecassation.fr/decision/67189203d8ceca1cd7018c82>, Letzter Abruf: 17. November 2024.

Zahlungsempfänger:innen zu benachrichtigen.<sup>289</sup> Doch diese Vorschrift findet keine Anwendung, wenn Zahlungsdienstnutzer:innen auf die Inanspruchnahme des Abgleichservice verzichtet haben (Art. 57 Abs. 5 PSR-E). Wie oben erläutert, sieht Art. 50 Abs. 4 PSR-E vor, dass die Zahlungsdienstleister allen Zahlungsdienstnutzer:innen die Möglichkeit anbieten, auf die Empfängerüberprüfung zu verzichten. Um die Betrugsprävention zu verstärken und den Zahlungsdienstleistern einen Anreiz zu bieten, sollte die Empfängerbestätigung bei den Zahlungsaufträgen von Verbraucher:innen zumindest für Überweisungen im SEPA-Raum ohne eine Verzichtmöglichkeit gestaltet werden, wie in der SEPA-VO enthalten. Kombiniert mit der Haftung des Zahlungsdienstleisters für die nicht ordnungsgemäße Durchführung des Abgleichservice würde diese Pflicht eine gute Betrugspräventionsmaßnahme darstellen.

Nicht zuletzt haben die Zahlungsdienstleister nach der Ergänzung des EP den Schaden zu tragen, falls sie es versäumt haben, betrügerische Kundenidentifikatoren zu sperren. Wie oben erläutert, sind die Zahlungsdienstleister verpflichtet, Überweisungen an solche Konten zu sperren, die ihnen als betrügerisch gemeldet wurden oder an nachweislich betrügerischen Vorgängen beteiligt waren (Art. 83 Abs. 5a PSR-E, EP-Bericht). Sollten Zahlungsdienstleister dieser Pflicht nicht nachkommen, tragen die Zahlungsdienstnutzer:innen keine sich daraus ergebenden finanziellen Verluste.

Wie diese Ausführungen deutlich machen, wird die Haftung des Zahlungsdienstleisters an mehreren Stellen stark untergraben. Dem allgemeinen Erstattungsanspruch der Verbraucher:innen steht die grob fahrlässige Verletzung der Sorgfaltspflichten durch die Verbraucher:innen entgegen. Das Gleiche gilt auch in den Identitätsbetrugsfällen. Die Regelung zur Empfängerbestätigung und die Haftung des Zahlungsdienstleisters daraus kann einfach durch einen Verzicht von Verbraucher:innen umgangen werden. Die Blockierung des Zahlungsauftrags ist vollkommen dem Ermessen der Bank überlassen. In sonstigen Fällen, also Sperrung des Zahlungsinstruments (Art. 51 Abs. 2 PSR-E) und Nutzung sicherer Kommunikationskanäle (Art. 53 Abs. 1 lit. ea PSR-E, EP-Bericht), ist es nicht eindeutig, ob der Schadensersatzanspruch der Bank aufgrund der grob fahrlässigen Verletzung der Sorgfaltspflichten durch die Verbraucher:innen zur Anwendung kommt oder ob dieser ausgeschlossen bleibt. Nicht zuletzt würde die Vielzahl von Maßnahmen und Regelungen zu Problemen in der Auslegung und Anwendung der künftigen Verordnung führen. Aus diesen Gründen wäre eine einfache Regelung sowohl für den Verbraucherschutz als auch für die einheitliche Anwendung der künftigen Verordnung wünschenswert.

Eine klare und einfache Regulierung, die den Verbraucherschutz in Betrugsfällen stärkt, hat das Vereinigte Königreich jüngst verabschiedet. Gemäß dieser Regulierung ist der Zahlungsdienstleister der Verbraucher:innen,<sup>290</sup> die Opfer von Zahlungsbetrug geworden sind, verpflichtet, sie in voller Höhe zu entschädigen, vorausgesetzt, es handelt sich um einen inländischen Zahlungsvorgang. Dies gilt sowohl für Echtzeit- als auch für normale Überweisungen.<sup>291</sup> Der Schaden ist dann

---

<sup>289</sup> Derzeit tragen die Zahlungsdienstnutzer:innen das Risiko, wenn die IBAN und der/die Empfänger:in nicht übereinstimmen, s. dazu Omlor (2024), S. 3483.

<sup>290</sup> Für die Anwendung dieser Regelungen umfasst der Begriff Verbraucher:in auch die Kleinstunternehmen (ein Unternehmen, das weniger als zehn Personen beschäftigt und entweder einen jährlichen Umsatz oder eine jährliche Bilanzsumme von höchstens 2 Millionen Euro aufweist) und gemeinnützige Organisationen.

<sup>291</sup> Für normale Überweisungen s. Payment Systems Regulator, Specific Direction 21 to PSPs participating in CHAPS that provide relevant CHAPS accounts, to reimburse CHAPS APP scam payments and comply with the CHAPS reimbursement rules of 6 September 2024, abrufbar auf , Letzter Abruf: 18. November 2024. Für Echtzeitüberweisungen s. Payment Systems Regulator, Specific Requirement 1 on the Faster Payments Operator to insert APP scam reimbursement rules into the Faster Payments Scheme rules of 12 July 2024, abrufbar auf: <https://www.psr.org.uk/media/xenefhgp/amended-specific-requirement-1-july-2024-corrected.pdf>, Letzter Abruf: 18. November 2024. Beide Regelungen sind am 7. Oktober 2024 in Kraft getreten. Ihre gesetzliche Grundlage ist im Section 72 des Financial Services and Markets Act 2023 und im Section 54 des Financial Services (Banking Reform) Act 2013 zu finden.

zwischen den Zahlungsdienstleistern der Zahler:innen und der Zahlungsempfänger:innen jeweils zur Hälfte zu teilen. Die Teilungsregelung gilt aber nur für das Innenverhältnis zwischen den beiden Zahlungsdienstleistern. Die Pflicht zur vollumfänglichen Entschädigung der Verbraucher:innen bleibt durch die Teilungsregel zwischen beiden Zahlungsdienstleistern unberührt.

Die Entschädigungspflicht gilt nach der UK-Regulierung dann nicht, wenn Verbraucher:innen folgende Sorgfaltspflichten grob fahrlässig verletzt haben:<sup>292</sup>

- Berücksichtigung jeder Intervention des überweisenden Zahlungsdienstleisters und/oder einer zentralen Meldestelle, die eine klare Einschätzung der Wahrscheinlichkeit bietet, dass es sich bei der beabsichtigten Zahlung um einen Betrugsfall handeln kann.
- Unverzögliche Anzeige des Betrugsfalls beim überweisenden Zahlungsdienstleister, spätestens am Ende des 13. Monats nach dem Datum der letzten Zahlung infolge des Betrugs
- Kooperation mit dem Zahlungsdienstleister zur Aufklärung des Betrugsfalls
- Meldung des Betrugsfalls an die Polizei oder an eine zentrale Meldestelle bzw. Zustimmung zur Meldung durch den Zahlungsdienstleister in ihrem Namen.

Diese Ausnahmeregelungen gelten nach UK-Recht wiederum nicht, wenn es sich um vulnerable Verbraucher:innen handelt und die Vulnerabilität einen wesentlichen Einfluss auf ihre Fähigkeit hatte, sich vor dem Betrug zu schützen. Vulnerabilität liegt vor, wenn eine Person aufgrund ihrer persönlichen Umstände besonders anfällig für Schaden ist.<sup>293</sup> Gemeint sind damit nicht nur körperliche Einschränkungen und schwere und lang andauernde Krankheiten, sondern auch Überschuldung, geringe Ersparnisse, schlechte Sprachkenntnisse, schlechte bzw. nicht vorhandene digitale Kompetenzen oder auch geringe emotionale Belastbarkeit aufgrund einer Scheidung oder Trennung.<sup>294</sup>

Mit dieser Regelung bietet das englische Recht ein umfassendes Erstattungsregime zugunsten von Verbraucher:innen. Lediglich die Verletzung einer recht geringen Anzahl von konkret benannten Sorgfaltspflichten führen zum Ausschluss der Erstattungspflicht des Zahlungsdienstleisters und dies nur, falls es sich nicht um vulnerable Verbraucher:innen handelt. Durch ein alle Lebensphasen und -ereignisse umfassendes Verständnis von Vulnerabilität gewährleistet die englische Regelung einen sozialen finanziellen Verbraucherschutz in Betrugsfällen. Eine ähnliche Regelung, die für Klarheit und somit für eine nicht komplizierte Anwendung in der Praxis sorgen würde, wäre für die EU auch wünschenswert.

### 3.3 Mangelnde Bereitschaft durch Anbieter adressieren

Als Daseinsvorsorge sollte die Teilnahme am Zahlungsverkehr auch in einer auf Abschlussfreiheit beruhenden Wirtschaftsordnung staatlich garantiert sein. Dies kann über eine Art Verpflichtung

---

<sup>292</sup> S. hierzu Payment Systems Regulator, Specific Requirement 1: Faster Payments APP Scam Reimbursement Rules – The Consumer Standard of Caution Exception of 19 December 2023, abrufbar auf: <https://www.psr.org.uk/media/tbbdhkcx/sr1-consumer-standard-of-caution-exception-dec-2023.pdf>, Letzter Abruf: 18. November 2024, sowie Payment Systems Regulator, Guidance Authorised push payment fraud reimbursement – The Consumer Standard of Caution Exception Guidance of December 2023, abrufbar auf <https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf>, Letzter Abruf: 18. November 2024.

<sup>293</sup> S. hierzu Financial Conduct Authority, Finalised guidance FG21/1 Guidance for firms on the fair treatment of vulnerable customers of February 2021, abrufbar auf: <https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf>, Letzter Abruf: 18. November 2024.

<sup>294</sup> S. Nummer 2.9 Finalised guidance FG21/1 Guidance for firms on the fair treatment of vulnerable customers.

privater Anbieter zu einem entsprechenden Angebot in Form von Abschlusszwängen wie beim Basiskonto oder über die Schaffung eines Anreizsystems für Finanzanbieter, flächendeckend bestimmte Leistungen anzubieten, erreicht werden.<sup>295</sup>

Ob diese Restriktionen dann in der Praxis problemlos umgesetzt werden, hängt vor allem davon ab, wie klar und eindeutig sie formuliert sind. Zusätzlich hat auch die Art und Weise der Sanktionierung von Fehlverhalten Bedeutung. Die europäischen Vorgaben fordern, dass die Sanktionen für die Verstöße wirksam, verhältnismäßig und abschreckend sein müssen. Allerdings gewährleisten gesetzliche Sanktionen nicht immer einen effektiven Schutz, prozessrechtliche Darlegungs- und die Beweislast spielen auch eine große Rolle bei der effektiven Durchsetzung der Verbraucherrechte. Die Praxis liefert zahlreiche Beweise, wie schwierig es ist, Verstöße der Finanzanbieter gegenüber verbraucherschutzrechtlichen Maßnahmen im Einzelfall nachzuweisen, wobei erschwerend hinzukommt, dass die Beweislast in aller Regel bei den Verbraucher:innen selbst liegt.

## 4. Regulatorische Barrieren

Wie oben dargestellt, entsteht ein regulatorisches Spannungsverhältnis, das zu einer Barriere beim Zugang zum digitalen Zahlungsverhältnis führt. Diese entsteht insbesondere in der Umsetzung der Regulierung zur Geldwäsche und Terrorismusfinanzierung und stellt vor allem für Personen mit Einschränkungen, aber auch für wohnungslose Personen oder solche ohne Ausweisdokumente, eine Barriere beim Zugang zum digitalen Zahlungsverkehr dar.

Ein prominentes Beispiel dafür ist, dass Menschen mit Einschränkungen während des Video-Identifizierungsverfahrens keine Unterstützung durch andere Personen in Anspruch nehmen dürfen. Zur Überwindung dieses regulatorischen Spannungsverhältnisses bedarf es gesonderter Regelungen, die unterschiedliche Arten von Einschränkungen in Betracht ziehen. Insofern müsste der Gesetzgeber bereits im Gesetzgebungsverfahren diese berücksichtigen und die Identifizierung dementsprechend ermöglichen. Denkbar wären gesonderte Ausweise, worauf die Ausweisnummer in der Art gedruckt wird, dass sie durch Finger spürbar ist. Eine alternative Bestätigungsmethode wäre auch denkbar, z. B. den Ausweis in die Kamera zu zeigen, anstatt einen Teil der Ausweisnummer vorlesen zu müssen.

Eine weitere regulatorische Barriere beim Zugang zum Basiskonto für vulnerable Personengruppen ist die Erfüllung von Formalitäten wie dem Adressnachweis. Da der Adressnachweis ein Hindernis für den Zugang zum Basiskonto für Menschen ohne ständige Meldeadresse darstellt, sollten auch Adressen von Unterstützungseinrichtungen wie Obdachloseneinrichtungen als C/O-Adresse als Adressnachweis ausreichen. Insofern sollte die Anwendung des § 11 Abs. 4 S. 1 lit. (e) GWG sichergestellt werden. Hilfreich hierfür ist eine Kommunikation zwischen Anbietern von Zahlungskonten und Unterstützungseinrichtungen.<sup>296</sup> Ein Beispiel hierfür ist die Obdachlosenhilfe Komasset Kirkers Korshaer in Dänemark, die eine spezielle Vereinbarung mit einer der Banken in Kopenhagen entwickelte, nach der ein Schreiben von Kirkens Korshær mit der Bestätigung, dass die potenziellen Bankkund:innen die Adresse von Komasset nutzen können, um ihre Karte und den PIN-Code zu erhalten, für den Adressnachweis ausreichend ist. Nach der europäischen Geldwäscheverordnung (GwVO) wird eine Postanschrift, unter der eine Person erreichbar ist, auch

---

<sup>295</sup> Knobloch u. a. (19.11.2012), S. 9.

<sup>296</sup> FEANTSA (Januar 2022), S. 8.

im Rahmen der Geldwäscheprävention akzeptabel sein, falls die Person nicht über eine feste Meldeadresse und einen rechtmäßigen Aufenthaltstitel in der Union verfügt (Art. 22 Abs. 1 GwVO). Im Rahmen dieser Regelung sollte es möglich sein, Lösungen wie in Dänemark anzubieten.

## 5. Ein Blick in die Zukunft: Digitaler Euro für alle Verbrauchergruppen

Der digitale Euro ist eine Initiative der EZB und soll eine digitale Ergänzung zum physischen Bargeld werden. Seine Einführung und technische Gestaltung werden derzeit noch im Detail organisiert. Im Folgenden wird erörtert, inwieweit der bislang vorliegende DigEUR-Vorschlag der Europäischen Kommission bereits oben genannte Aspekte der Zugänglichkeit und Nutzung für alle berücksichtigt und bei den bestehenden Barrieren Verbesserungen schaffen kann.

Das Hauptziel der Einführung des digitalen Euro ist es, den Euro als gesetzliches Zahlungsmittel auch in digitaler Form zur Verfügung zu stellen und die finanzielle Inklusion fördern. Verbunden mit der gesetzlichen Annahmepflicht wird der digitale Euro sowohl Online- als auch Offline-Zahlungen ermöglichen. Zudem wird geplant, seine Verfügbarkeit in weitem Umfang und zu jedem Zeitpunkt zu gewährleisten sowie seine Handhabung benutzerfreundlich zu gestalten. Durch eine solche Gestaltung wird bezweckt, die Beteiligung von bisher gehinderten Gruppen am Zahlungsverkehr zu erleichtern und zu verstärken.

Die vulnerablen Verbrauchergruppen sollten einen kostenfreien Zugang zum Basiskonto erhalten, sodass der digitale Euro den Anspruch auf die finanzielle Inklusion erfüllen kann. Der digitale Euro wird durch die Zahlungsdienstleister bereitgestellt (Art. 13 DigEUR-Vorschlag). Die Verbraucher:innen sind dabei nicht gezwungen, digitale Euro über ein eigens bei einem Zahlungsdienstleister eröffnetes Konto zu beziehen (Art. 22 Abs. 2 DigEUR-Vorschlag). Es soll ein Zugang ohne ein Konto auch dadurch gewährleistet werden, dass öffentliche Stellen (lokale oder regionale Behörden oder Postämter) den digitalen Euro auch natürlichen Personen bereitstellen, die kein Konto für den digitalen Euro bei Kreditinstituten oder anderen Zahlungsdienstleistern eröffnen möchten (Art. 14 Abs. 3 lit. a DigEUR-Vorschlag).<sup>297</sup> Diejenigen Verbraucher:innen, die bereits über ein Zahlungskonto verfügen, können bei ihrer Bank ein Konto (Wallet) für den digitalen Euro eröffnen. Eine freie Wahlmöglichkeit zwischen beiden Alternativen steht allerdings nur denjenigen zu, für die die Eröffnung eines Kontos durch keinerlei Barrieren behindert bzw. erschwert wird. Wie unten zu zeigen ist, bietet dabei eine digitale Euro-Wallet bei der Nutzung durchaus Vorteile, da z. B. damit online Käufe bezahlt werden können. Voraussetzung ist dafür allerdings ein „normales“ Bankkonto, so dass das „Aufladen“ der Euro-Wallet mittels Überweisungen von diesem Konto erfolgen kann. Möglich wird dadurch auch der sogenannte „waterfall“: Sollte also der Kaufpreis einer mit digitalen Euro zu bezahlenden Ware über den Höchstbetrag hinausgehen, der in digitalen Euro gehalten werden darf, so erfolgt in Höhe des Differenzbetrags ein automatischer Zugriff auf das Girokonto. In diesem Zusammenhang ist hier die regulatorische Barriere aufgrund der mangelhaften Umsetzung beim Zugang zum Basiskonto von Relevanz. Der Zugang zum Basiskonto ist in der Praxis mit vielen Hürden verbunden.<sup>298</sup> Wenn insbesondere den vulnerablen Verbrauchergruppen der Zugang zum Basiskonto aufgrund hoher

---

<sup>297</sup> DigEUR-Vorschlag, S. 4.

<sup>298</sup> M. w. N. Finance Watch (2024).

Kosten verwehrt bleibt, werden sie auch keine Möglichkeit für das Onboarding beim digitalen Euro haben.

Um den Zugang zu und die Nutzung vom digitalen Euro zu unterstützen, nimmt der europäische Gesetzgeber die Kosten gesondert in den Blick. Gemäß Art. 17 Abs. 1 DigEUR-Vorschlag haben die Zahlungsdienstleister die grundlegenden Zahlungsdienste im Zusammenhang mit dem digitalen Euro kostenlos anzubieten. Zudem sieht der Vorschlag vor, dass für die Menschen ohne ein Zahlungskonto die Vorschriften des ZKRL gelten, und zwar in Bezug auf den Zugang zu „Konten für den digitalen Euro mit grundlegenden Diensten“ (Art. 14 Abs. 2 DigEUR-Vorschlag). So hat der europäische Gesetzgeber die Banken verpflichtet, den Zugang zum Basiskonto für den digitalen Euro den Verbraucher:innen kostenfrei anzubieten (Art. 14 Abs. 2 DigEUR-Vorschlag). Um in diesem Zusammenhang tatsächlich einen umfassenden Beitrag zur finanziellen Inklusion zu leisten, sollte dann aber auch das Basiskonto mit seinen Kosten nochmals ins Visier genommen werden.

Eine Verpflichtung, lediglich das Basiskonto für den digitalen Euro kostenlos anzubieten, würde dagegen in Deutschland ein zweigleisiges System zur Folge haben. Einerseits wäre das Basiskonto für den digitalen Euro kostenfrei, wohingegen das Basiskonto für den nicht-digitalen Euro doch in der Praxis kostenpflichtig ist. Um das inklusive Potenzial voll ausschöpfen zu können, ist die Verpflichtung, die grundlegenden Zahlungsverpflichtungen, zumindest für vulnerable Verbrauchergruppen, kostenlos anzubieten, auch auf das herkömmliche Basiskonto zu erweitern. Der digitale Euro könnte so dazu beitragen, den Zugang zu digitalen Finanzdienstleistungen zu verbessern, insbesondere für Menschen ohne Bankkonto oder mit begrenztem Zugang zu traditionellen Finanzsystemen.

Zum Schluss haben sämtliche Anbieter Unterstützungsleistungen zu erbringen. Sowohl Zahlungsdienstleister als auch die öffentlichen Stellen (z. B. lokale oder regionale Behörden oder Postämter) haben Menschen mit Behinderungen, funktionalen Einschränkungen oder begrenzten digitalen Fähigkeiten sowie älteren Menschen Unterstützung bei der digitalen Inklusion an Ort und Stelle zu bieten (Art. 14 Abs. 3 lit. b, Abs. 4 DigEUR-Vorschlag). Diese Unterstützung umfasst bei der digitalen Inklusion eine spezielle Hilfe beim Onboarding eines Kontos für den digitalen Euro und bei der Nutzung aller grundlegenden Zahlungsdienste im Zusammenhang mit dem digitalen Euro. Zu diesem Zweck sollten die Zahlungsdienstleister ihre Mitarbeiter:innen zielgruppenorientiert sensibilisieren und ihre Kompetenzen aufbauen.

Es bleibt abzuwarten, ob diese Vorhaben auch tatsächlich in der Praxis ihre Umsetzung finden, zumal daran die Zahlungsdienstleister selbst einen erheblichen Anteil haben. Für sie aber ist der digitale Euro ein Konkurrenzprodukt. Es ist somit nicht ausgeschlossen, dass sie Strategien entwickeln, die geeignet sind, die Attraktivität des digitalen Euro als Zahlungsmittel zu untergraben. Die Regulierung sollte in diesen Fällen zügig mit Gegenmaßnahmen antworten.

## V. Fazit

Die fortlaufende Digitalisierung des Zahlungsverkehrs hat viele Vorteile gebracht, geht aber auch mit neuen Barrieren beim Zugang zum Zahlungsverkehr einher. So lassen sich Zahlungen schnell, bequem und flexibel abwickeln – ob per App, Kreditkarte oder Online-Banking. Diese Vorteile können jedoch nicht alle Menschen für sich nutzen. Verantwortlich hierfür sind unterschiedliche Barrieren, die ihren Ursprung sowohl im voraussetzungsvollen Zugang als auch in der fehlenden Bereitschaft haben. Sowohl die jeweils gebräuchlichen Arten der Zahlungsmittel als auch der Bezahlmethoden unterliegen seit jeher einem steten Wandel, und jedes Mal ist eine Innovation nicht nur freudig akzeptiert worden.

Jede Neuerung war und ist immer auch mit gewissen Lernprozessen verbunden, um den Zugang, die Nutzung und Abstimmung auf den jeweiligen Bedarf auch faktisch möglich zu machen. Zudem ist gerade in einer Einführungsphase die Reibungslosigkeit, aber auch die Sicherheit der Abwicklung von Bezahlvorgängen häufig nicht gewährleistet. Aber gerade im Zusammenhang mit der Digitalisierung steigt die Bedeutung des Faktors Sicherheit, da nun nicht mehr allein technisches Versagen und eine fehlende Integrität des Zahlungsdienstleisters dafür entscheidend sind, sondern die Cyberkriminalität mit immer raffinierteren Methoden eine ständige Bedrohung bedeutet. Damit verbunden wird Vertrauen als wichtige Voraussetzung für eine breite Akzeptanz digitaler Bezahlmethoden erschwert.

Im Rahmen der gutachterlichen Arbeit wurden vier Kategorien von Barrieren zum digitalen Zahlungsdienst identifiziert:

1. **Praktische Barrieren** umfassen eine mangelnde technische Ausstattung auf Seiten der Verbraucher:innen sowie Kosten, die mit der Teilnahme am digitalen Zahlungsverkehr einhergehen.
2. Bei der Barriere der **mangelnden Kompetenz** geht es um eine mangelnde finanzielle und digitale Kompetenz auf Seiten der Verbraucher:innen, aber auch um die mangelnde Kompetenz auf Seiten der Zahlungsdienstleister, eine gruppenorientierte Unterstützung der Verbraucher:innen beim Zugang zu und bei der Nutzung von Zahlungsdiensten zu leisten.
3. Die dritte Barriere umfasst die **fehlende Bereitschaft** sowohl auf Seiten der Verbraucher:innen, die „neuen“ Technologien misstrauen, als auch auf Seiten der Anbieter, die vorhandene Regulierungen nicht umsetzen.
4. **Regulatorische Barrieren** liegen vor, wenn die Regulierung selbst den Zugang zum Zahlungsverkehr behindert.

Es gilt, die beschriebenen Barrieren zu überwinden. Angesprochen sind dabei aber nicht nur digitale Bezahlmethoden. Vielmehr sollte sowohl im Interesse einer Wahlfreiheit für Verbraucher:innen als auch im Interesse der einzel- wie gesamtwirtschaftlichen finanziellen Stabilität dem Zugang und der Nutzung von Bargeld weiterhin Bedeutung zukommen.

Je nach Barriere braucht es verschiedene Maßnahmen, um die jeweilige Barriere abzubauen. Die Zugangsbarrieren zu Bargeld sind sowohl praktischer Natur als auch einem betriebswirtschaftlichen Kalkül der Anbieter geschuldet. Sie hängen sowohl mit der abnehmenden Zahl an Bankfilialen (vor allem in der Fläche) zusammen als auch mit begrenzten Möglichkeiten des Einzelhandels, entstehende Lücken zu füllen. Der Rückgang der Bargeldversorgung wird mit zu hohen Kosten für die Bargeldbereitstellung begründet. Insofern braucht es konkrete Vorgaben, die Banken dazu verpflichtet, ihre Kund:innen mit Bargeld kostengünstig auszustatten und über diese Zugangsmöglichkeiten zu kommunizieren.

**Digital Abgehängt**

Mit der steigenden Digitalisierung erhöhen sich auch die Voraussetzungen für die Nutzung des digitalen Zahlungsverkehrs. So müssen Bezahlsysteme barrierefrei gestaltet werden, indem einfache Technologien verwendet und alternative Mittel angeboten werden. Auch die digitale Kompetenz, die für die Nutzung des digitalen Zahlungsverkehrs notwendig wird, sollte sowohl auf Verbraucher- als auch auf Anbieterseite gestärkt werden. Entsprechend sollten Banken ihre Mitarbeiter:innen zielgruppenorientiert sensibilisieren, beispielsweise indem die Schulungspflicht im Zahlungsverkehr um die Kundenorientierung erweitert wird.

Die Digitalisierung geht auch mit Unsicherheit einher, die dazu führen kann, dass Verbraucher:innen nicht bereit sind, digitale Techniken zu nutzen. Um diese Barriere abzubauen, sollte beim digitalen Zahlungsverkehr der Schutz der Privatsphäre beachtet werden und durch Betrugsprävention das Vertrauen in die Digitalisierung gestärkt werden. Dabei geht es auch darum, Haftungsfragen zu adressieren und Anbieter hier stärker in die Pflicht zu nehmen.

Die Qualität bestehender Regulierung ist das Thema bei der Adressierung von Barrieren, die mit einer mangelnden Bereitschaft von Anbietern zu Regulierungen zusammenhängen. Um Umgehungsstrategien bestehender Regulierung durch Anbieter zu vermeiden, sollte die Zahlungsdiensteaufsicht gestärkt und gesetzliche Regelungen klar und eindeutig formuliert werden. Zudem sollten Gesetzgebungsverfahren und Gesetzesevaluierung nicht intendierte Exklusionseffekte für vulnerable Verbrauchergruppen stärker in den Fokus nehmen. So sollte bei der Anwendung des Geldwäschegesetzes die Expertise von Vertretungsorganisationen eingeholt werden.

Zusammenfassend kann festgehalten werden, dass der digitale Zahlungsverkehr eine Errungenschaft ist, die unseren Alltag erleichtert – aber nur, wenn er sicher und für alle zugänglich bleibt. Abgehängt zu sein im Zahlungsverkehr, ist kein Problem einer bestimmten Gruppe – es kann alle treffen, ob durch technische Probleme, Sicherheitsrisiken oder fehlende Alternativen. Präventionsmaßnahmen gegen Betrugsfälle und die Förderung digitaler Inklusion sind dabei entscheidend, um sicherzustellen, dass niemand im digitalen Zeitalter zurückbleibt oder zum Opfer von Betrug wird. In diesem Zusammenhang wird regulatorischen Maßnahmen des Verbraucherschutzes eine steigende Bedeutung zukommen. Die EU hat dieses Problem zwar erkannt, allerdings ist Skepsis angebracht, ob die geplanten Regelungen dem Einfluss der Finanzlobby standhalten – sowohl, was die gesetzlichen Vorgaben als auch ihre Umsetzung angeht. Umso wichtiger ist es somit, über die Erfordernisse Klarheit zu bekommen, wie eine passfähige Regulierung auszusehen hätte. Mit dieser Arbeit wird versucht, einen Beitrag hierzu zu leisten.

## VI. LITERATURVERZEICHNIS

Aktion Mensch (2021): Barrierefreiheitsstärkungsgesetz in der Kritik, Stand: <https://www.aktion-mensch.de/inklusion/barrierefreiheit/barrierefreiheitsstaerkungsgesetz>.

Arrighetti, Alessandro/Bachmann, Reinhard/Deakin, Simon (1997): Contract Law, Social Norms and Inter-Firm Co-operation, in: Cambridge Journal of Economics, 21. Jg., S. 329–349.

Bachmann, Reinhard/Inkpen, Andrew C. (2011): Understanding Institutional-based Trust Building Processes in Inter-Organizational Relationships, in: Organization Studies, 32. Jg., Nr. 2, S. 281–301.

Bachmann, Reinhard/Zaheer, A. (2006): Handbook of trust research, Cелtenham.

BaFin (2024): Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG), URL: [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb\\_111222\\_zag.html?nn=19646120](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html?nn=19646120), Stand: 23. November 2024.

BAGSO (2022): Leben ohne Internet - geht's noch. Ergebnisbericht zu einer Umfrage der BAGSO, URL: <https://www.bagso.de/studie/leben-ohne-internet-gehts-noch/>.

Barber, Bernard (1983): The Logic and Limits of Trust, New Brunswick.

Beckert, Jens (20002): Vertrauen und die performative Konstruktion von Märkten/Trust and the Performative Role of Marktes, in: Zeitschrift für Soziologie, Nr. 31.1, S. 27–43.

Beil, Anna/Hohmann, Iris (2014): Future of 1 and 2 Euro Cent Coins, URL: [https://www.cep.eu/fileadmin/user\\_upload/cep.eu/Analysen/COM\\_2013\\_281\\_Muenzen/cepPolicyBrief\\_CO M\\_2013\\_281\\_Future\\_of\\_1\\_and\\_2\\_Cent\\_Coins.pdf](https://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2013_281_Muenzen/cepPolicyBrief_CO M_2013_281_Future_of_1_and_2_Cent_Coins.pdf), Stand: 24. November 2024.

Beilner, Maximilian (2024): Der digitale Euro wird vier: Eine Zwischenbilanz auf dem Weg zum digitalen Bargeld, in: Recht Digital, 4. Jg., Nr. 10, S. 469–476.

BEUC (o.J.): DIGITAL EURO. BEUC response to the ECB's consultation, URL: [https://www.researchgate.net/publication/350873543\\_DIGITAL\\_EURO\\_BEUC\\_response\\_to\\_the\\_ECB's\\_consultation\\_by\\_BEUC\\_The\\_Consumer\\_Voice\\_in\\_Europe](https://www.researchgate.net/publication/350873543_DIGITAL_EURO_BEUC_response_to_the_ECB's_consultation_by_BEUC_The_Consumer_Voice_in_Europe).

BEUC (2020): A New Digital Finance Strategy for Europe / FinTech Action Plan.

BEUC (2022): EU Consumer Protection 2.0 - Protecting fairness and consumer choice in a digital economy, URL: [https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015\\_protecting\\_fairness\\_and\\_consumer\\_choice\\_in\\_a\\_digital\\_economy.pdf](https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf).

Bitkom Research (2024): Bilanz Cyberkriminalität 2023: 7 von 10 Internetnutzern betroffen, Berlin, URL: <https://www.bitkom.org/Presse/Presseinformation/Bilanz-Cyberkriminalitaet-7-von-10-betroffen>, Stand: 24. November 2024.

Bock, Kirsten (2024): Bargeld ist mehr als nur ein Notgroschen, URL: <https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/bargeld-ist-mehr-als-nur-ein-notgroschen>.

Braatz, Frank (Hrsg.) (2024): Bundesbank: Zahlungsverhalten stärker verändert, in: Source Informationsdienst, 31. Jg., Nr. 7, S. 1–12.

**Digital Abgehängt**

Broekhoff, Marie-Claire/van der Crujisen, Carin/Haan, Jakob de (2024): Towards financial inclusion: Trust in banks' payment services among groups at risk, in: Economic Analysis and Policy, 82. Jg., S. 104–123.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2017): Basiskonto - Rechtsanspruch für Verbraucher: Erfahrungen und Herausforderungen, URL: [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa\\_bj\\_1712\\_Basiskonto.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1712_Basiskonto.html), Stand: 24. November 2024.

Cambier, Claire (2024): 'Call me maybe'...How do you call your bank to cancel your credit card if you're deaf?, URL: <https://www.beuc.eu/blog/call-me-maybe-how-do-you-call-your-bank-to-cancel-your-credit-card-if-youre-deaf/>.

Child, John/Möllering, Guido (2003): Contextual Confidence and Active Trust Development in the Chinese Business Environment, in: Organization Science, 14. Jg., Nr. 1, S. 69–80.

Currall, Steven C. (1992): Group Representatives in Educational Institutions: An Empirical Study of Superintendents and Teacher Union Presidents, in: Journal of Applied Behavioural Science, Nr. 28, S. 296–317.

Damar, Duygu (2021): Infobrief 23+24/2021. Diskriminierung aufgrund Behinderung im Zahlungsverkehr.

De Nederlandsche Bank (2023): Digitalisation of the payment system: a solution for some, a challenge for others, URL: [https://www.dnb.nl/media/v5lgqudn/impact-digitalisering\\_en\\_web.pdf](https://www.dnb.nl/media/v5lgqudn/impact-digitalisering_en_web.pdf).

Demirguc-Kunt, Asli u. a. (2018): Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution, Washington, DC, URL: <https://openknowledge.worldbank.org/entities/publication/ed800062-e062-5a05-acdd-90429d8a5a07>, Stand: 24. November 2024.

Demirguc-Kunt, Asli u. a. (2022): The Global Findex Database 2021. Financial Inclusion, Digital Payments, and Resilience Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19, Washington, DC, URL: <https://openknowledge.worldbank.org/bitstream/handle/10986/37578/9781464818974.pdf>, Stand: 24. November 2024.

Deutsche Bundesbank (2022a): Anzahl der Bankstellen in Deutschland in den Jahren von 1957 bis 2021., URL: <https://de.statista.com/statistik/daten/studie/72095/umfrage/anzahl-der-bankstellen-in-deutschland/> (Simone Ehrenberg-Silies bargeld-der-zukunft-data, S. 134), Stand: 29. Oktober 2024.

Deutsche Bundesbank (2022b): Anzahl der Geldautomaten in Deutschland in den Jahren von 2001 bis 2021, URL: <https://de.statista.com/statistik/daten/studie/6703/umfrage/anzahldergeldautomatenindeutschlandseitdemjahr1996/>, Stand: 29. Oktober 2024.

Deutsche Bundesbank (2023): Zugang zu Bargeld in Deutschland - Auswertungen zur räumlichen Verfügbarkeit von Abhebeorten, Monatsbericht Januar 2023, 97-111, URL: <https://www.bundesbank.de/resource/blob/903524/9b01c5239e9ac9dcffe7aaa784c94312/mL/2023-01-zugang-bargeld-data.pdf>.

Deutsche Bundesbank (2024): Zahlungsverhalten in Deutschland 2023, URL: <https://www.bundesbank.de/resource/blob/934826/cf30c0491030c0c6eab3d341d1990e12/mL/zahlungsverhalten-in-deutschland-2023-data.pdf>.

Deutscher Bundestag (2021): Kritik an Regierungs-ent-wurf zur Barriere-freiheit von Produk-ten, URL: <https://www.bundestag.de/dokumente/textarchiv/2021/kw20-pa-arbeit-soziales-barrierefreiheit-840416>, Stand: 24. November 2024.

**Digital Abgehängt**

Die Fachverbände für Menschen mit Behinderung (2021): Forderungen der Fachverbände für Menschen mit Behinderung zur digitalen Teilhabe von Menschen mit Behinderung, URL: [https://www.diefachverbaende.de/files/stellungnahmen/20211026\\_Fachverbaende\\_Forderungen%20zur%20digitalen%20Teilhabe\\_END.pdf](https://www.diefachverbaende.de/files/stellungnahmen/20211026_Fachverbaende_Forderungen%20zur%20digitalen%20Teilhabe_END.pdf).

Ehrenberg-Silies, Simone u. a. (2024): Bargeld der Zukunft, URL: <https://www.bundesbank.de/resource/blob/921808/f6dcdae210f341925ad26d86691ecfe7/mL/bargeld-der-zukunft-data.pdf>.

Ellenberger, Jürgen/Bunte, Hermann-Josef (Hrsg.) (2022): Bankrechts-Handbuch, 6. Aufl., München.

Ergebnisse der SIM-Studie 2021 (2022): Medienumgang von Menschen ab 60 Jahren. Rathgeb, Thomas; Doh, Michael; Tremmel, Florian; Jokisch, Mario; Groß, Ann-Kathrin.

European Central Bank (2022): Study on the payment attitudes of consumers in the euro area (SPACE), URL: [https://www.ecb.europa.eu/stats/ecb\\_surveys/space/shared/pdf/ecb.spacereport202212~783ffdf46e.en.pdf](https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.spacereport202212~783ffdf46e.en.pdf), Stand: 28. November 2024.

European Parliament (März 2024): Implications of the Digital Transformation on Different Social Groups, URL: [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/760277/IPOL\\_STU\(2024\)760277\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/760277/IPOL_STU(2024)760277_EN.pdf).

Eurostat (2023): Anteil der Haushalte in Deutschland mit Internetzugang von 2002 bis 2023.

FEANTSA (2022): Homelessness services provide solutions to ensure homeless people are financially included in increasingly cashless societies, URL: <https://www.feantsa.org/en/report/2022/02/08/financial-inclusion-of-people-experiencing-homelessness-in-increasingly-cashless-societies?bcParent=27>.

Finance Watch (2024): Report: Breaking down barriers to basic payment accounts in the EU, URL: [https://www.finance-watch.org/wp-content/uploads/2024/04/Finance-Watch\\_Report\\_payment-accounts.pdf](https://www.finance-watch.org/wp-content/uploads/2024/04/Finance-Watch_Report_payment-accounts.pdf), Stand: 7. Juni 2024.

Financial Services User Group (FSUG) (2023): FSUG Report 2022-2023, URL: [https://finance.ec.europa.eu/document/download/b862c473-7712-4eb0-a102-38984e5515ef\\_en?filename=fsug-annual-report-2022-2023\\_en.pdf](https://finance.ec.europa.eu/document/download/b862c473-7712-4eb0-a102-38984e5515ef_en?filename=fsug-annual-report-2022-2023_en.pdf).

Fohrer, Katja (2024): Haftung von Banken bei Online-Banking-Missbrauchsfällen, Phishing sowie bei Diebstahl und Missbrauch von EC- und Kreditkarten.

Giddens, Anthony (1984): The Constitution of Society: Outline of the Theory of Structuration, Cambridge.

Grotluschen, Anke u. a. (2019): LEO 2018 – Leben mit geringer Literalität, Hamburg, URL: <https://leo.blogs.uni-hamburg.de/wp-content/uploads/2022/09/LEO2018-Presseheft.pdf>, Stand: 26. November 2024.

Jalava, Janne (2006): Trust as a Decision. The Problems and Functions of Trust in Luhmannian Systems Theory. Research Report 1.

Kalisz, Sven (2023): Barrierefreiheit von Bankprodukten und -dienstleistungen. Oder warum Kreditinstitute zukünftig auch besser als Gesetzgeber formulieren können müssen, in: Zeitschrift für Bank- und Kapitalmarktrecht, Nr. 5, S. 292–301.

Khan, Omar (2021): Gute Ideen zu wirtschaftlicher Inklusion: Zugang zu Bankgeschäften, URL: [https://rshare.library.torontomu.ca/articles/report/Gute\\_Ideen\\_zu\\_wirtschaftlicher\\_Inklusion\\_Zugang\\_zu\\_Bankgesch\\_fen/17049380?file=31531217](https://rshare.library.torontomu.ca/articles/report/Gute_Ideen_zu_wirtschaftlicher_Inklusion_Zugang_zu_Bankgesch_fen/17049380?file=31531217).

**Digital Abgehängt**

Knobloch, Michael/Feldhusen, Claire/Tiffe, Achim (2012): Basisprodukte bei Finanzdienstleistungen. Gutachten im Auftrag des Verbraucherzentrale Bundesverbandes e.V., Hamburg, URL: <https://www.vzbv.de/sites/default/files/downloads/Basisprodukte-Finanzdienstleistungen-Gutachten-iff.pdf>.

Knümann, Fabio/Krüger, Malte/Seitz, Franz (2024): Kosten von Bargeld und Kartenzahlungen aus Verbrauchersicht.

Linardatos, Dimitrios (2021): Kontaktloses Zahlen im Zahlungsdienstrecht. Ein Überblick über die zivil- und aufsichtsrechtlichen Regeln, in: Zeitschrift für Bank- und Kapitalmarktrecht, S. 665–675.

Lippert, Susan K. (2007): Investigating postadoption utilization: An examination into the role of interorganizational and technology trust, in: IEEE Transactions on Engineering Management, 54. Jg., Nr. 3, S. 468–483.

Luhmann, Niklas (1979): Trust and Power, Chichester.

McKnight, D. Harrison u. a. (2011): Trust in a specific technology: An investigation of its components and measures, in: ACM Transactions on management information systems (TMIS), 2. Jg., Nr. 2, S. 1–25.

Middlesex University London (2018): Study on risks and opportunities of digitalisation for financial inclusion. The perspective of vulnerable users in Estonia, Italy and UK with a focus on groups covered by the European Accessibility Act, URL: <https://op.europa.eu/en/publication-detail/-/publication/61e0f61f-802c-11e9-9f05-01aa75ed71a1>.

Möllering, Guido (2006): Trust: Reason, Routine, Reflexivity, Oxford.

Nass, Clifford/Moon, Youngme (2000): Machines and mindlessness: Social Responses to Computers, in: Journal of Social Issues, 56. Jg., Nr. 1, S. 81–103.

OECD (2024): Finanzbildung in Deutschland. Finanzielle Resilienz und finanzielles Wohlergehen verbessern, URL: [https://www.bundesfinanzministerium.de/Content/DE/Downloads/Internationales-Finanzmarkt/Finanzielle-Bildung/oecd-bestandaufnahme-zur-finanzbildung.pdf?\\_\\_blob=publicationFile&v=2](https://www.bundesfinanzministerium.de/Content/DE/Downloads/Internationales-Finanzmarkt/Finanzielle-Bildung/oecd-bestandaufnahme-zur-finanzbildung.pdf?__blob=publicationFile&v=2), Stand: 24. Juni 2024.

OECD/INFE (2023): OECD/INFE 2023 international survey of adult financial literacy. Annex D. Tables, URL: <https://www.oecd-ilibrary.org/docserver/56003a32-en.pdf?expires=1719260327&id=id&accname=guest&checksum=506C03031DD26F6F7C93C7CD8C4E0327>, Stand: 24. Juni 2024.

Omlor, Sebastian (2024): Echtzeitüberweisung und Empfängerüberprüfung nach der reformierten SEPA-Verordnung, in: Neue Juristische Wochenschrift, S. 3478–3485.

Ozili, Peterson (2020): Theories of financial inclusion, URL: <https://mpira.ub.uni-muenchen.de/104257/>.

Pavlou, Paul A. (2003): Consumer Acceptance of Electronic Commerce: integrating Trust and Risk with the Technology Acceptance Model, in: Journal of Electronic Commerce, 7. Jg., Nr. 3, S. 101–134.

Säcker, Franz Jürgen u. a. (Hrsg.) (2023): Münchener Kommentar zum Bürgerlichen Gesetzbuch, 9. Aufl., München.

Sako, Mari (1992): Prices, Quality and Trust: Inter-firm Relationships in Britain and Japan, Cambridge.

Shapiro, Susan P. (1987): The Social Control of Impersonal Trust, in: American Journal of Sociology, 93. Jg., S. 623–658.

**Digital Abgehängt**

SINUS (2020): Digitale Teilhabe von Menschen mit Behinderung. Trendstudie, URL: <https://www.aktion-mensch.de/inklusion/barrierefreiheit/studie-digitale-teilhabe>.

S-Payment (2024): Bezahlverhalten der Verbraucher. S-Payment Studie 2024, URL: [https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.s-payment.com/bin/servlets/sparkasse/download%3Fpath%3D%252Fcontent%252Fdam%252Fmandant-s-payment%252Fpresse%252F2023%252Fpdf%252FStudie\\_Bezahlverhalten-der-Verbraucher.pdf%26name%3DStudie\\_Bezahlverhalten-der-Verbraucher.pdf&ved=2ahUKEwjEiPD7pKSJAxV1zQIHdibBLUQFnoECBUQAQ&usg=AOvVaw2mXx7S2Mk7cjg-JXwRospU](https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.s-payment.com/bin/servlets/sparkasse/download%3Fpath%3D%252Fcontent%252Fdam%252Fmandant-s-payment%252Fpresse%252F2023%252Fpdf%252FStudie_Bezahlverhalten-der-Verbraucher.pdf%26name%3DStudie_Bezahlverhalten-der-Verbraucher.pdf&ved=2ahUKEwjEiPD7pKSJAxV1zQIHdibBLUQFnoECBUQAQ&usg=AOvVaw2mXx7S2Mk7cjg-JXwRospU).

statista/YouGov (2020): Was (junge) Kunden von ihrer Bank erwarten, URL: <https://de.statista.com/infografik/22814/was-junge-kunden-von-ihrer-bank-erwarten/>, Stand: 24. November 2024.

Statistisches Bundesamt (2021): Öffentliche Sozialleistungen. Lebenslagen der behinderten Menschen Ergebnis des Mikrozensus, Wiesbaden, URL: [https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Gesundheit/Behinderte-Menschen/Publikationen/Downloads-Behinderte-Menschen/lebenslagen-behinderter-menschen-5122123199004.pdf?\\_\\_blob=publicationFile](https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Gesundheit/Behinderte-Menschen/Publikationen/Downloads-Behinderte-Menschen/lebenslagen-behinderter-menschen-5122123199004.pdf?__blob=publicationFile), Stand: 24. November 2024.

Statistisches Bundesamt (2024): Schwerbehinderte: Deutschland, Stichtag, Geschlecht. Code: 22711-0001, Wiesbaden, URL: <https://www-genesis.destatis.de/datenbank/online/statistic/22711/table/22711-0001>, Stand: 24. November 2024.

Statistisches Bundesamt (2024): 7,9 Millionen schwerbehinderte Menschen leben in Deutschland. 9,3 % der Gesamtbevölkerung haben eine schwere Behinderung, Wiesbaden, URL: [https://www.destatis.de/DE/Presse/Pressemitteilungen/2024/07/PD24\\_281\\_227.html](https://www.destatis.de/DE/Presse/Pressemitteilungen/2024/07/PD24_281_227.html), Stand: 24. November 2024.

Thatcher, Jason Bennett u. a. (2010): The role of trust in postadoption IT exploration: An empirical examination of knowledge management systems, in: IEEE Transactions on Engineering Management, 58. Jg., Nr. 1, S. 56–70.

Themenpapier BdZ-DG (2024a): Bargeld erhalten – für persönliche und gesellschaftliche Resilienz sowie Autonomie, URL: <https://www.bundesbank.de/resource/blob/938508/9eda74a1e9650556d4f09db0649f3e9b/mL/2024-08-22-bargeld-anlage1-data.pdf>.

Themenpapier BdZ-DG (2024b): Bargeld erhalten – für schnelles und unkompliziertes Bezahlen, als Korrektiv im Zahlungsverkehr und für individuelle und gesellschaftliche Resilienz, URL: <https://www.bundesbank.de/resource/blob/938510/4353f3b1d0395ed6633f3705a4066c74/mL/2024-08-22-bargeld-anlage2-data.pdf>.

Verbraucherzentrale Bundesverband e.V. (2023): Bargeld zukunftssicher machen. Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zum Legislativvorschlag der Europäischen Kommission on the legal tender of euro banknotes and coins, COM (2023) 364 final, URL: [https://www.vzbv.de/sites/default/files/2023-08/230810\\_Stellungnahme\\_Bargeld\\_Legativvorschlag\\_BMF\\_final.pdf](https://www.vzbv.de/sites/default/files/2023-08/230810_Stellungnahme_Bargeld_Legativvorschlag_BMF_final.pdf), Stand: 28. Januar 2025.

Verbraucherzentrale Bundesverband e.V. (2024): Basiskonto-Entgelte im europäischen Vergleich, Berlin, URL: [https://www.vzbv.de/sites/default/files/2024-03/24-01-15%20Bericht\\_Basiskontoentgelte.pdf](https://www.vzbv.de/sites/default/files/2024-03/24-01-15%20Bericht_Basiskontoentgelte.pdf).

Verbraucherzentrale Bundesverband e.V. (2024): Bank oder Betrüger? Erhebung zur Erkennbarkeit von Betrug im digitalen Zahlungsverkehr, URL: [https://www.vzbv.de/sites/default/files/2024-05/24-05-09%20Bericht\\_vzbv\\_Betrugserkennung.pdf](https://www.vzbv.de/sites/default/files/2024-05/24-05-09%20Bericht_vzbv_Betrugserkennung.pdf).

Verbraucherzentrale Bundesverband e.V. (2024): Geldforum: Bezahlen zukunftsfest machen. Repräsentative vzbv-Befragung legt nahe: Akzeptanz und Zugang zum Bargeld wird für Verbraucher:innen schwieriger.

Zahrte, Kai (2024a): Aktuelle Entwicklungen im Zahlungsdiensterecht (2022–2023), in: Zeitschrift für Bank- und Kapitalmarktrecht, Nr. 4, S. 135–143.

Zahrte, Kai (2024b): Warnpflichten der Banken zum Schutz ihrer Kunden, in: Zeitschrift für Bank- und Kapitalmarktrecht, Nr. 14, S. 593–601.

Zucker, Lynne G. (1986): Production of Trust: Institutional Sources of Economic Structure, 1840-1920, in: Staw, B. M./Cummings, L. L. (Hrsg.): Research in Organizational Behaviour, Greenwich, CT, S. 53–111.