Gesetz soll mobiles Bezahlen und Sicherheit stärken

Unbar

Tobias Haar

Im Bereich mobile Bezahlsysteme und Fintech-Start-ups bewegt sich derzeit einiges. Mit der Umsetzung der Zweiten Zahlungsdiensterichtlinie soll das deutsche Recht angepasst werden. Zahlreiche IT-technische Vorgaben sind aber noch offen.

Deutsche schwören auf Bargeld und Girokarten. „Zahlen per Handy mag im Ausland gängig sein – in Deutschland nicht." So stand es jüngst im Handelsblatt in einem Artikel über eine Studie des Forschungsinstituts EHI Retail Institute. Danach können sich 69 Prozent der Verbraucher hierzulande mobiles Bezahlen nicht vorstellen. Nur 19 Prozent wären dazu bereit. Häufig genannter Grund für die Ablehnung sind Sicherheitsbedenken. Die Angebote nehmen gleichwohl zu. Bei Shell ist mittlerweile das Bezahlen der Tankfüllung via Handy möglich. Apple Pay soll demnächst in Deutschland verfügbar sein. Bis diese Bezahlformen aber gleich beliebt sein werden wie beispielsweise in China, wird es noch dauern.

Unterdessen tut sich im Bereich der gesetzlichen Rahmenbedingungen einiges. Auf EU-Ebene wurde im Herbst 2015 die EU-Richtlinie über Zahlungsdienste überarbeitet (sie ist über „Alle Links" im blauen Kästchen zu finden). Unter Fachleuten ist sie schlicht als Payment Service Directive 2 (PSD2) bekannt. Kurz vor Ende der laufenden Legislaturperiode hat der Bundestag jüngst das „Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie", kurz ZDUG, verabschiedet. Der Bundesrat hat keine Einwände dagegen erhoben, sodass es nun durch den Bundespräsidenten ausgefertigt und im Bundesgesetzblatt veröffentlicht werden kann.

Da es sich bei PSD2 um eine Richtlinie und nicht um eine Verordnung der EU handelt, muss jedes EU-Mitgliedsland – selbst das Vereinigte Königreich ungeachtet des Brexit – deren Vorgaben in nationales Recht umsetzen. Die Frist dazu läuft am 13. Januar 2018 ab. Ab diesem Zeitpunkt gilt dann auch das ZDUG, womit Deutschland seiner Umsetzungspflicht fristgerecht nachgekommen ist. Die EU strebt eine gleichzeitige Vollharmonisierung in diesem Bereich an, um in den Mitgliedsländern gleiche Wettbewerbsbedingungen zu schaffen.

Keine Gebühren für einzelne Zahlarten

Beim ZDUG handelt es sich um eine weitgehend unveränderte Umsetzung der PSD2 in deutsches Recht. Es bringt zahlreiche Änderungen der bisherigen regulatorischen Vorschriften insbesondere im Bereich Compliance mit sich. Neben klassischen Banken und etablierten Bezahldiensten wie PayPal und Co. betrifft es auch Unternehmen, die künftig Zahlungsdienstleistungen erbringen wollen. Zusätzlich bringt es Änderungen zivilrechtlicher Vorschriften, beispielsweise des Bürgerlichen Gesetzbuches, mit sich. Verboten wird zum Beispiel das sogenannte Surcharging, also das Erheben einer Zusatzgebühr für bestimmte Bezahlmethoden etwa im Onlinehandel oder beim Buchen von Flugreisen im Internet und dergleichen (Abbildung 1).

Geändert haben sich auch die Voraussetzungen, wann ein „Zahlungsdienst" vorliegt, der sich an die teils strengen Regularien zu halten hat. Nicht unter die neuen Regelungen fallen unter anderem „Dienste, die von technischen Dienstleistern erbracht werden, die zwar zur Erbringung der Zahlungsdienste beitragen, jedoch zu keiner Zeit in den Besitz der zu übertragenden Gelder gelangen". Gemeint sind damit in erster Linie Hardware-, Software- und Datenbanklieferanten oder rein technische Dienstleister für aufsichtspflichtige Zahlungsdienstleister.

iX-TRACT

- Das gerade verabschiedete Gesetz zur Umsetzung der Zweiten EU-Zahlungsdiensterichtlinie soll innovative Bezahlverfahren innerhalb der EU fördern und Verbraucherrechte stärken.
- Die neuen Regulierungen sehen unter anderem vor, diskriminierungsfrei für Zahlungsdiensteanbieter Schnittstellen für den Zugriff auf Daten etablierter Finanzinstitute zu schaffen. Damit einhergehende Sicherheitsmaßnahmen sind noch nicht abschließend geregelt.
- Verbraucher können sich freuen: Extragebühren für Kreditkartenzahlung sollen bald der Vergangenheit angehören.

Solche zusätzlichen Gebühren für einzelne Zahlungsarten gehören bald der Vergangenheit an, denn nach den neuen EU-Regelungen sind sie unzulässig (Abb. 1).

Ausgenommen sind auch „Zahlungsvorgänge, die von einem Anbieter elektronischer Kommunikationsnetze oder -dienste zusätzlich zu elektronischen Kommunikationsdiensten für einen Teilnehmer des Netzes oder Dienstes bereitgestellt werden“, wenn es dabei um den „Erwerb von digitalen Inhalten und Sprachdiensten“ wie Klingeltönen, Hintergrundbildern, Musik, Spielen, Videos oder Apps von maximal 50 Euro pro Transaktion und höchsten 300 Euro pro Monat geht. Allerdings müssen diese Dienstleister derartige Tätigkeiten bei der Bundesanstalt für Finanzdienstleistungsaufsicht anzeigen. Dies gilt aber nur, wenn die technische Transportleistung, also etwa die Informationsübertragung, die „inhaltliche Leistung“ überwiegt.

Sonderfall: Karten mit begrenzter Reichweite

Handelsvertreter dagegen müssen sich künftig in manchen Fällen der Aufsicht über Zahlungsdienste unterwerfen. Dies gilt, wenn sie Plattformen des elektronischen Geschäftsverkehrs betreiben und dort beim Verkauf von Waren und Dienstleistungen sowohl im Namen des Zahlenden, also des Kunden, als auch des Zahlungsempfängers, also des Verkäufers oder Dienstleisters, auftreten. Das betrifft B2B-Plattformen, aber in etlichen Fällen auch Verkaufsportale wie Amazon.

Ausgenommen von der neuen Regulierung sind „Zahlungsinstrumente in begrenzten Netzen“. Darunter sind Kundenkarten, Tankkarten, Mitgliedskarten, Fahrkarten des öffentlichen Verkehrs, Parktickets, Essensgutscheine oder Gutscheine für bestimmte Dienstleistungen zu verstehen. Die Ausnahme greift, wenn diese Zahlungsinstrumente nur „innerhalb eines begrenzten Netzes von Dienstleistern im Rahmen einer Geschäftsvereinbarung mit einem professionellen Emittenten“ oder nur „für den Erwerb eines sehr begrenzten Waren- oder Dienstleistungsspektrums eingesetzt werden können“.

Nicht ganz klar ist in diesem Zusammenhang, wie man beispielsweise Tankkarten bewerten soll, mit denen sich neben dem Kraftstoff auch der Reiseproviant et cetera bezahlen lässt. Essensgutscheine oder Gutscheine im sozial- oder arbeitsrechtlichen Bereich sind ebenfalls von der Regulierung ausgenommen. In zahlreichen Fällen besteht jedoch zumindest eine Anzeigepflicht.

Viel diskutiert sind derzeit die Vorschriften über „Dritte Zahlungsdienstleister“. Hierbei handelt es sich um Anbieter von Zahlungsauslöse- und Kontoinformationsdiensten. Zum einen werden diese Dienste einer stärkeren Regulierung unterworfen, die Einfluss auf das Geschäftsmodell – etwa von Fintechs in diesem Bereich – haben können. Zum anderen erhalten sie über eine Schnittstelle einen gesetzlich abgesicherten Zugriff auf die Konten des Kunden bei den kontenführenden, also in der Regel den etablierten Banken (Abbildung 2). Diese müssen Zahlungsaufträge von Zahlungsauslösedienstleistern diskriminierungsfrei genauso behandeln wie Zahlungsaufträge, die ihre Kunden direkt abgeben.

Die Vorgaben in Bezug auf die Sicherheit beim Erbringen von Zahlungsdiensten treten erst zu einem späteren Zeitpunkt in Kraft. Vorgesehen ist, dass zunächst die EU-Kommission technische Regulierungsstandards für die Kundenauthentifizierung sowie die Kommunikation erarbeitet. Die European Banking Authority, kurz EBA, hat der EU-Kommission Ende Februar 2017 ihren finalen Entwurf für diese sogenannten „technischen Regulierungsstandards (RTS)“ übermittelt.

Dem war eine intensive Diskussion mit Unternehmen und Branchenverbänden vorausgegangen, die zahlreiche Än-

derungswünsche vorgebracht hatten. Ein Punkt war beispielsweise, dass Drittanbieter zur Nutzung der jeweiligen Schnittstelle der kontenführenden Bank verpflichtet werden sollten. Dagegen soll das bislang genutzte Screen-Scraping-Verfahren untersagt werden – was einige Fintechs bereits deswegen bedauern, weil sie damit kein Backup für den Fall haben, dass die Schnittstellenlösung nicht funktioniert. Den etablierten Banken geht es in ihrer Lobbyarbeit stark um die Hoheit über Daten, Infrastruktur und vor allem ihre Kunden. Kritiker befürchten zudem, dass dadurch die Hemmschwelle für ein Verbot des Screen Scraping für Zugriffe auf Depot- und Kreditkarten sinkt.

Strenge Sicherheitsprüfungen vorgesehen

Der RTS-Entwurf enthält Vorgaben, dass Nutzer einer Multibanking-App sich alle 90 Tage mit zwei Sicherheitsfaktoren authentifizieren müssen. Das Synchronisieren der Kontodaten zwischen Bank und Dienstleister soll bis zu vier Mal innerhalb von 24 Stunden gestattet sein, wenn keine individuellen Regeln, zum Beispiel für eine Aktualisierung in Echtzeit, getroffen wurden. Nach einigen Diskussionen hat man sich bei Kartenzahlungen und Überweisungen darauf verständigt, dass erst ab einem Betrag in Höhe von 30 Euro eine strenge Sicherheitsüberprüfung mittels Fingerabdruck oder Passworteingabe vorgeschrieben werden soll.

Des Weiteren stellte sich die Frage, ob Verhaltensdaten Bestandteil einer starken Kundenauthentifizierung sein dürfen. Zur Authentifizierung verlangt die PSD2 grundsätzlich die Nutzung zweier unabhängiger Faktoren mit Elementen aus den Bereichen Wissen, Besitz und Eigenschaften des Nutzers (Inhärenz; zum Beispiel Fingerabdruck oder Netzhaut). In diesem Bereich soll es nach dem Willen der EBA auch zum Einsatz von Leistungen eines Vertrauensdiensteanbieters nach der neuen eIDAS-Verordnung kommen, die EU-weit die Grundlagen für die elektronische Identifizierung und Vertrauensdienste schafft.

Ende Mai 2017 hat die EU-Kommission die EBA zur Nachbesserung ihres „Final Draft“ aufgefordert. Es wird also noch dauern, bis diese Vorgaben endgültig feststehen und veröffentlicht werden. Danach haben die betroffenen Unternehmen sowohl nach PSD2 als auch nach ZDUG 18 Monate Zeit zur Umsetzung. „Bis zu deren Inkrafttreten ist auf die Grundsätze einer ordnungsgemäßen Geschäftsorganisation der Zahlungsdienstleister abzustellen, aus denen sich die Erforderlichkeit elementarer IT-Sicherheitsmaßnahmen ergeben, insbesondere auch eine Verschlüsselung der Kommunikation bei der Übertragung vertraulicher Informationen“, heißt es in der Gesetzesbegründung. Damit sind auch die „Leitlinien zur Sicherheit von Internetzahlungen“ der EBA von Dezember 2014 noch eine Weile verbindlich („Alle Links“).

Bislang galten in diesem Bereich die Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht in den „Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi)“ [1]. Sobald allerdings die RTS final verabschiedet sein werden, müssen auch die MaSi angepasst werden. Es ist absehbar, dass es hier zu neuen technischen Vorgaben kommen wird.

Stufenweise Abschaffung der Extragebühren

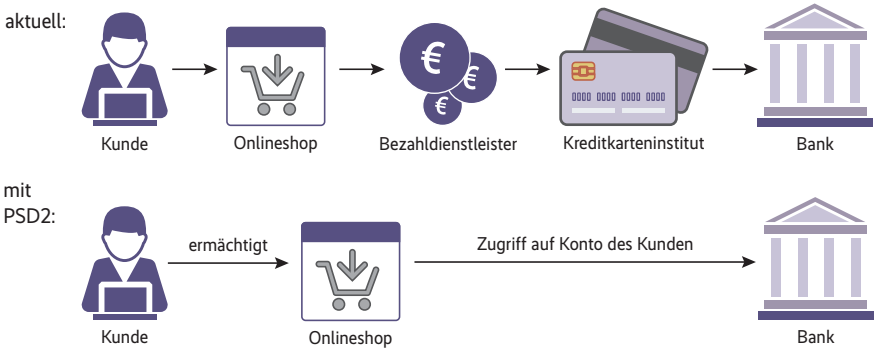
Die Einführung eines künftigen § 270a in das Bürgerliche Gesetzbuch regelt „Vereinbarungen über Entgelte für die Nutzung bargeldloser Zahlungsmittel“. Zentraler Regelungspunkt ist das Verbot von Entgelten „für die Nutzung einer SEPA-Basislastschrift, einer SEPA-Firmenlastschrift, einer SEPA-Überweisung oder einer Zahlungskarte“. Vielen Verbraucherschützern war es in der Vergangenheit ein Dorn im Auge, dass beispielsweise bei Flugbuchungen für die Bezahlung mit Kreditkarten häufig Zusatzkosten anfielen. Nach dem Willen des Gesetzgebers ist damit ab dem 13. Januar 2018 Schluss. Laut Justizstaatssekretär Kelber (SPD) wird damit „ein Ärgernis für viele Verbraucher“ abgeschafft (Abbildung 3).

Allerdings gilt dies nur für sogenannte Vier-Parteien-Kartenzahlverfahren, wozu laut Gesetzesbegründung „die gängigsten Kartenzahlverfahren in der Bundesrepublik Deutschland“ zählen. Bei sogenannten Drei-Parteien-Kartenzahlverfahren greift das Surcharging-Verbot erst ab Herbst 2018, um deren Besonderheiten zu berücksichtigen. Bei diesen Verfahren erbringt der jeweilige Dienstleister „selbst Annahme- und Abrechnungs- sowie Kartenausgabedienste“ und nimmt „kartengebundene Zahlungsvorgänge von dem Zahlungskonto eines Zahlers auf das Zahlungskonto eines Zahlungsempfängers“ vor. Beispiele hierfür sind American Express und girocard, weil hier die Kreditkarten direkt an Kunden und ohne zwischengeschaltete „Issuing Bank“ ausgegeben werden.

Verbraucher muss wählen können

Erst kürzlich hat die Deutsche Bahn in einem Streit mit dem „Verbraucherzentrale Bundesverband“ (vzbv) diesbezüglich vor dem Bundesgerichtshof (Aktenzeichen KZR 39/16) eine empfindliche Niederlage erlitten. Wenn „Sofortüberweisung“ als einzige kostenlose Bezahlmethode angeboten wird, ist dies rechtswidrig, so die Richter. Der vzbv fasst in einer Pressemitteilung das Ergebnis zusammen: Das Angebot von Bezahlmethoden dürfe Kunden „nicht dazu zwingen, mit einem nicht beteiligten Dritten in vertragliche Beziehungen zu treten und diesem hochsensible Finanzdaten zu übermitteln, zumal dies gegen die vertragliche Vereinbarung mit ihrer Bank verstoße“. Zwar darf diese Bezahlmethode weiterhin angeboten werden, es müssten aber weitere kostenlose Bezahlmethoden hinzukommen.

Weitere den Verbraucher schützende Vorgaben sehen vor, dass dieser auch



Die neue Richtlinie soll unter anderem innovative Zahlungsdienste ermöglichen und die dafür erforderlichen Vorgänge vereinfachen. Ein Mittel dazu sind die Schnittstellen, die den direkten Zugriff auf Daten der etablierten Banken erlauben (Abb. 2).

künftig Lastschriften innerhalb von acht Wochen widerrufen kann. Erstmals soll dies EU-weit gelten. Bei nicht autorisierten Zahlungen sinkt der maximale Haftungsbetrag für Verbraucher von 150 Euro auf 50 Euro.

Die PSD2 sieht vor, dass bis Anfang 2021 eine Überprüfung der Vorschriften auf etwaigen Anpassungsbedarf erfolgt. Bereits jetzt ist absehbar, dass durch Angebote in den Bereichen Instant Payment und Blockchain weitere Geschäftsmodelle entstehen werden, die ganz eigene Regularien und Vorgaben benötigen. Die Verabschiedung zusätzlicher regulatorischer Vorgaben ist also nur eine Frage der Zeit.

Auch die Bahn muss sich in Kürze von ihrem Zahlungsmittelentgelt verabschieden – Verbraucher und Verbraucherschützer wird es freuen (Abb. 3).

Alles noch zu langsam

Gerade dem Instant Payment werden dabei große Auswirkungen zugeschrieben. Die Einführung von SEPA konnte die Dauer von Überweisungen innerhalb der Eurozone auf einen Werktag reduzieren. Innerhalb Deutschlands funktioniert dies bislang ebenfalls in dieser Geschwindigkeit, die mit Echtzeit noch wenig zu tun hat. Manche sprechen hier von „digitaler Ungeduld“. Der Grund dafür liegt beispielsweise bei Überweisungen darin, dass diese über die Bundesbank zur Prüfung geschickt werden, bevor dann Buchungen und Gegenbuchungen bei den verschiedenen Finanzinstituten erfolgen.

Ziel der EU-Kommission ist es, diese Zeitspanne auf Sekunden zu verkürzen. Für Beträge bis zu 15 000 Euro soll dies künftig nur noch bis zu zehn Sekunden in Anspruch nehmen und maximal 0,2 Eurocent kosten. Ab November 2017 soll ein Testbetrieb und ab November 2018 ein Livebetrieb der „Target Instant Payment Settlements“-Plattform, kurz TIPS, erfolgen. Verbindlich ist die Teilnahme daran aber (noch) nicht. Fachleute gehen davon aus, dass im Vergleich zu SEPA mit relativ geringen Implementierungskosten hier große IT-Projekte mit entsprechenden Investitionsvolumina auf die Finanzbranche zukommen werden. Wenn künftig Überweisungen sofort und nicht zu bestimmten und abgestimmten Uhrzeiten übermittelt werden sollen, sind insbesondere an die IT-Sicherheit deutlich höhere Anforderungen zu stellen.

Mit PayPal, Sofortüberweisung und giropay gibt es zwar heute schon erste Anbieter zeitnaher Überweisungen. Sie tragen allerdings das Risiko des Scheiterns derjenigen Geldtransaktion in sich, die im Hintergrund nach den beschriebenen bisherigen Abläufen oder über Kreditkartenzahlungen erfolgt. Laut Umfragen sollen elektronische Zahlungen bis 2020 bereits 12 Prozent des Transaktionsvolumens ausmachen, Tendenz weiter steigend. Da solche Zahlungen allerdings unumkehrbar sind, sind etliche Haftungsfragen insbesondere aus Kundensicht noch offen und müssen auf Ebene des Gesetzgebers noch diskutiert werden. Die PSD2 regelt diesen Bereich deswegen auch noch nicht.

Fazit

Mit der Zweiten Zahlungsdiensterichtlinie hat die EU 2015 die erste Richtlinie aus dem Jahr 2007 an die geänderten Rahmenbedingungen angepasst. Ab Januar 2018 gilt in Deutschland ein Gesetz zur Umsetzung der regulatorischen Vorgaben. Ziel ist ein verbesserter Verbraucherschutz sowie die Entwicklung und Nutzung innovativer Bezahlmethoden mittels mobiler Geräte und bei Onlinegeschäften. Zusätzlich sollen grenzüberschreitende Zahlungsdienste sicherer und schneller werden.

Ein wesentlicher Bereich der neuen Regelungen betrifft den sogenannten „Open Access“. Er soll es Zahlungsdienstanbietern ermöglichen, neuartige Dienste zu entwickeln und anzubieten. Dazu müssen die etablierten Banken Zugriff auf Kunden- und Kontendaten gewähren. Über die technischen Details streiten die verschiedenen Interessengruppen aber derzeit noch. Für die etablierten Banken könnten sich die Veränderungen teilweise als große Herausforderung erweisen. Mitunter ist in diesem Zusammenhang von einem bevorstehenden „IT-Mammutprojekt“ die Rede.

Bis die technischen Regulierungsstandards durch die EU-Kommission veröffentlicht und in Kraft gesetzt werden, kann es noch dauern. Bis dahin gelten die bisherigen Vorgaben und der „Stand der Technik“ [2] als Mindestmaßstab für die erforderliche IT-Sicherheit.

Schließlich ist bei Digitalisierungsprojekten, zum Beispiel App-gestützten Fahrkartensystemen für den öffentlichen Verkehr, im B2C-Umfeld stets darauf zu achten, dass die gesetzlichen Bedingungen eingehalten werden. Dies gilt auch für Instant Payment sowie den Einsatz von Blockchain-Verfahren, die noch nicht ausdrücklich Gegenstand der jetzt verabschiedeten Gesetzesreform sind. Alle diese Geschäftsmodelle können aber der Definition eines „Zahlungsdienstes“ und damit den strengen regulatorischen Vorgaben unterliegen. Mit weiteren gesetzlichen Änderungen ist in der Finanzbranche auf jeden Fall zu rechnen. (ur)

Tobias Haar, LL.M., MBA,

ist Rechtsanwalt mit Schwerpunkt IT-Recht bei Vogel & Partner mbB in Karlsruhe.

Literatur

[1] Tobias Haar; Recht; Zwei aus drei; Sicherheitsvorgaben für Internet-Zahlungsdienstleister; *iX* 8/2015, S. 100

[2] Karsten U. Bartels; Recht; Gretchenfrage; Der Stand der Technik in der IT-Sicherheit – komplexe technische und rechtliche Anforderungen; *iX* 7/2017, S. 48

Alle Links: www.ix.de/ix1709098