www.jusletter-it.eu

Rehana Harasgama

Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme

Bericht über die Tagung vom 29. Oktober 2014, in Zürich

The conference «Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme» held on 29 October 2014 addressed the legal and technological challenges of web-based and mobile payment systems which are quickly gaining momentum and show a lot of potential for the future. This conference formed a part of a series of events dealing with issues at the interface of information technologies and law which are held in collaboration with the «Schweizer Forum für Kommunikationsrecht (SF-FS)» by Prof. Dr. Rolf H. Weber, professor and director of the Center for Information and Communication Law at the University of Zurich and Prof. Dr. Florent Thouvenin, assistant professor and head of the chair for Information and Communication Law at the University of Zurich.

Category: Conference Proceedings
Field of law: E-Commerce
Region: Switzerland

Citation: Rehana Harasgama, Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, in: Jusletter IT 11 December 2014

Inhaltsübersicht

1 Überblick über die rechtlichen Rahmenbedingungen für webbasierte und mobile Zahlungssysteme

[Rz 1] Gemäss Prof. Dr. Rolf H. Weber fehlt bis heute in der Schweiz und auch in weiten Teilen des Auslands eine Regulierung neuer Marktteilnehmer im Bereich der Zahlungsdienste. Immerhin gibt es einige wenige Beispiele für Regulierungsansätze von webbasierten und mobilen Zahlungssystemen im Ausland, wie Brasilien und der Staat New York. Die EU hat im Hinblick auf neue Zahlungssysteme die Richtlinie zu E-Geld-Instituten bereits 2009 revidiert; zudem ist eine Revision der Zahlungsdienste-Richtlinie vorgesehen. Nachdem der Bundesrat nun aber seinen Bericht zu virtuellen Währungen[1] veröffentlicht hat, scheinen Regulierungen in diesem Gebiet für die Schweiz in weiter Ferne zu liegen, zumal er in diesem Bericht einen dringenden Handlungsbedarf verneint und den Standpunkt einnimmt, dass aktuelle Rechtsfragen mit den bestehenden Regulierungen lösbar sind.

[Rz 2] Bei virtuellen Zahlungen (anhand von virtueller Währung, hierzu zählen elektronisches Geld, Kryptowährungen, Bitcoins) handelt es sich primär um «alle Zahlungsvorgänge, die über ein elektronisches Netzwerk getätigt werden». Im Gegensatz dazu beruhen mobile Zahlungen auf mobilen Geräten, die Funktionsweise ist jedoch praktisch identisch. Somit ist es möglich, anhand beider Vorgänge digitale Währung gegen herkömmliches Geld zu tauschen. Die technischen Rahmenbedingungen dieser Angebote stellen aus Sicht des Regulators bedeutende Sicherheitsanforderungen an die Anbieter, welche Weber in zwei Gruppen zusammenfasst: IT-Sicherheitsarchitektur (umfasst Rechnersysteme, Kryptographie und Hardware-/Softwarelösungen und soll eine gewisse Sicherheitsumgebung für webbasierte und mobile Zahlungssysteme gewährleisten) und einzelne Sicherheitsaspekte (Authentizität, Vertraulichkeit, Integrität und Anonymität, die Transaktionspartner überprüfbar und den Inhalt sowie die Übermittlung der Zahlungen vertraulich, integer und anonym machen). Die Systemsicherheit («state of the art») muss gewährleistet werden und die Systeme müssen akzeptanzfähig sein. Zudem muss die Zahlung rückverfolgbar und haltbar sein.

[Rz 3] Für die verschiedenen Rechtsgebiete führen diese neuen Zahlungsmodelle teilweise zu

[1] Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070), abrufbar unter: http://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf, zuletzt besucht am 19. November 2014.

hohen, zum Teil aber auch zu geringen «Rechtsrisiken». Zu den Bereichen mit geringen Risiken zählen das Bargeldmonopol des Bundes (Art. 99 Abs. 1 der Bundesverfassung [BV]), die Normen zu Zahlungssystemen gemäss dem Nationalbankgesetz (NBG) und die Regelungen zur Börse sowie zu alternativen Handelsplattformen gemäss dem Börsengesetz (BEHG), weil Bitcoins und andere virtuelle Währungen heute nicht zu den alternativen Handelsplattformen zählen. Schwierigkeiten bietet eher die Anwendung des Bankengesetzes (BankG), da in der Schweiz keine Sonderregelung zu E-Geld-Instituten, wie etwa in der EU, oder zu Rechnungseinheiten besteht. Es stellt sich die Frage, ob Anbieter von webbasierten und mobilen Zahlungssystemen als Bank gem. Art. 1 Abs. 2 BankG und Art. 3a der Bankenverordnung (BankV) und Ziff. 18bis des FINMA-Rundschreibens 2008/3 qualifiziert werden können. Zur Beantwortung dieser Frage müsste zunächst zwischen den verschiedenen Diensten der Anbieter unterschieden werden. So können webbasierte und mobile Zahlungssysteme folgende Tätigkeiten übernehmen: Betreiben von Plattformen für den Kauf und Verkauf virtueller Währungen, die Verwendung und Annahme von webbasierten und mobilen Zahlungen als Zahlungsmittel für den Erwerb von Gütern und Dienstleistungen sowie für den Kauf und Verkauf virtueller Währungen (hierzu eingehend das Referat von Prof. Dr. Seraina Grünewald). Das Rundschreiben der FINMA fasst den Begriff der Bankintermediäre sehr weit. Entsprechend ist es zwar denkbar, Anbieter neuer Zahlungsformen als Bankintermediäre zu qualifizieren, in der Regel werden Drittanbieter jedoch nicht dazu zu zählen sein.

[Rz 4] Wie einleitend erwähnt, hängt der Erfolg neuer Zahlungssysteme primär vom Vertrauen der Nutzer in die Integrität und Authentizität dieser Systeme ab. Aus der Perspektive des Datenschutzes schaffen webbasierte und mobile Zahlungssysteme entsprechend zahlreiche Risiken, welche sich grundsätzlich in zwei Problemkreise aufteilen lassen. Einerseits bestehen bei der Anwendung solcher Zahlungsmodelle Datensicherheits- und Systemrisiken, so vor allem im Hinblick auf Datenverlust oder Datenmissbrauch innerhalb des Systems. Andererseits bestehen allgemeine datenschutzrechtliche Risiken, da in solchen Anwendungen stets Daten gesammelt und aufbewahrt werden. Dadurch besteht bspw. die Gefahr, dass Persönlichkeitsprofile erstellt werden. Der EDÖB hat denn auch bereits 2012 eine Empfehlung zu mobilen Zahlungsdiensten abgegeben; darin beschreibt er Massnahmen, welche die Anbieter solcher Zahlungssysteme vorsehen sollten und stellt vor allem die Prinzipien der Datenminimierung und Zweckbindung in den Vordergrund. Primär geht es darum, Missbrauchsrisiken früh zu identifizieren und präventiv zu minimieren.

[Rz 5] Weber hält abschliessend fest, dass neue Anbieter weiterhin auftauchen, die Sicherheitsanforderungen an webbasierte und mobile Zahlungssysteme steigen und wohl auch die Auflagen für das Anbieten solcher Zahlungsmodelle zunehmen werden.

2 Technische Rahmenbedingungen für und Risikolage bei webbasierten mobilen Zahlungen

2.1 Risiken bei der Anwendung von Mobilgeräten

[Rz 6] Adrian Eberle, Senior Engineer bei SIX Payment Services, eröffnete den technischen Teil der Veranstaltung, indem er je zwei Anwendungsfälle von webbasierten und mobilen Banking- bzw. Zahlungssystemen vorstellte.

[Rz 7] Bei einer ersten E-Banking Anwendung ist das Handy Hilfsmittel («Second Factor») beim

Einloggen via PC auf dem E-Banking Portal der Bank, wobei der Bankkunde nach Eingabe seines Passwortes («First Factor») am PC bei jedem Login auch noch einen einmaligen Zusatzcode eingibt, den er von der Bank über sein Handy erhält. Bei der zweiten Anwendung wird direkt vom Handy aus (d.h. ohne PC) auf das E-Banking Portal zugegriffen (M-Banking). Hier kann optional ein Second Factor in Form eines von der Bank an den Kunden herausgegebenen und auf diese Funktion spezialisierten externen Geräts verwendet werden.

[Rz 8] Das Handy als Zahlungsmittel ermöglicht hingegen die direkte Zahlung von Produkten oder Dienstleistungen «Face-to-Face» am «Point of Sale» (POS) bzw. von Käufen im Internet mit einer sog. Wallet- oder In-App-Zahlung.

[Rz 9] Gemäss Eberle stellt sich die Frage nach der Sicherheit solcher Banking- und Zahlungssysteme im Hinblick auf die Schutzbedürfnisse der Benutzer. Schutzbedürfnisse bestehen aus seiner Sicht in der Privatsphäre, namentlich hinsichtlich der Meta- (Bank, Verkäufer, Ort etc.) und Transaktionsdaten (Kontonummer, Betrag, Zahlungszweck etc.). Zudem müssen die Authentisierungs-Credentials geschützt werden, welche die Identifikatoren (Vertragsnummer, User-ID, Kartennummer etc.), First Factors (Statisches Passwort, PIN etc.) und Second Factors (Einmal-Passwörter, Kryptographische Schlüssel etc.) umfassen. Schliesslich müssen die Hardware (Verarbeitung und Interfaces) und die Prozesse (Registrierung wie z.B. Ersatz des Handys oder des SIMs) innerhalb des Zahlungssystems geschützt werden. Das Problem beim Schutz all dieser Faktoren liegt darin, dass Smartphones allgegenwärtig einsetzbar sein müssen und gleichzeitig verschiedene Interessen in einem Produkt repräsentieren. Zudem sind sie beinahe immer mit dem Internet verbunden. Ein Nutzer will mit seinem Smartphone alles erledigen können und gleichzeitig vor potentiellen Gefahren geschützt sein (Spannungsfeld: Universalität vs. Sicherheit). Die Anbieter (z.B. Apple, Google, Microsoft, Handyhersteller, Mobile Operator, App-Anbieter) wollen hingegen die gesammelten Daten speichern, aggregieren und auswerten (Big Data Analytics), wobei sie aber trotzdem dazu verpflichtet sind, die Privatsphäre ihrer Nutzer zu schützen (Spannungsfeld: Big Data vs. Privatsphäre), zumindest in Ländern mit entsprechender Gesetzgebung. Betrüger anderseits wollen monetäre Beute machen. Schliesslich melden Strafverfolgungsbehörden und Geheimdienste Ansprüche zum Schutz der nationalen Sicherheit an, teilweise über ihre Landesgrenzen hinaus. So verlangt die Strafverfolgung Zugang zu den vom Anbieter gespeicherten Daten (Spannungsfeld: Sicherheit vs. Überwachungssaat).

[Rz 10] Die geschilderten Banking- und Zahlungsmodelle sind mit verschiedenen Bedrohungen konfrontiert, so etwa dem Geräteverlust oder -diebstahl, Software-Fehler, Schadcodes, Rooting[2], Täuschung oder Backdoors[3]. Das bekannteste Beispiel ist wohl die Manipulierung von Sensoren in einem Gerät, bspw. der Kamera oder des Mikrofons. So ist es etwa möglich, die Kamera auf einem Handy unbemerkt aus einem App heraus oder über das Handynetzwerk bzw. das Internet (remote) einzuschalten. Dadurch kann dann z.B. ab einer Frontkamera-Auflösung von ca. 10 Megapixeln der eingegebene E-Banking Pin aus der Spiegelung in den Augen des Nutzers abgelesen werden. Darüber hinaus tragen die Nutzer dieser Zahlungssysteme oft selber zum Problem bei, indem sie sich täuschen lassen bzw. die vom Anbieter vorgegebenen Sicherheitsregeln nicht ein-

[2] Rooting nennt man den Prozess, der Nutzern von Smartphones, Tablets oder anderen Geräten erlaubt, mit dem bestehenden Betriebssystem eine privilegierte Steuerung innerhalb des Subsystems dieser Geräte zu erlangen. Rooting wird oft mit dem Ziel der Überwindung von (Sicherheits-) Einschränkungen genutzt.

[3] Als Backdoor (auch Trapdoor oder Hintertür genannt) bezeichnet man einen (oft vom Autor eingebauten) Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.

halten. Weitere Gefahren bestehen etwa im unbemerkten Erheben von Metadaten, im Ausspähen von Credentials, im App-Spoofing[4], im verdeckten Rooting oder in Angriffen auf den Lockscreen.

[Rz 11] Abschliessend verweist Eberle auf drei verschiedene Ansätze, um webbasierte und mobile Zahlungssysteme zu sichern: den *rein technischen*, den *interdisziplinären* und den *rein rechtlichen Ansatz*. Wird zum Schutz eines Zahlungssystems der erste Ansatz angewendet, können zwar die meisten technischen Risiken verhindert werden, die Gefahren durch Hacking mit neuen Methoden, Sicherheitslücken wegen Systemfehlern, Täuschung und staatlichen Angriffen werden aber immer bestehen. Beim interdisziplinären Ansatz handelt es sich um eine Kombination aus technischen, operativen und juristischen Elementen. Dadurch kann ein Gerät z.B. zu 99% vor potentiellen Bedrohungen geschützt werden. Das verbleibende z.B. 1% Risiko wird in Kauf genommen und aus den Erträgen der Zahlungsdienstleistung gedeckt, welche entsprechend hoch sein müssen. Der dritte (möglicherweise noch nie vertieft untersuchte) Ansatz wäre Sicherheit durch eine Regulierung von webbasierten und mobilen Zahlungssystemen.

2.2 Zukunftsszenarien für Cryptocurrencies — Wenn sich die Wolke verselbständigt

[Rz 12] Nachdem Adrian Eberle die heutige Technologie hinter webbasierten und mobilen Zahlungssystemen dargestellt hatte, wagte MSc ETH Luzius Meisser eine Zukunftsprognose von Bitcoins.

[Rz 13] Bei Bitcoins (die erste Kryptowährung überhaupt) handelt es sich um eine Währung ohne identifizierbaren Emittenten. Es ist ein dezentrales und sicheres Zahlungssystem, das von einem anonymen Kollektiv betrieben wird. Das Eigentum an dieser Währung wird im Gegensatz zu herkömmlichen Währungen nicht rechtlich, sondern technisch gewährleistet. So ist im Bitcoin System alles öffentlich, was bedeutet, dass jedermann jederzeit einsehen kann, wieviele Bitcoins von wo nach wo geschickt wurden (pseudonymisiert).

[Rz 14] Bitcoins sind durch die Distributed Ledger Technology (DLT) dezentral organisiert. Die DLT ist eine Art Eigentumsregister in der Cloud, das ohne zentrale Instanz das System der Bitcoins kontrolliert und vollständig transparent (Open Source) ist. Die Bitcoins werden anhand eines digitalen Signatur-Systems verifiziert und übertragen. Trotz dieser Öffentlichkeit sind die beteiligten Personen nicht direkt identifizierbar. Transaktionen können hier nur insoweit zurückverfolgt werden, als einzelne Transaktionen auf ein Pseudonym zurückführen.

[Rz 15] Heute gibt es bereits auf Bitcoins spezialisierte Hardware: Trezor Wallet, Bitcoin Bankomaten, physische Münzen, Noten und Mining Hardware. Der Trezor Wallet ist ein mobiles Gerät, auf welchem Bitcoins direkt als Währung gespeichert sind. Dies im Gegensatz zu einem Mobiltelefon, auf dem auch andere Applikationen installiert sind. Der Trezor Wallet bietet somit weniger Angriffsfläche für Hacker, Geheimdienste, Anbieter oder Verbrecher. An einem Bitcoin Bankomaten kann man hingegen offizielle Währung, also bspw. Schweizer Franken, einführen, um im Gegenzug Bitcoins in einer Art Urkunde ausgezahlt zu erhalten.

[Rz 16] Der Referent verweist nach seiner technischen Einführung auf die wichtigsten Rechtsfra-

[4] Spoofing (auf Deutsch Manipulation, Verschleierung oder Vortäuschung) nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken oder in diesen Fällen mobilen Geräten zur Verschleierung der eigenen Identität des Angreifers («Wolf im Schafspelz») mit dem Ziel des Missbrauchs der betroffenen Geräte.

gen im Bereich von Bitcoins: Ist ein Bitcoin ein Zahlungsmittel nach Geldwäschereigesetz (GwG) und Mehrwertsteuergesetz (MWStG)? Können Bitcoins als Währung oder Devisen nach dem Kollektivanlagengesetz (KAG) qualifiziert werden? Sind Miner[5] als Finanzintermediäre zu qualifizieren? In der Schweiz setzt der Betrieb einer Bitcoin-Börse wegen der Kundeneinlagen nach Auffassung von Meisser eine Bankenlizenz voraus. Aus seiner Sicht sollten Bitcoins jedoch nicht als E-Geld definiert werden, da E-Geld einen Emittenten voraussetzt. Ferner ist Meisser der Ansicht, dass Miner nicht als Finanzintermediäre qualifiziert werden können, da sie zu keinem Zeitpunkt über die transferierten Bitcoins verfügen. Die Frage, ob Bitcoins als Währung zu klassifizieren sind, ist umstritten, würde aber aus Sicht des Referenten Sinn machen.

[Rz 17] Meisser sieht in digitalen Währungen und generell in «Cryptofinance» grosses Potential. So erweitert zum Beispiel das Zuger Startup Ethereum das Bitcoin-Konzept soweit, dass nicht nur beliebige Währungen emittiert, sondern auch kryptographisch gesicherte Verträge oder gar ganze Organisationsabläufe in Computercode spezifiziert werden können. Solche Verträge (sog. self-executing contracts) werden von der Wolke durchgesetzt und automatisch ausgeführt, ohne auf ein funktionierendes Rechtssystem angewiesen zu sein. Allerdings muss sich erst noch zeigen, ob es überhaupt einen Bedarf für solche Systeme gibt.

3 Podiumsdiskussion

[Rz 18] An der ersten Podiumsdiskussion, welche sich den technischen Hintergründen und Möglichkeiten von webbasierten und mobilen Zahlungssystemen widmete und die von Florent Thouvenin moderiert wurde, nahmen neben den drei Referenten des ersten Teils auch Frau lic. iur. Claudia Keller, Rechtsanwältin in Zürich, und Frau lic. iur. Nicole Beranek Zanon EMBA HSG, Rechtsanwältin in Zug, teil.

[Rz 19] Beranek Zanon hielt einleitend fest, dass sich die Gesellschaft in einem Paradigmenwechsel befindet. So findet zurzeit eine Ablösung bestehender Zahlungsmöglichkeiten statt, wodurch das Geschäftsmodell der Banken ins wanken gerät. Dadurch können Distanzen überwunden werden, da z.B. eine Zahlung von den USA in die Schweiz mit der Hilfe von Bitcoins innert Sekunden ausgelöst werden kann. Diese Mobilität von Zahlungen wird die derzeit noch bestehenden regulatorischen Hürden und sicherheitstechnischen Risiken langfristig überwinden, weshalb sich bestehende Dienstleistungsanbieter (bspw. Banken) mit diesen neuen Modellen auseinandersetzen und ihre Geschäftsmodelle anpassen müssen. Das grösste Problem stellt derzeit die Regulierung dar, welche die neuen Modelle zu verhindern bzw. sie unter die geltenden Bestimmungen zu subsumieren versucht.

[Rz 20] Keller eröffnete ihr Statement damit, dass diese Entwicklungen bereits Realität sind. Webbasierte und mobile Zahlungssysteme werden sich in Zukunft aber noch stärker verbreiten. Das Problem liege wie in anderen Bereichen (beispielsweise im Bereich des Urheberrechts) primär darin, dass die Technologie dem Recht weit vorauseile. Es stelle sich die Frage, ob der Regulator in diesem Bereich tätig werden müsse, vor allem um die Sicherheit solcher Zahlungsmodelle und Transaktionen zu gewährleisten, ansonsten werden die Risiken weder von Anbieter-

[5] Grundsätzlich können sich alle Teilnehmer am Mining mit Hilfe von Bitcoin Cores beteiligen. Durch das Mining werden neue Blöcke erzeugt und anschliessend zur Blockkette hinzugefügt. Durch neue Blöcke werden neue Bitcoins ausgegeben und gleichzeitig ein Teil der neuen oder noch offenen Transaktionen bestätigt. Auf diese Weise findet eine dezentrale Geldschöpfung statt.

noch Nachfrageseite übernommen. Unter Verweis auf den Vortrag von Eberle äussert sich Keller gegenüber einem interdisziplinären Ansatz zur Regulierung dieser Zahlungsmärkte sehr positiv.

[Rz 21] Nach diesen Einstiegsstatements eröffnet Thouvenin die Diskussion für alle Teilnehmer der Tagung. Es stellt sich zuerst die Frage, ob ein Gerät geschützt ist, wenn Citrix darauf installiert ist? Eberle führt aus, dass in der PC-Welt verbreitete Schutzkonzepte (z.B. Virenscanner, Firewalls) auf Handys wenig effektiv seien, weil Handys eine andere Softwarearchitektur aufweisen: Im Gegensatz zu PCs wirken Schutzprogramme auf Handys i.d.R. nur auf Anwendungs- und Anwenderebene, d.h. mit höchstens gleich langen Spiessen wie Malware, und nicht wie bei PCs auf Betriebssystem- und Administratorebene, d.h. ohne taktische Vorteile gegenüber dem Angreifer. Für Anbieter von Sicherheitssoftware sei es i.d.R. nicht möglich, ihre Schutzprodukte im Betriebssystem und mit Root-Privilegien zu installieren. In der «Sandbox»[6] eines Apps gespeicherte Daten seien nur so sicher wie die Wände der Sandbox. Durch Softwarefehler, Rooten oder Aktivieren des Debugmodus würden die Wände der Sandbox durchlässig. Weitere Gefahren lauern im «Repackaging»[7] von Apps gepaart mit Betriebssystemschwachstellen, so dass sich ein schon länger installiertes App plötzlich bösartig verhält (z.B. scheinbar wie bisher funktioniert, aber den eingegebenen PIN stillschweigend an einen externen Server weiterleitet). Stammen zwei Android-Apps vom gleichen Entwickler, ist es möglich, dass diese Apps verdeckt miteinander kommunizieren und so ihre indivdiuellen Sicherheitsfreigaben (Permissions) kombinieren (sog. «Privilege Escalation»).

[Rz 22] Thouvenin lenkt die Diskussion zum Schluss auf die Frage des Datenschutzes in webbasierten und mobilen Zahlungssystem. Er weist daraufhin, dass sich herausgestellt hat, dass sich die Anbieter der Probleme bewusst sind, ihre Dienstleistungen aber dennoch oft nicht datenschutzfreundlich ausgestalten. Immerhin erlaube aber bspw. Apple Pay Transaktionen anonym zu tätigen. Namentlich mache Apple geltend, dass die relevanten Personendaten nicht gespeichert werden und damit auch keine Datenanalysen durchgeführt werden. Damit stellt sich nach Thouvenin die Frage, ob die Entwicklung in diese Richtung gehen werde oder ob es sich letztlich nur um leere Versprechungen handle? Eberle sieht das Problem dabei darin, dass Apple die Daten zwar nicht speichere, diese aber natürlich über das Internet laufen und damit von Dritten abgefangen und ausgewertet werden könnten. Auch Bitcoin Transaktionen sind nicht anonym sondern pseudonym, bemerkt Meisser. Somit lassen sich zwar die Nummernkonten nachverfolgen, die Personen, die dahinter stehen sind in der Regel aber immerhin nicht leicht identifizierbar.

4 Rechtliche Fragestellungen webbasierter und mobiler Zahlungssysteme

4.1 Rechtsfragen bei virtuellen Währungen

[Rz 23] Prof. Dr. Seraina Grünewald, Assistenzprofessorin für Finanzmarktrecht an der Universität Zürich, setzte den Schwerpunkt ihrer Ausführungen auf das Finanzmarktaufsichtsrecht im

[6] Die Sandbox steht für Besonderheiten der Laufzeitumgebung einer Software oder der lokalen Arbeitskopie eines in einem Versionskontrollsystem abgelegten Software-Moduls. Die Software wird vom Rest des Systems in beide Richtungen abgeschirmt, quasi in den Sandkasten gesetzt, in dem sie einerseits keinen Schaden anrichten kann und andererseits gegenüber Einflüssen von ausserhalb der Sandbox geschützt ist.

[7] Unter Repackaging wird das Dekompilieren, Modifizieren und erneutes Kompilieren eines Apps verstanden.

Zusammenhang mit virtueller Währung.

[Rz 24] Grünewald definiert zunächst zwei Unterscheidungskriterien virtueller Währungen: offene/geschlossene und zentralisierte/dezentralisierte Währungssysteme. Offene Modelle erlauben den Umtausch in eine offizielle Währung. Geschlossene Systeme hingegen basieren auf einer Art Gutscheingedanken, indem die virtuelle Währung nur innerhalb eines Systems (z.B. Amazon Coins) genutzt werden kann. Zentralisierte und dezentralisierte virtuelle Währungssysteme unterscheiden sich dadurch, ob sie zentral von einer Art Überwachungsstelle kontrolliert werden oder nicht. Da Kryptowährungen auf offenen, dezentralisierten Systemen beruhen, fehlen in diesen Modellen Ansprechpersonen und Durchsetzungsmöglichkeiten. Entsprechend gehen von ihnen die grössten rechtlichen Risiken aus.

[Rz 25] Nach dieser kurzen Einführung nimmt Grünewald eine währungsrechtliche Einordnung von virtuellen Währungen vor. Auch sie kommt zum Schluss, dass die Schaffung virtueller Währungssysteme grundsätzlich zulässig ist. Hingegen sei es problematisch, virtuelle Währung rechtlich als Fremdwährung zu qualifizieren.

[Rz 26] Im Finanzmarktaufsichtsrecht stellt sich die Frage, ob und unter welchem Titel die Verwendung virtueller Währung einer Bewilligung durch die FINMA bedarf. In Betracht fällt eine Bewilligung nach BankG und/oder GwG. Das BEHG kann hier keine Anwendung finden, weil virtuelle Währungen nicht als Effekten zu behandeln sind. Grundsätzlich gilt, dass einer Bewilligungspflicht nach Art. 3 ff. BankG und Art. 4 ff. BankV untersteht, wer Gelder von Dritten gewerbsmässig entgegennimmt. Im Gegensatz dazu erfordert die schlichte Nutzung virtueller Währungen zum Kauf von Produkten oder Dienstleistungen keine Bewilligung. Wird aber eine virtuelle Währung eingesetzt, um herkömmliche Währung zu kaufen (und umgekehrt), wird der Händler möglicherweise bewilligungspflichtig. Geschieht dies aber Zug-um-Zug, ist eine solche Transaktion nicht als Einlage, sondern als reines Geldwechselgeschäft zu qualifizieren. Nimmt hingegen der Händler Guthaben für ein künftiges Wechselgeschäft entgegen, so können Einlagen im Sinne des BankG vorliegen. Betrachtet man die (Online-)Handelsplattformen, dann ist das reine Zusammenführen (Matching) von Käufern und Verkäufern virtueller Währungen nicht bewilligungspflichtig. Nimmt der Plattformbetreiber jedoch virtuelle oder offizielle Währung dauernd entgegen und können die Nutzer dieses Geld auf der Plattform beliebig einsetzen, wird der Plattformbetreiber bewilligungspflichtig.

[Rz 27] Für das Geldwäschereigesetz gilt, dass Geschäftsmodelle, die einer Bankenbewilligung bedürfen, auch dem GwG unterstellt sind. Die reine Nutzung virtueller Währungen als Zahlungsmittel ist in jedem Fall unproblematisch, weil sie nicht als Finanzintermediation zu qualifizieren ist. Der Kauf und Verkauf von virtueller Währung gegen offizielle Währung kann verschiedene Formen annehmen. Es kann ein berufsmässiger Geldwechsel (Zweiparteienverhältnis) oder ein Geldübertragungsgeschäft (Mehrparteiengeschäft) vorliegen. Bietet man Handelsplattformen für virtuelle Währungen an, so ist ein reines Matching nicht unterstellungspflichtig. Handelt es sich aber um einen Plattformbetreiber, der auch die Zahlungsprozesse abwickelt, so fallen solche Transaktionen unter das GwG und sind bewilligungspflichtig. Ist die Nutzung von virtueller Währung dem GwG unterstellt, besteht die Möglichkeit, sich einer Selbstregulierungsorganisation (SRO) anzuschliessen oder eine Bewilligung als direkt unterstellter Finanzintermediär (DUFI) zu erhalten. Fällt ein mit virtueller Währung verbundenes Geschäftsmodell unter die Bewilligungspflicht, bestehen Schwierigkeiten bezüglich der Sorgfaltspflichten und der Pflichten bei Geldwäschereiverdacht nach Art. 3 ff. GwG. Entsprechend schwierig gestalten sich namentlich die Identifikation der Vertragspartei und die Feststellung der wirtschaftlich Berechtigten. Die

Verwendung von virtueller Währung kann zudem unter den Geldwäschereitatbestand nach Art. 305bis des Strafgesetzbuches (StGB) fallen.

[Rz 28] Grünewald kommt in ihrem Vortrag zum Schluss, dass sich bei der Nutzung von virtueller Währung vor allem die Rechtsdurchsetzung als problematisch herausstellt. Aus ihrer Sicht ist das materielle Recht weniger das Problem.

4.2 E-Banking 2.0: Regulierung und Marktzutritt von Drittanbietern von Zahlungsdienstleistungen heute und morgen

[Rz 29] Prof. Dr. Hans Rudolf Trüeb, Rechtsanwalt in Zürich und Titularprofessor an der Universität Zürich, referierte zu Fragen über die Regulierung und den Marktzutritt von Drittanbietern.

[Rz 30] Im E-Banking Business stehen verschiedene Interessen im Fokus. Kunden möchten ihren Online-Einkauf oder Zahlungen einfach und rasch erledigen. Dritte Anbieter von Zahlungsdienstleistungen (TPPs) befriedigen dieses Kundenbedürfnis mit ihren Angeboten. Dazu brauchen solche Anbieter den Zugang zu den Bankschnittstellen. Diesem Interesse stehen jedoch legitime Interessen der Banken gegenüber. So haben sie die Pflicht ihre Kunden und deren Daten zu schützen. Ferner müssen sie die Compliance mit den regulatorischen Anforderungen sicherstellen und eine faire Zuordnung von Rechten, Pflichten und Risiken erreichen. Wird Drittanbietern der Zugang zu diesen Schnittstellen ermöglicht, entstehen Gefahren. Werden z.B. die höchstpersönlichen Legitimationsmittel mit diesen Dritten geteilt (z.B. würden die Credentials übertragen), kommt es zu einer sog. Impersonation[8]. Dadurch wird die Zuordnung der Verantwortung bei Fehlkontakten in solchen Zahlungssystemen erschwert. Heute übernehmen z.T. die Banken die Schäden, welche aus Phishing-Aktionen wegen der Überlassung des Zugangs entstehen, solange die Kunden ihre Sorgfaltspflichten beachten. Die Sorgfaltspflicht der Banken wiederum bedingt, dass Kunden aufzuklären, Transaktionen zu überwachen sind und in der Regel die Sicherheit der IT-Systeme sicherzustellen ist. Ist ein TPP involviert, stellt sich die Frage, inwieweit die Bank noch Kontrolle über diese Prozesse hat.

[Rz 31] Der aktuelle Rechtsrahmen der EU für TPPs präsentiert sich wie folgt: Gemäss der Verordnung EU Nr. 260/2012 erfolgen Zahlungen innerhalb der EU nach den Standards der SEPA (Single European Payment Area). Die SEPA dient der Vereinheitlichung von bargeldlosen Zahlungen. 150 Schweizer Institute sind diesem System angeschlossen. Das Angebot von webbasierten und mobilen Zahlungssystemen unterliegt der PSD (Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt [Zahlungsdienste-Richtlinie]). Die PSD regelt das Bank-zu-Kunden-Verhältnis und dient dem Wettbewerbs- und Konsumentenschutz. Dadurch werden grenzüberschreitende Zahlungen ermöglicht und der Marktzutritt und die Transparenz gewährleistet. Unter diese Richtlinie fallen auch sog. Zahlungsinstitute, wie z.B. PayPal, also Zahlungsdienstleister, die keine Einlagen entgegennehmen und damit keine Bankenfunktion haben (sog. Enabler). Die novellierte PSD (PSD-2) wird überdies Anforderungen an Zahlungsauslöse- und Kontoinformationsdienste enthalten. Diese werden künftig auch der sog. NIS Richtlinie (Richtlinie des Europäischen Parlaments und des Rates über die Massnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und In-

[8] Hierunter wird die Imitation eines Nutzers zu eigenen Vorteilen bei Missbrauch seiner Credentials durch eine Drittperson verstanden.

formtionssicherheit in der Union [«Cybersecurity-RL»]) unterliegen.

[Rz 32] Es stellt sich die Frage, welche Auswirkungen die PSD-2 bei in Kraft treten auf die Schweiz hätte. Eine fortgesetzte SEPA Teilnahme bedingt u.a. verbindliche und äquivalente nationale Anforderungen an TPPs. So wäre die Teilnahme an der SEPA wohl gefährdet, wenn die Schweiz in Sachen Regulierung von Drittanbietern untätig bleibt. Die SEPA Rulebooks verlangen, dass Titel III und IV der PSD im Schweizer Recht oder in der verbindlichen Rechtspraxis reflektiert werden müssen («effectively represented in law or in substantially equivalent binding practice»). Die EU-rechtliche TPP-Regelung wurde neu in Title IV der PSD-2 eingefügt. Die EZB hat Empfehlungen für die Behandlung von TPPs abgegeben, welche dieses Jahr noch in Kraft treten sollen, in denen verlangt wird, dass TPPs die gleichen Sicherheits- und Kontrollmassnahmen wie Banken in ihren Systemen implementieren müssen. Weiter empfiehlt die EZB, dass Drittanbieter einen hohen Grad an Transparenz gewährleisten. Darüber hinaus sollen keine Credentials zwischen der Bank und den TPPs ausgetauscht werden, und die Dauer des Kontozugangs über das Internet oder Mobiltelefon soll auf ein Minimum reduziert werden.

[Rz 33] Abschliessend ging Trüeb der Frage nach, was die Schweiz nun tun kann? Eine Möglichkeit besteht aus seiner Sicht in einer vertraglichen Zugangsregelung zu den Schnittstellen der Banken. Entsprechend müssten Banken jedoch gewisse Schutzvorkehrungen treffen, um ihrer Sorgfaltspflicht nachzukommen. Die zweite Möglichkeit läge darin, dass Banken ihr Schnittstellenangebot für TPP schliessen würden. Dieses Szenario scheint jedoch unwahrscheinlich. Besser wäre eine vernünftige Regulierung mit Augenmass im künftigen Finanzinstitutsgesetz (FINIG).

4.3 Rechtliche Anforderungen an System- und Datensicherheit und Compliance für webbasierte und mobile Zahlungen

[Rz 34] Dr. Martin Hess, Rechtsanwalt in Zürich, befasste sich in seinem Vortrag mit der Compliance der Anbieter von webbasierten und mobilen Zahlungssystemen.

[Rz 35] Bis anhin waren die am Zahlungsverkehr beteiligten Parteien auf wenige Kategorien beschränkt: die Schweizerische Nationalbank und die Banken (des Zahlers und des Empfängers) sowie die Post. Die Realität gestaltet sich heute etwas anders. So besteht der Zahlungsverkehrsmarkt (auch grenzüberschreitend) aus diversen Marktakteuren: Banken, Nationalbank, Postfinance, Kartenherausgeber, Emittenten von E-Geld und virtuellen Währungen und TPPs. Sie alle agieren in einem regulatorischen Umfeld. Dabei ist oft unklar, welche Regeln auf welche Akteure anwendbar sind.

[Rz 36] Hess beleuchtet in seiner Präsentation die Regelung der Geheimhaltungspflichten der Finanzinstitute, welche sich in drei Gruppen unterteilen lassen: Persönlichkeitsschutz, Auftrags-/Verwaltungsrecht, wie zum Beispiel die Treuepflicht des Arbeitnehmers (Art. 398 des Obligationenrechts [OR]) oder das Gewährserfordernis (Art. 3 BankG, Art. 10 BEHG), und Verwaltungsstrafrecht. Auch er qualifiziert die Drittanbieter als Finanzintermediäre nach GwG. So steht ihnen der Entscheid frei, ob sie sich einer Selbstregulierungsorganisation anschliessen oder einer Aufsicht der FINMA unterstellen. Das FINMA-Rundschreiben 2008/7 regelt die Auslagerung von gewissen Aufgaben/Dienstleistungen von einem regulierten Finanzdienstleister an eine andere Unternehmung. Das Finanzinstitut bleibt jedoch gegenüber der FINMA weiterhin verantwortlich für den ausgelagerten Geschäftsbereich.

[Rz 37] Nach dem Fernmeldegesetz besteht das Fernmeldegeheimnis für alle mit fernmelde-

dienstlichen Aufgaben betrauten Personen/Unternehmen. Die Compliance von Fernmeldeanbietern erstreckt sich auf die Informationspflicht über Abhör- und Eingriffsrisiken der Betroffenen und auf die Pflicht zur Bereitstellung oder Nennung geeigneter Hilfsmittel zur Beseitigung dieser Risiken. Für reine Internetanbieter bestehen keine spezialgesetzlichen Regelungen.

[Rz 38] Im Hinblick auf die Compliance eines Anbieters von webbasierten oder mobilen Zahlungsdiensten mit dem Datenschutzgesetz (DSG) ist vor allem die Einhaltung der in Art. 4 DSG genannten Datenschutzgrundprinzipien von Bedeutung: Rechtmässigkeit der Datenbearbeitung, Bearbeitung nach Treu und Glauben, Zweckbindungs-, Verhältnismässigkeits- und Erkennbarkeitsprinzip. Darüber hinaus verankert Art. 6 DSG strikte Voraussetzungen für den Datenaustausch mit Drittstaaten. So muss eine Bearbeitung der ins Ausland transferierten Personendaten den gleichen Datenschutzstandards wie in der Schweiz unterliegen. Hierzu hat der EDÖB eine Art Mustervertrag das «Swiss Transborder Data Flow Agreement» für grenzüberschreitendes Outsourcing veröffentlicht. Die Bekanntgabe von Kundendaten an Dritte ist zudem nur erlaubt, wenn vorher die Einwilligung des Betroffenen eingeholt wurde[9]. Aus technischer Sicht ist Art. 7 DSG, welcher die Datensicherheit gewährleistet, für die Compliance von grosser Bedeutung. So legt dieser Artikel fest, dass alle Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Dies setzt die Vertraulichkeit, Verfügbarkeit und Richtigkeit der Daten (Art. 5 DSG) des Betroffenen voraus[10].

[Rz 39] Für die Anforderungen hinsichtlich Compliance von Anbietern webbasierter und mobiler Zahlungssysteme bestehen bereits zahlreiche Regulierungen oder Empfehlungen, die als Soft Law verbindlich sind, wie z.B. das FINMA-Rundschreiben 2008/21: Operationelle Risiken Banken, Anhang 3, die ECB-Recommendations for the security of internet payments oder die Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten. Zusammenfassend kann für diese Vorgaben festgehalten werden, dass eine Security Policy erstellt werden muss, die ein Rahmenkonzept, die Prozesse und die dauernde Anpassung an neue Entwicklungen festlegt. Ferner wird verlangt, dass eine Risikoeinschätzung, -kontrolle und -minderung vorgenommen wird, sensitive Daten angemessen geschützt werden, das System stetig kontrolliert wird (Fraud Detection, Blockierung und Traceability), Limiten hinsichtlich Transaktionen, Maximalumsatz und geografischer Anwendung gesetzt werden, eine Disaster Recovery Vorsorge (bspw. Backup-Systeme) vorgesehen ist und Kunden informiert werden (Bewusstseinsschaffung für Risiken).

[Rz 40] Hess schliesst seinen Vortrag mit der Feststellung, dass heute in der Schweiz Rechtsunsicherheit besteht hinsichtlich die anwendbaren Regeln für Anbieter webbasierter und mobiler Zahlungsdienste. Neue Zahlungssysteme müssen reguliert (es bieten sich Art. 81 f. des Finanzmarktinfrastrukturgesetzes [FinfraG] an als gesetzliche Grundlage) und Verantwortlichkeiten definiert werden, um mehr Rechtssicherheit zu garantieren. An oberster Stelle sollte die Schaffung von Vertrauen in ein solches System stehen, denn nur dann können sich diese neuen Zahlungsmodelle durchsetzen.

9 Sofern auch kein anderer Rechtfertigungsgrund nach Art. 13 DSG vorliegt.

10 Die Mindestanforderungen für die Datensicherheit sind in Art. 8—12 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) aufgelistet.

5 Schlussdiskussion

[Rz 41] Die Tagung endete mit einer Podiums- und Plenumsdiskussion, an dem die drei Referenten des zweiten Teils und die beiden Gäste Claudia Keller und Nicole Beranek Zanon teilnahmen. Rolf H. Weber moderierte das zweite Plenum.

[Rz 42] Keller stellte die These auf, dass die ganze Problematik letztlich auf die Frage zurückgeführt werden kann, ob diese neuen Zahlungsmodelle reguliert werden sollen. Aus den Referaten ging aus ihrer Sicht klar hervor, dass gesetzlicher Handlungsbedarf besteht, die Umsetzung aber Zeit beanspruchen wird. In der Zwischenzeit kann diese Regulierungslücke mit vertraglichen Abmachungen geschlossen werden. In diesem Zusammenhang ist jedoch klar, dass Banken ihre Schnittstellen nicht wegbrechen lassen und Drittanbieter nicht gleich viel Verantwortung wie die Banken übernehmen wollen.

[Rz 43] Ausgehend von dieser These, stellt sich die Frage, ob es möglich wäre, die bestehenden Risiken auf die Nutzer zu überwälzen (Stichwort: Eigenverantwortung). Aus Sicht von Beranek Zanon wäre ein solches Vorgehen aber aus Reputationsüberlegungen nicht dienlich. Wichtiger wäre vielmehr, vermehrt vertragliche Abmachungen zwischen den Banken und den Drittanbietern zu schliessen, um die Verantwortlichkeiten zwischen Nutzer, Drittanbieter und Bank klar zu regeln. Eine allfällige Regulierung der Drittanbieter darf keine Markteintrittshürde werden und muss ausserdem allen Marktteilnehmern gleiche Möglichkeiten bieten. Es gilt also eine Abwägung zwischen den sich gegenüberstehenden Interessen vorzunehmen. Darüber hinaus sollten Banken in Zukunft selber Dienstleistungen, welche TPPs bereits heute anbieten, in ihr Angebot integrieren. Gemäss Trüeb ist es notwendig, Regelungen zu schaffen, weil nur so die Rechtssicherheit für alle Teilnehmer (Bank, Drittanbieter, Nutzer) erhöht werden kann. Eine solche Regelung muss allen Interessen Rechnung tragen und entsprechend verhältnismässig ausgestaltet werden. Basierend auf klaren rechtlichen Grundlagen können Unternehmen eine Best Practice in diesem Bereich entwickeln und ihren Sorgfaltspflichten nachkommen.

[Rz 44] Weber fügt an, dass vor allem das Äquivalenzerfordernis gemäss EU Recht ein grosses Problem darstellt. So stellt er die Frage, wie die Schweiz darauf reagieren soll. Gemäss Hess ist es eine Frage des Bewusstseins innerhalb der Legislative, welche mit der juristischen Analyse von webbasierten und mobilen Zahlungssystemen noch gar nicht begonnen hat. Trüeb schlägt deshalb einen Diskurs zwischen den Anbietern von webbasierten und mobilen Zahlungssystemen und der Bankenvereinigung vor. So könnte bspw. ein gemeinsames Gremium gebildet werden, das sich für die Regulierung dieses Bereichs einsetzen würde, damit das geltende Recht nicht weiterhin neuen Zahlungsmodellen hinterherhinkt.

Rehana Harasgama, M.A. HSG, studierte an der Universität St.Gallen (HSG) Rechtswissenschaften und schloss ihren Master 2013 ab. Seither ist sie an der Forschungsstelle für Informationsrecht der Universität St.Gallen (FIR-HSG) als Doktorandin tätig. Sie verfasst ihre Dissertation im Rahmen des SNF-Projekts «Remembering and Forgetting in the Digital Age» bei Prof. Dr. Peter Hettich und Prof. Dr. Florent Thouvenin. Dabei beschäftigt sie sich intensiv mit dem Schnittpunkt der drei Themenbereiche Datenschutz, staatlicher Informationsanspruch und Archivierungsrecht. Seit Januar 2014 ist sie Mitglied des Herausgeberteams der Schriftenreihe der Assistierenden der Universität St.Gallen und Vorstandsmitglied des Doktorandenvereins DocNet der Universität St. Gallen.