M2M-Payments – wie „unsichtbar“ dürfen Zahlungen sein?

Von Udo Steger

Es ist nur eine Frage der Zeit, bis Plattform-Anbieter rechtskonforme M2M-Transaktionen werden anbieten können, sagt Udo Steger. Eine Reihe von rechtlichen Herausforderungen können heute schon mit geltendem Recht abgebildet werden. Als Beispiel nennt er das Erfordernis einer natürlichen oder juristischen Person, das sich durch Definition von Signaturen oder Zertifikaten als Blankoerklärung lösen ließe. In diesem Modell wäre aufgrund der damit verbundenen Verschlüsselung wohl auch keine starke Kundenauthentifizierung erforderlich. Aus datenschutzrechtlicher Sicht bewertet Steger indessen die Verzögerung bei der E-Privacy-Verordnung als Hemmschuh für EU-interne, grenzübergreifende M2M-Zahlungen. Red.

Die Entwicklung des Internet of Things (IoT) schreitet immer weiter voran. Die Anzahl von Geräten, die miteinander Daten austauschen können und die im Folgenden kurz als „Maschinen“ bezeichnet werden, steigt massiv an. Die Machine-to-Machine (M2M) Kommunikation verspricht, Prozesse zu beschleunigen oder zu ermöglichen und dabei Kosten einzusparen. Zwar ist M2M-Kommunikation nichts grundlegend Neues, denn schon bisher kommunizieren in jedem (Unternehmens-)Netzwerk die dort eingebuchten Maschinen miteinander. Im IoT-Kontext bedeutet M2M-Kommunikation jedoch, dass die Kommunikation über private Netze, öffentliche Netze wie das Internet, ein Mobilfunknetz oder mittels Kurzstreckenverfahren wie NFC erfolgt, wobei mehrere Verfahren hintereinander geschaltet sein können. Die Kommunikation kann ad-hoc erfolgen und ohne vorherige Kopplung durch manuellen Eingriff. Eine Maschine kann so mit einer potenziell unbegrenzten Anzahl von anderen Maschinen kommunizieren.

Für solche Maschinen ist es höchst interessant, Zahlungen von Beträgen aller Art vornehmen zu können, bei denen die Sicherheit gewahrt bleibt, den rechtlichen Anforderungen Genüge getan wird und möglichst geringfügige Transaktionskosten anfallen. M2M-Zahlungen müssen aber nicht notwendigerweise unter völliger Abwesenheit von Menschen ablaufen. Ein Auto, welches den geladenen Strom selbstständig mit dem Anbieter abrechnet oder bei einer Mautstelle zügiges Weiterfahren ermöglicht, stellt dem Fahrer Komfortmerkmale zur Verfügung, die dieser sicher zu schätzen weiß.

Rechtskonformität nur eine Frage der Zeit

Etablierte Kreditkartenunternehmen, Banken und Zahlungsdienstleister, die sich dem Thema M2M-Zahlungen widmen, haben dabei Herausforderer unter anderem in Fintechs, die M2M-Zahlungen mit alternativen Transaktionsmodellen realisieren wollen, insbesondere mittels der Blockchain-Technologie. Gleichzeitig tut sich ein neuer Markt für neue, aber auch etablierte Plattformen wie zum Beispiel Amazon auf, die Anbieter und Nachfrager zusammenbringen und die Zahlungen möglicherweise selber abwickeln könnten.

Erste kleine Schritte in die M2M-Welt wie zum Beispiel der „Dash“ Button von Amazon sind zwar von der Rechtsprechung unter anderem wegen Verstößen gegen den Verbraucherschutz für rechtswidrig[1)] erklärt worden, aber es dürfte nur eine Frage der Zeit sein, bis die Anbieter ihre Plattformen rechtskonform gestaltet haben werden.

Viele rechtliche Implikationen

Eine zu M2M-Zahlungen befähigte Maschine ist in der Lage, in erheblichem

Udo Steger, Annerton Rechtsanwaltsgesellschaft mbH, München

Umfang rechtlich relevante Abläufe auszulösen oder diese zu beeinflussen. Ein Beispiel: Angenommen, bei einer Maschine geht ein von ihr überwachter Materialvorrat zu Neige. Sie könnte dann mittels M2M-Kommunikation bei einem geeigneten Lieferanten eine Bestellung auslösen. Dabei soll sie unter mehreren im Wettbewerb stehenden Anbietern den am besten geeigneten Lieferanten ermitteln. Dieser würde freilich nur liefern, wenn (a) das Rechtsgeschäft wirksam ist und jemandem als Haftungssubjekt rechtssicher zugeordnet werden kann, (b) der Inhalt der Bestellung genuin, vollständig und richtig ist, (c) alle für die Lieferung notwendigen Daten vorliegen und (d) eine hohe Sicherheit besteht, bezahlt zu werden, bei Bestellungen von bisher Unbekannten idealerweise sofort und unwiderruflich.

Im Folgenden sollen daher jeweils zivilrechtliche (Ziff. 3), datenschutzrechtliche (Ziff. 4) und aufsichtsrechtliche (Ziff. 5) Aspekte beschrieben werden, die für M2M-Zahlungen relevant sind. Diese stellen sich dem Grunde nach sowohl bei den etablierten Zahlungsverfahren als auch bei Blockchain-basierten Verfahren.[2)]

Abstraktionprinzip im Zivilrecht

Eine Zahlung ist rechtlich betrachtet ein Verfügungsgeschäft über Geld. Die Zahlung „erfüllt" eine Geldschuld. Die Geldschuld kann privat oder hoheitlich veranlasst sein, zum Beispiel durch einen zuvor abgeschlossenen Kaufvertrag, sie kann aber auch aus einem Pflichtverstoß oder einem Delikt begründen, etwa in Form eines Schadensersatzes. Im hoheitlichen Bereich können etwa Gebühren für Leistungen einer öffentlichen Einrichtung verlangt werden oder Bußgelder wegen eines Verstoßes gegen Ordnungsvorschriften.

Das sogenannte „Abstraktionsprinzip" ist ein Grundprinzip des deutschen Zivilrechts. Danach unterscheidet man das Verpflichtungsgeschäft und das oder die Verfügungsgeschäft(e). Somit hat die Gültigkeit oder Ungültigkeit des einen Geschäfts nicht notwendigerweise die Gültigkeit oder Ungültigkeit des anderen Geschäfts zur Folge.

Das Verpflichtungsgeschäft verpflichtet beide Parteien, etwas zu bewirken, eben das Verfügungsgeschäft vorzunehmen und zu „verfügen". Plastisch wird das am Beispiel des Erwerbs von Brötchen beim Bäcker. Dabei werden (mindestens) drei Rechtsverhältnisse begründet: 1. der Kaufvertrag über Brötchen als Verpflichtungsgeschäft, 2. die Übergabe der Brötchen und das Verschaffen des Eigentums daran als Verfügungsgeschäft des Bäckers sowie 3. die Zahlung des Preises als Verfügungsgeschäft des Kunden. Das Verfügungsgeschäft muss dabei nicht unmittelbar gegenüber der anderen Partei erbracht werden, so wird sich zum Beispiel der Käufer bei Kartenzahlung eines Dritten, seiner Bank, bedienen, der er über das PoS-Terminal des Bäckers eine Weisung zur Auszahlung an einen weiteren Dritten, den Zahlungsdienstleister des Bäckers, erteilt.

Maschinen können keine Personen sein

Sowohl bei einem Verpflichtungs- als auch beim Verfügungsgeschäft handelt stets eine natürliche oder juristische Person[3)] beziehungsweise wird verpflichtet – denn nur eine solche Person kann Träger von Rechten und Pflichten sein. Sie kann sich Vertreter, Angestellter oder Dienstleister bedienen, aber letztlich ordnet die Rechtsordnung dieser Person eine bestimmte Pflicht zu, oder das Eigentum an einer Sache.

Angesichts großer Fortschritte bei der Künstlichen Intelligenz (KI) und der Erstellung von autonomen Softwareagenten ist es aus heutiger Sicht zwar nur eine Frage der Zeit, wann es soweit ist, dass eine in Maschinen beziehungsweise Software enthaltene algorithmische Intelligenz einen maturierten Grad erreicht hat, mit dem gesellschaftlich Rechtszuweisungen als notwendig erscheinen. Die Zuweisung staatsbürgerschaftlicher Rechte an die „Computerfrau Sophia" durch den Staat Saudi-Arabien[4)] bleibt jedoch eher ein PR-Gag als ein rechtliches Phänomen.

Zumindest im Moment ist es in unserer Rechtsordnung daher nicht vorgesehen, dass eine Maschine selbst als „Person" Träger von Rechten und Pflichten wird. Die Maschine und das, was die Maschine bewirkt, bleibt stets einer natürlichen oder juristischen Person zugeordnet.

Bis auf Weiteres wird es bei M2M-Transaktionen und damit auch M2M-Zahlungen zwei grundlegende Probleme geben: Es fehlt Maschinen an einer eigenen Rechtspersönlichkeit und es fehlt ihnen an einer damit einhergehenden Haftung und an Regelungen zur Authentifizierung. Ohne diese können Maschinen keine Willenserklärungen abgeben, nicht Partei eines Vertrags sein, kein Eigentum halten und somit auch nicht Zahler sein. Daher wird man vorerst eine natürliche oder juristische Person brauchen, für die die Maschine die M2M-Transaktion veranlasst oder abwickelt.

Für eine M2M-Anwendung wäre es vorteilhaft, wenn die Maschine dergestalt in die Anbahnung und Abwicklung eines mittels M2M angebahnten Geschäfts einbezogen werden kann, dass rechtlich zwar eine Zuordnung zu einer natürlichen oder juristischen Person bestehen bleibt, im Übrigen aber die Maschine „autonom" zu handeln scheint. Dazu müsste eine rechtssichere Zurechnung von durch Maschinen veranlassten Vertragsschlüssen zu einer natürlichen oder juristischen Person erfolgen.

Man könnte eine Maschine etwa als Boten sehen. Ein Bote ist bloßer Übermittler einer Willenserklärung und muss weder rechts- noch geschäftsfähig oder menschlich sein. Jedoch geht bei M2M-Transaktionen wie im obigen Beispiel (Ziff. 2) der Einfluss der Maschine weit über eine bloße Boteneigenschaft hinaus, sie bestimmt beispielsweise die Menge und wählt den Lieferanten. Einem Stellvertreter wäre ein solches Handeln grundsätzlich möglich, jedoch muss ein Stellvertreter eine Rechtspersönlichkeit besitzen, was zurzeit für Maschinen nicht der Fall ist.[5)]

„Halter" einer Maschine und Blankoerklärung

Pragmatisch ist ein Ansatz, der die Erklärung der Maschine unter Vertrauensgesichtspunkten und nach dem objektiven Empfängerhorizont stets demjenigen zuordnet, der die Maschine „betreibt". In diesem Zusammenhang stellt sich die Frage nach der Schaffung rechtsverbindlicher Maschinenidentitäten, also von Mechanismen, die eine Maschine eindeutig identifizieren (siehe Ziff. 7.7) und somit einer Person zuordnen. Es müsste Voraussetzung für eine M2M-Transaktion und insbesondere eine M2M-Zahlung sein, dass eine natürliche oder juristische Person die Ver-

antwortung für die Maschine übernimmt. Dies könnte erfolgen, indem etwa ein Zertifikat oder eine digitale Signatur der Person quasi als „Blankoerklärung" in der Maschine hinterlegt wird. Die Maschine kann dann damit kenntlich machen, für wen sie das Geschäft abschließt.

Dabei könnte sogar dahingestellt bleiben, ob der Vertragspartner erkannt hat, dass er es mit einer Maschine zu tun hat. Entscheidend ist vielmehr, dass der „Halter" mittels Zertifikat beziehungsweise der Signatur in der Maschine einen Vertrauenstatbestand geschaffen hat, wonach er sich die maschinell erzeugte Erklärung zurechnen lassen will (objektiver Empfängerhorizont).

Umgekehrt gilt Gleiches: Bedient sich der andere Vertragspartner einer Maschine, muss er sich zurechnen lassen, was „seine" Maschine mit der anderen Maschine vereinbart hat. Zwar ist der menschliche Einfluss auf die Erklärungen dabei sehr rudimentär. Allerdings erkennt unsere Rechtsordnung Blankoerklärungen als zulässig an – füllt der Empfänger eine Blankoerklärung aus, wird der so erstellte Inhalt dem Erklärenden zugerechnet.

Dieser nach heutigem Recht mögliche Ansatz ist prinzipiell sowohl für Verpflichtungsgeschäfte (zum Beispiel Abschluss eines Kaufvertrags) als auch für Erfüllungsgeschäfte, eben die M2M-Zahlung, geeignet.

Beim Datenschutz entscheidet der Personenbezug

Bei konventionellen Zahlungen mittels Karte ist der Zahler der „Betroffene", dessen Daten erhoben und verarbeitet werden. Zumindest die Akzeptanzstelle, ihr Zahlungsdienstleister sowie die Bank des Zahlers sind als „Verantwortliche" im Sinne der EU-Datenschutzgrundverordnung (DSGVO) anzusehen, denn sie verarbeiten die Daten des Zahlers und der Transaktion im eigenen Interesse und aufgrund von Rechtsgrundlagen, die teilweise nur ihnen zugänglich sind (zum Beispiel § 59 ZAG). Daher sind sie nicht etwa „gemeinsam Verantwortliche". Die Übermittlung der Daten des Zahlers zwischen den genannten Parteien ist regelmäßig durch den Zweck der Vertragserfüllung gerechtfertigt, Art. 6 Abs. 1 Satz 1 lit. b DSGVO, denn um die Zahlung zu bewirken, müssen personenbezogene Daten übermittelt werden. Weitere Rechtsgrundlagen für die Verarbeitung ergeben sich zum Beispiel aus dem ZAG, KWG oder GwG.

An M2M-Zahlungen sind zwar nur Maschinen beteiligt, sie sind deshalb aber nicht zwingend dem Datenschutzrecht entzogen. Die DSGVO schützt die Daten natürlicher Personen, nach Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten" jedoch auch solche Daten, die sich auf eine „identifizierbare natürliche Person" beziehen. Die Beziehbarkeit wird dabei objektiv bestimmt, das heißt, es kommt nicht darauf an, ob einer Partei den Personenbezug konkret herstellen kann, sondern vielmehr darauf, ob es objektiv irgendjemandem möglich wäre.

Datenschutzrechtlich wie Kartenzahlungen zu behandeln

Die „Personenbeziehbarkeit" der Daten einer Machine-to-Machine-Zahlung ist ohne Weiteres zu bejahen, wenn der „Halter" der Maschine eine natürliche Person ist, denn die bloße Tatsache der Zahlung ist eine Information über den Zahler. Auch wenn der „Halter" eine juristische Person ist, können personenbeziehbare Daten enthalten sein: Löst beispielsweise ein Dienstwagen entlang einer Mautstrecke M2M-Zahlungen aus und/oder an Ladestationen oder Drive-in-Schaltern, lässt dies Aussagen über Route und Geschwindigkeit des Fahrzeugs und seiner Insassen zu. Die Insassen mögen allen an der M2M-Zahlung Beteiligten unbekannt sein, aber der Zahler kennt regelmäßig die Identität des Fahrers oder der Insassen oder kann diese durch Zusammenführung mit anderen Daten ermitteln lassen, zum Beispiel Fahrtenbuch, Navigationssystem, Mobilfunkgespräche. M2M-Zahlungen sind daher aus datenschutzrechtlicher Sicht nicht anders zu behandeln als konventionelle Zahlungen mit Karte.

„Verantwortlicher" ist in Art. 4 Abs. 7 DSGVO, und „Auftragsverarbeiter" in Art. 4 Abs. 8 DSGVO definiert. Dort wird eindeutig auf eine natürliche oder juristische Person oder eine Organisation abgestellt. Zwar ist der Begriff „Verantwortlicher" weit zu verstehen (vergleiche DSGVO, Erw. Gründe 20, 22, 36, 48), aber selbst für den Begriff „Stelle" lässt sich der DSGVO entnehmen, dass es sich zumindest um einen eigenständig handelnden Teil einer rechtsfähigen Organisation handeln muss.

Regelungslücke bezüglich Sicherheit?

Da eine Maschine nach bisherigem Rechtsverständnis keine eigenständige Person oder Organisation ist, ist „Verantwortlicher" beziehungsweise „Auftragsverarbeiter" stets die Stelle, die die Maschine betreibt. Ist der „Halter" eine juristische Person, ist diese in Bezug auf personenbezogene Daten, die bei einem M2M-Payment im Zusammenhang mit der Zahlerrolle anfallen, als „Verantwortlicher" anzusehen, etwa weil der „Halter" beim oben genannten Beispiel die Daten des Fahrer des PKW kennt, weil es sich um einen Mitarbeiter handelt.

Bei M2M-Zahlungen könnte man eine Regelungslücke in der DSGVO sehen, wenn der Zahler, der sich der Maschine bedient, eine natürliche Person ist. Eine Partei, die als „Verantwortlicher" personenbezogene Daten verarbeitet, hat gemäß Art. 5 und 32 DSGVO für eine angemessene Sicherheit ihrer Systeme zu sorgen, etwa dem Lesegerät, mit dem die Maschine des Zahlers kommuniziert. Dies gilt aber nicht automatisch auch für den Betroffenen, denn Art. 5 und 32 DSGVO stellen eindeutig auf den „Verantwortlichen" ab, nicht auf den „Betroffenen". Dieser kann über seine eigenen Daten mehr oder weniger frei verfügen, zum Beispiel Einwilligungen in Datenverarbeitungen erklären, die anders nicht zulässig wären. Eine Pflicht zur Absicherung der Maschine des Zahlers wäre daher zumindest nach der DSGVO nicht gefordert.

Zivilrechtlich sieht dies regelmäßig anders aus. Zum muss ein Zahler auch ohne ausdrückliche Regelung stets die „im Verkehr erforderliche Sorgfalt" (§ 276 Abs. 2 BGB) anwenden, zum anderen kann die Bank einem Zahler der sich M2M-Zahlungen bedienen will, besondere Sorgfaltspflichten auferlegen.

Verzögerung der E-Privacy-Verordnung als Hemmschuh

Die E-Privacy-Verordnung soll zukünftig die Bereitstellung und Nutzung elek-

tronischer Kommunikationsdienste regeln. Ursprünglich sollte sie bereits 2018 gemeinsam mit der EU-Datenschutz-Grundverordnung (DSGVO) in Kraft treten. Nachdem ein Entwurf für die E-Privacy-Verordnung im November 2019 abgelehnt wurde, arbeitet die EU nun an einem neuen Vorschlag.

Bis die E-Privacy-Verordnung verabschiedet und anwendbar wird, regelt Art. 95 DSGVO das Verhältnis zwischen TK- und allgemeinem Datenschutz. Die DSGVO verweist dazu schlicht auf die EU-Richtlinie 2002/58/EG, die sogenannte „E-Privacy-Richtlinie", die verbindliche Mindestvorgaben für den Datenschutz in der Telekommunikation setzt und die nach einer Überarbeitung im Jahr 2009 auch als sogenannte „Cookie-Richtlinie" bekannt ist.

In der Praxis führt dies zu zahlreichen Problemen, weil in vielen Ländern eine über die Richtlinie hinausgehende Umsetzung im nationalen telekommunikationsrechtlichen Datenschutz erfolgte und auch der personelle Anwendungsbereich abweichend geregelt wurde. Insofern sind die Verzögerungen bei der E-Privacy-Verordnung ein Hemmschuh zumindest für EU-interne, grenzübergreifende M2M-Anwendungen und -Zahlungen.

M2M-Zahlung als Fernzahlungsvorgang?

Zahler ist gemäß § 1 Abs. 15 Zahlungsdiensteaufsichtsgesetz (ZAG) eine natürliche oder juristische Person, die Inhaber eines Zahlungskontos ist und die Ausführung eines Zahlungsauftrags von diesem Zahlungskonto gestattet oder, falls kein Zahlungskonto vorhanden ist, eine natürliche oder juristische Person, die den Zahlungsauftrag erteilt. Zahlungsempfänger ist gemäß § 1 Abs. 16 ZAG die natürliche oder juristische Person, die den Geldbetrag, der Gegenstand eines Zahlungsvorgangs ist, als Empfänger erhalten soll. Dabei ist es unerheblich, ob die Zahlung selbst von einer Maschine ausgelöst und von einer Maschine verbucht wird, jedenfalls so lange nicht, wie auf der Seite des Zahlers die Maschine lediglich Vorgaben des Zahlers umsetzt und die Maschine, bei der die Zahlung verbucht wird, wirtschaftlich dem Empfänger zuzurechnen ist. Bei dem hier vertretenen „Halter"-Ansatz wäre das jeweils gegeben, eine M2M-Zahlung ließe sich somit stets auch einem Zahler beziehungsweise Zahlungsempfänger zuordnen.

Man könnte allerdings überlegen, ob eine M2M-Zahlung als „Fernzahlungsvorgang" im Sinne des § 1 Abs. 19 ZAG zu qualifizieren ist. Ein „Fernzahlungsvorgang" wird über das Internet oder mittels eines Geräts ausgelöst, das für die Fernkommunikation verwendet werden kann. Dies hätte zur Folge, dass für M2M-Zahlungen eine sogenannte „starke Kundenauthentifizierung" (SCA) erforderlich ist, § 55 Abs. 2 ZAG. SCA soll die Sicherheit von Internetzahlungen erhöhen, weil diese in einer offenen technischen Infrastruktur erfolgen. Zudem sieht das Gesetz vor, dem Zahler stets Klarheit über den Betrag und den Zahlungsempfänger der von ihm gerade autorisierten Transaktion verschaffen.

Starke Kundenauthentifizierung nicht zwingend

Würde das vertretene „Haltermodell" mit Signaturen umgesetzt, würde der Begründung von SCA wohl weitgehend der Boden entzogen. Unterstellt, die Maschinen verwenden eine verschlüsselte Verbindung für die M2M-Kommunikation, wäre das Auslösen einer Zahlung unter Verwendung einer digitalen Signatur jedenfalls nicht weniger sicher als die Verwendung einer Karte vor Ort am PoS. Vielmehr kann bei M2M-Zahlungen mittels geeigneter Zertifikate/Signaturen eine Situation hergestellt werden, die der der vernetzten Geldautomaten und PoS-Terminals vergleichbar ist, deren Netzwerke besonders gesichert sind und die eben keine Fernzahlungsvorgänge darstellen.

Von daher ist zu hoffen, dass die Aufsichtsbehörden bei der Auslegung der Vorschrift die Absicherung einer Maschine entsprechend berücksichtigen.

Geldwäscherechtliche Pflichten für Zahlungsempfänger

Das Geldwäschegesetz (GWG) definiert in § 2 „Verpflichtete" als Parteien, bei denen Zahlungen unmittelbar ausgelöst oder Finanztätigkeiten erbracht werden. Die Definition erfasst natürliche oder juristische Personen sowie bestimmte Behörden oder Körperschaften und Anstalten öffentlichen Rechts. Maschinen sind somit nicht unmittelbar vom GwG umfasst. Sie sind auch keine „Agenten" im Sinne von § 2 Abs. 1 Nr. 4 GWG in Verbindung mit § 1 Abs. 9 ZAG.

Solange Maschinen aufsichtsrechtlich nicht als eigene Rechtssubjekte erfasst werden, kommt allenfalls eine Zurechnung des Handelns der Geräte zu dem jeweiligen Eigentümer in Betracht. Voraussetzung wäre dann, dass es sich bei den Betreibern der Geräte, also den „Haltern (Ziff. 0) um Verpflichtete im Sinne des § 2 GWG handelt. Das könnte gemäß § 2 Abs. 1 Nr. 16 etwa bei sogenannten „Güterhändlern" der Fall sein. Dies könnte auf das Beispiel in Ziff. 2 zutreffen, aber es gilt nichts anderes, wenn das gehandelte Gut etwa Strom wäre. Auch der Handel mit Strom wird als geldwäscherechtlich relevanter Güterhandel erfasst.

Das GWG hat unter anderem das Ziel, das Einschleusen von aus Straftaten stammenden Vermögenswerten in den Finanzkreislauf zu verhindern, jedenfalls aber einen Anknüpfungspunkt für Ermittlungen zur Aufdeckung der Straftat zu liefern. Aus dem Zurverfügungstellen von Zahlungsempfangsstellen – in Form zum Beispiel von Maschinen, die M2M-Transaktionen und M2M-Zahlungen akzeptieren – resultiert die Gefahr, dass derartige Vermögenswerte von dem Zahlenden in den Finanzkreislauf eingeschleust werden. Jedenfalls der Zahlungsempfänger wird daher bei über M2M angebahnten Geschäften im Rahmen des Verkaufsprozesses die geldwäscherechtlichen Pflichten zu berücksichtigen haben.

Unter dem Strich lässt sich festhalten: M2M-Zahlungen stehen vor vielen Herausforderungen, aber erstaunlich viele Aspekte können schon heute mit dem geltenden Recht abgebildet werden.

Fußnoten
1) OLG München, Urt. vom 10.01.2019, Az. 29 U 1091/18.
2) Dazu: Keding, „Die aufsichtsrechtliche Behandlung von Machine-to-Machine-Zahlungen unter Rückgriff auf Peer-to-Peer-Netzwerke", in: WM 2018, S. 64ff.
3) Der sprachlichen Einfachheit halber soll nachfolgend nur von „Person" die Rede sein.
4) Siehe https://de.wikipedia.org/wiki/Sophia_(Roboter), abgerufen am 19.10.2020.
5) Ausführlich: Groß, „AGB 4.0: Allgemeine Geschäftsbedingungen im Rahmen autonomer Vertragsschlüsse", in: InTeR 2018, S. 4ff.