Das Handy als digitale Geldbörse

Apps zum kontaktlosen Bezahlen: Verwendung und Einschätzung in Österreich

Wien, 07.12.2021
KFV (Kuratorium für Verkehrssicherheit) Bereich Eigentumsschutz

Das Handy als digitale Geldbörse

Apps zum kontaktlosen Bezahlen: Verwendung und Einschätzung in Österreich

Autor*innen
Dr. Georg Plattner
Patricia Jeßner, BA

Mitarbeit
Mag. Dagmar Lehner
Dr. Claudia Riccabona-Zecha

Fachliche Verantwortung
Dr. Georg Plattner

Auftraggeber
Dr. Armin Kaltenegger

Inhaltsverzeichnis

1. Key Facts 1

2. Einleitung 2

3. Methodik 3

4. Das Handy als digitale Geldbörse 4

4.1. Allgemeines und Funktionsweise 4

4.2. Sicherheit 5

4.3. Rechtliche Aspekte 6

4.3.1. Relevante Rechtstexte 6

4.3.2. Recht mit Technik im Gleichschritt für starken Schutz der Konsument*innen 7

5. Bezahlen in Österreich: Verhalten der Bevölkerung 11

6. Ergebnisse der KFV-Bevölkerungsbefragung 13

6.1. Kontaktloses Bezahlen 13

6.2. Bewertung der Sicherheit von Zahlungsweisen 15

7. Fazit: Beide Bezahlungsformen sind sicher – aber Vorteil Smartphone 19

1. Key Facts

Mobile Payment ist an mobile Endgeräte wie Handys, Tablets oder Smartphones geknüpft, die über einen NFC-Chip verfügen. Diese Technologie ist auch bei Scheckkarten im Einsatz.

Entgegen den Befürchtungen sind mit NFC-Chips ausgestattete Mobilgeräte sehr sicher: Während Scheckkarten immer "bereit" sind und ihre Daten unverschlüsselt senden, erfolgt dies bei Smartphones nur bei Aktivierung und mittels Verschlüsselung ("Tokenisierung").

Rechtlich gesehen ist sowohl die Bezahlung über Mobilgeräte als auch mittels Scheckkarte sehr gut vor Missbrauch abgesichert.

KFV-Befragung: Über ein Viertel der österreichischen Bevölkerung hat bereits über Smartphone bezahlt. 13% nutzen diese Bezahlform wöchentlich. Die Bevölkerung schätzt die Scheckkarte als deutlich sicherer als das Smartphone ein: 79% der Bevölkerung bewertet die Scheckkarte als "eher bis sehr sicher", beim Smartphone sinkt dieser Wert auf 39% ab.

2. Einleitung

Immer mehr Menschen nutzen in Österreich die Möglichkeit des kontaktlosen Bezahlens. Besonders in der Covid-19-Pandemie bietet es eine keimarme Bezahlmöglichkeit, mit der die Kontaktansteckung mit Viren minimiert werden kann. Nachdem vor einigen Jahren das kontaktlose Bezahlen mit der Kredit- oder Scheckkarte eingeführt wurde, ist der nächste Schritt der Digitalisierung in Österreich angekommen: Das Handy wird zur digitalen Geldbörse. Alles was dafür nötig ist, ist ein **Smartphone mit NFC-Chip**. Über eine **App einer Bank** oder der zwei großen Dienstleister **GooglePay** und **ApplePay** kann eine Kreditkarte oder ein Bankkonto direkt am Gerät hinterlegt werden. Die App wird aktiviert und der Bezahlvorgang kontaktlos am Terminal durchgeführt.

Doch ist diese neue Bezahlmethode auch sicher? Von den NFC-Chips in Kredit- und Scheckkarten ist bekannt, dass sie von Kriminellen theoretisch ausgelesen werden können. Auch die Karten selbst stellen ein Sicherheitsrisiko dar, wenn etwa an einem präparierten Terminal Geld abgehoben wird und dabei sämtliche Kartendaten kopiert werden. Ist dies beim Smartphone auch der Fall? Wo existieren Sicherheitsrisiken für die Konsument*innen bei dieser neuen Bezahlform, wie ist die rechtliche Absicherung bei illegalem Zugriff? Allen diesen Fragen ist das KFV in eigenen Recherchen nachgegangen, um zu veranschaulichen, wie der Stand der Technologie und der rechtlichen Rahmenbedingungen für deren Nutzung sind.

Vor der Corona-Pandemie war in Österreich das Barzahlen noch so weit verbreitet wie in wenigen anderen Ländern der EU. Das KFV hat sich in dieser Studie der Frage angenommen, ob sich diese Tendenz mittlerweile ändert und ob das Smartphone oder die Scheckkarte hier die Nase vorn haben. Gleichzeitig soll aber auch untersucht werden, wie die Österreicher*innen die Sicherheit der zwei hauptsächlichen kontaktlosen Bezahlmöglichkeiten bewerten. Sehen Sie einen Unterschied in der Sicherheit zwischen der Bezahlung mit Scheckkarte und der mit dem Handy? Und wie ist der tatsächliche Sicherheitsstandard der zwei Zahlungsoptionen zu bewerten?

Diese Studie dient daher der Abgleichung von tatsächlicher und subjektiver Sicherheit der neuen kontaktlosen Bezahlformen. Neue Technologien werden oftmals von der Bevölkerung kritisch beäugt, und das KFV möchte hier einen Beitrag zur Aufklärung leisten und zeigen, wie sicher das kontaktlose Bezahlen sein kann, aber auch, worauf die Österreicher*innen trotzdem noch achten sollten, wenn sie mit Handy oder Scheckkarte bezahlen.

3. Methodik

Um den Kenntnisstand der österreichischen Bevölkerung zum Thema „Bezahlen mit dem Smartphone“ darzustellen, wurde eine repräsentative Bevölkerungsbefragung durchgeführt. Hierbei wurden, in Zusammenarbeit mit dem Marktforschungsinstitut Spectra, im März 2021 1.000 Österreicher*innen, die repräsentativ für die „Internet-Bevölkerung“ stehen, per Online-Fragebogen befragt.

4. Das Handy als digitale Geldbörse

4.1. Allgemeines und Funktionsweise

Die Zeit des Bargeldes neigt sich langsam, aber sicher, dem Ende zu. Auch das Bezahlen „mit Karte“ wird in der Zukunft wohl an Bedeutung verlieren. Die Konzentration aller möglichen Alltagsutensilien auf ein Endgerät nimmt immer weiter zu und macht natürlich auch vor dem Bezahlen nicht Halt. Smartphones sind Telefon, Kamera, Musikplayer, Zeitung, Straßenkarte und vieles mehr – dass sie auch die Funktionen der Geldbörse übernehmen, war nur eine Frage der Zeit.

Beim so genannten **Mobile Payment** handelt es sich um elektronische Zahlungsformen, die an die Verwendung von mobilen Endgeräten wie **Mobiltelefone** („Handypayment“), aber auch **Tablets** oder **Smartwatches**, geknüpft sind. Dieses kontaktlose Bezahlen und Geldbeheben mit dem Handy ist in den USA und in asiatischen Ländern längst verbreitet und setzt sich seit einiger Zeit auch in Europa durch. Der Vorteil: Der*die Kund*in spart Zeit und benötigt weder Bargeld noch Karten.

Um das Smartphone in ein digitales Portemonnaie zu verwandeln, muss eine entsprechende App installiert werden. In weiterer Folge ist ein Bank- oder Kreditkartenkonto zu hinterlegen – außer die App ist Produkt der eigenen Bank. Zudem müssen Smartphones als auch der Bezahlterminal (am gängigsten) mit einem **NFC-Chip** („Near Field Communication“) ausgerüstet sein.

Ein NFC-Chip kann auf zweierlei Arten genutzt werden:

- „**passiv**“ bedeutet, dass der verbaute Chip kein eigenes elektromagnetisches Feld erzeugt und daher auch keine Daten empfangen, sondern lediglich an einen „aktiven“ Chip versenden kann. Diese Art Chips ist in Scheckkarten verbaut. Ein „passiver“ Chip kann nur mit einem „aktiven“ Chip kommunizieren.
- „**aktiv**“ bedeutet, dass der verbaute Chip ein elektromagnetisches Feld erzeugt und damit sowohl Daten senden als auch empfangen kann. „Aktive“ Chips werden z.B in Bezahlterminals oder in Smartphones eingesetzt. Ein „aktiver“ Chip kann sowohl mit einem anderen „aktiven“ als auch mit einem „passiven“ Chip kommunizieren.

Das bedeutet, dass für das kontaktlose Bezahlen mit Smartphone **dieselbe Technologie** verwendet wird, wie sie bereits in Scheck- und Kreditkarten im Einsatz ist (allerdings als „aktiver“ Chip). Dementsprechend funktioniert die Abwicklung auch gleich: die App wird geöffnet oder läuft im Hintergrund, das Handy ans Terminal gehalten und der Betrag wird bezahlt. Die Datenübertragung ist hier bereits über wenige Zentimeter hinweg möglich. Kleine Beträge können bei entsprechender Einstellung ohne PIN-Abfrage bzw. Touch- oder Face-ID abgebucht.

Auf dem Markt etabliert haben sich vor allem zwei neue Typen von Zahlungsdiensten. Einerseits so genannte **Zahlungsauslöse**- und andererseits so genannte **Kontoinformationsdienste**. Letzteres beschreibt die jeweils am Internet-Banking des Kreditinstituts hängende Funktion,

Zahlungs- bzw. Kontodaten zwischen Banken, deren Kund*innen und Onlinehändler*innen zu übermitteln, ohne dabei selbst Kundengelder zu übernehmen oder zu transferieren.

Beim **Zahlungsauslösedienst** beauftragt der*die Kund*in den*die Dienstleister*in, für ihn*sie bei dem*der kontoführenden Zahlungsdienstleister*in eine Überweisung auszulösen, etwa wenn er*sie im Shop eines Händlers einkauft. In der Gewissheit, dass die Zahlung ausgelöst wurde, ist der*die Händler*in bereit, die Ware unverzüglich freizugeben bzw. die Dienstleistung zu erbringen.

Als Zahlungsinstrument kann grundsätzlich jedes Instrument angesehen werden, das einen Zahlungsvorgang veranlassen kann. Relevant ist jedoch, dass ein solches Instrument nur dann zulässig ist, sofern es einer bestimmten Person zugerechnet werden kann (Personalisierung und Authentifizierung). Daher ist ein Mobiltelefon erst durch eine Unterschrift oder den PIN personalisiert und somit als Zahlungsinstrument anzusehen. Ein nicht klar einer Person zuordenbares Smartphone ist daher nicht zulässig (z.B. anonyme Wertkartentelefone).

4.2. Sicherheit

Das Smartphone als kontaktlose Bezahlmöglichkeit ist international gesehen also auf der Überholspur. Doch das Smartphone hat nach wie vor – vor allem in der älteren Bevölkerung – ein **Image-Problem**. Schließlich kann ein Endgerät theoretisch gehackt werden, es können Viren darauf platziert werden, oder ein Trojaner.

So schrecken nach wie vor Menschen davor zurück, ihre Bankgeschäfte digital abzuwickeln, geschweige denn am Handy. Beim Bezahlen kommt ein weiterer Faktor hinzu, der die **Unsicherheit der weniger digitalaffinen Bevölkerung** erhöht: das kontaktlose Bezahlen, unter Umständen auch noch ohne Eingabe eines PIN-Codes. Dies führt dazu, dass der neuen Bezahlform speziell in Ländern wie Österreich, die eine stark verwurzelte Bargeld-Kultur aufweisen, mit großem Misstrauen begegnet wird.

Doch wie ist es um die Sicherheit des kontaktlosen Bezahlens mit dem Smartphone tatsächlich bestellt?

Für die deutsche Verbraucher*innenzentrale ist das Urteil recht eindeutig: **„Anders als befürchtet, ist der vorherrschende technische Standard – das mit NFC (Nearfield Communication) ausgestattete Smartphone – jedoch eine vergleichsweise sichere Technologie“** (Verbraucherzentrale, 2018). Die Beurteilung der Institution fällt vor allem im Vergleich zu Scheck- und Kreditkarten sehr gut für das Smartphone aus. **Karten sind ständig „bereit“ ihre Daten unverschlüsselt zu senden (es muss ein „aktiver“ Chip in Reichweite sein).** Die Reichweite der NFC-Chips ist zwar begrenzt, sie kann allerdings von Kriminellen verlängert werden. Außerdem gibt es gerade im Gedränge des urbanen Raumes theoretisch Möglichkeiten bis auf wenige Zentimeter an andere Menschen heranzukommen und so die Daten auszulesen. Darüber hinaus kann eine funkfähige Scheckkarte mittels manipulierter Lesegeräte ausspioniert werden.

Das Smartphone ist im Gegensatz dazu sicherer. Zum einen **sendet das Smartphone seine Daten nur bei aktivierter App**. Das bedeutet, dass die App einmalig bewusst gestartet werden muss, um das Handy zahlungsbereit zu machen. **Viele Banken ermöglichen die Funktion, dass das Handy bis zu einem Betrag von 50€ immer „zahlungsbereit" ist, ohne dass eine Aktivierung und/oder Identifikation (über Pin, Fingerabdruck oder Face-ID) nötig ist**. Bei höheren Beträgen ist dies jedenfalls nötig. **Zusätzlich kann man jedoch weitere Sicherheitsparameter einziehen und zum Beispiel einstellen, dass auch bei Kleinstbeträgen eine Aktivierung der App durch eine Identifikation notwendig ist**.

Zum anderen sind die Daten, die vom Gerät zum Lesegerät an der Supermarktkassa gesendet werden, **keine 1:1-Übertragung der Bankdaten, zum Beispiel der Kreditkartennummer, sondern bloß eine verschlüsselte Kopie (ein so genannter Token)**. Und diese Kopie gilt auch nur für den Vorgang, der gerade durchgeführt wird. Dieser Vorgang wird als "Host Card Emulation" (HCE) bezeichnet. Dadurch ist es – selbst für den Fall, dass ein*e Kriminelle*r nahe genug an das Smartphone kommt, um das Signal abzufangen – nicht möglich, mit diesen Daten widerrechtlich Zugriff auf das Konto oder die Kreditkarte zu bekommen, und auch sonst werden keine Daten offen gesendet.

Im Gegensatz dazu ist die Kredit- oder Scheckkarte ständig sendebereit und würde bei Aktivierung die Daten unverschlüsselt senden. Es sind aber normalerweise keine sensiblen Daten, die hier gesendet werden. Auch hier gilt außerdem, wie bereits oben erwähnt, dass der*die Kriminelle sich sehr nah an seinem*ihrem Opfer befinden muss. Bezahlungen illegal zu starten ist ebenso unmöglich, da die Chips nur auf registrierte Terminals reagieren. Daher sind beide Zahlungsmethoden insgesamt als sicher zu bewerten. Das Handy hat jedoch auf diesem hohen Niveau die Nase etwas weiter vorn, was die Sicherheit der eigenen Daten angeht, da diese zum Einen verschlüsselt sind, und zum anderen (bei entsprechender Sicherheitseinstellung durch den*die Nutzer*in) immer eine Authentifizierung notwendig ist, um das Senden der Daten zu starten.

4.3. Rechtliche Aspekte

4.3.1. Relevante Rechtstexte

Um diese neuen Zahlungsmethoden rechtlich zu umrahmen, wurden auf europäischer wie auch auf österreichischer Ebene Gesetzestexte geschaffen, die dieser neuen Entwicklung Rechnung trugen und sowohl Konsument*in als auch Bank-/Kreditinstitut schützen sollen. Auf europäischer Ebene wurde im Jahr 2015 mit der Zahlungsdienstrichtlinie (**PSD II-RL**) dem Umstand Rechnung getragen, dass sich seit der PSD I-RL 2007 (umgesetzt in Österreich durch das Zahlungsdienstegesetz 2009) einerseits der Markt für den Massenzahlungsverkehr erheblich vergrößert hatte und andererseits eine Reihe neuer technischer Innovationen aufgetreten waren. Zudem hatten sich neue Formen von Zahlungsdienstleister*innen entwickelt. Die PSD II-RL hat somit die rechtliche Basis dafür geschaffen, dass Zahlungsauslösedienste oder Kontoinformationsdienste tätig werden dürfen und trägt in einem digitalisierten Zeitalter zur (Kunden-)Sicherheit im elektronischen Zahlungsverkehr bei. Zu erwähnen ist auch noch die **delegierte Verordnung (EU) 2018/389** der Kommission mit Technische Regulierungsstandards

für eine starke Kund*innenauthentifizierung und für sichere offene Standards für die Kommunikation (anzuwenden seit 14.9.2019).

In Österreich wurde die erwähnte Richtlinie PSD II durch das **Zahlungsdienstegesetz 2018** umgesetzt und trifft Rahmen- und Aufsichtsregelungen für Zahlungsauslöse- und Kontoinformationsdienste. Die Haftungssituation für Zahlungsdienstnutzer*innen ist damit etwas günstiger (jedenfalls, sofern sie Verbraucher*innen sind) als zuvor und im entsprechenden Anwendungsbereich der neuen Vorgabe einer „starken" Kund*innenauthentifizierung angepasst (siehe hierzu unten).

Das Zahlungsdienstegesetz 2018 ist anzuwenden, wenn ein Zahlungsdienst innerhalb Österreichs erbracht wird. Anknüpfungspunkte für die Erbringung des Zahlungsdienstes innerhalb Österreichs sind der Sitz des*der Zahlungsdienstleister*in oder der Wohnort des*der Zahlungsdienstnutzer*in.

Das Zahlungsdienstegesetz 2018 ist auf Unternehmer*innen und Verbraucher*innen zunächst gleichermaßen anzuwenden. Allerdings gibt es einige Bestimmungen, die gegenüber Verbraucher*innen relativ zwingend sind, also nicht zu deren Nachteil abgeändert werden können. Diese sind im § 55 Abs 1 Zahlungsdienstegesetz 2018 aufgelistet und umfassen neben Sorgfaltspflichten insbesondere Vorschriften betreffend Informationspflichten, transparente Vertragsbedingungen, Autorisierung und Ausführung von Zahlungsvorgängen sowie auch Haftungsbestimmungen.

Als Verbraucher*in gilt nach dem Zahlungsdienstegesetz 2018 jede natürliche Person, die Zahlungsvorgänge tätigt, die nicht zu Zwecken ihrer gewerblichen oder beruflichen Tätigkeit zuzurechnen sind.

4.3.2. Recht mit Technik im Gleichschritt für starken Schutz der Konsument*innen

Im Bereich der digitalen Zahlungsdienste hat die EU es geschafft, dass die rechtlichen Bestimmungen mit den technologischen Entwicklungen quasi im Gleichschritt marschieren. So ergibt sich eine sehr gute rechtliche Absicherung des*der Konsument*in in fast allen Aspekten des kontaktlosen Zahlens.

Die Dienstleister*innen benötigen seit 2018 eine Konzession, um ihre Dienste erbringen zu können. Damit sind **Konsument*innen vor unseriösen Anbieter*innen** weitgehend **geschützt**. Auch dürfen diese Dienstleister*innen nur dann tätig werden, wenn **der*die Kund*in einen Vorgang** (z.B. die Anweisung einer Überweisung) **ausdrücklich beauftragt hat**. Sie haben das Recht auf Zugang zum Zahlungskonto des*der Kund*in mit dessen*deren Zustimmung. Allerdings sind sowohl der Zugriff als auch die Verwendung der dadurch erlangten Informationen durch Datenschutz- und Sicherheitsvorschriften beschränkt.

2019 erfolgte ein Zusammenschluss von mehreren Mobile-Payment-Anbieter*innen zur **European Mobile Payment Association** mit Sitz in Zürich, darunter auch Blue Code aus Österreich. Damit gibt es auch für Europa ein eigenes Regelwerk mit europäischen Datenschutzstandards und Anonymität (Kund*innendaten bleiben bei der Hausbank).

Abgesehen von der organisatorischen Regulierung führten bei Umsetzung der EU-Richtlinie auch inhaltliche Vorgaben für Haftung und Nachweis der Zugangsberechtigung zu einer Steigerung der Sicherheit des Konsumenten.

- So ist rechtlich klar geregelt, dass der*die Zahlungsdienstleister*in das Risiko eines nicht ordnungsgemäß autorisierten Zahlungsvorgangs trägt (verschuldensunabhängige Haftung). Darüber hinaus zeigt sich die verbesserte Rechtsstellung des Zahlers durch folgendes Haftungssystem: **Bei missbräuchlicher Verwendung eines Zahlungsinstruments haftet der*die Zahler*in nur, wenn er in der Lage war, den Verlust, den Diebstahl oder die sonstige missbräuchliche Verwendung des Zahlungsinstruments zu bemerken.**
- **Aber selbst in diesem Fall ist die Haftung des*der Zahler*in auf höchstens 50 Euro begrenzt** (früher lag die Haftungsgrenze bei 150 Euro). Die Haftungsgrenze gilt – wie bereits zuvor – nicht, wenn der*die Zahler*in in betrügerischer Absicht gehandelt oder die Pflicht, seine personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen, vorsätzlich oder grob fahrlässig verletzt hat.
- **Anstelle des*der Zahler*in hat nun der Zahlungsdienstleister den Nachweis für Betrug, Vorsatz oder grobe Fahrlässigkeit zu erbringen.**

Ferner hat im Fall eines „elektronischen Zahlungsvorganges“ der*die Zahlungsdienstleister*in eine so genannte **starke Kund*innenauthentifizierung** zu verlangen, die Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem*einer bestimmten Zahlungsempfänger*in verknüpfen. Damit soll das Risiko eines Betrugs im Zahlungsverkehr oder anderer Missbrauch minimiert werden. Folglich bedeutet das System der starken Kund*innenauthentifizierung bei der Durchführung von Online-Zahlungen, eindeutig und nachweisbar festzustellen, dass ein*e bestimmte*r Zahler*in eine bestimmte Zahlung in Auftrag gegeben hat. Zur Sicherstellung sind mindestens zwei Elemente der folgenden Kategorien erforderlich (so genannte „Zwei-Wege-Authentifizierung“):

- **Besitz: etwas, das ausschließlich der*die Zahler*in besitzt (z.B. Mobiltelefon)**
- **Wissen: etwas, das ausschließlich der*die Zahler*in weiß (z.B. Passwort, PIN)**
- **Inhärenz: ein Merkmal des*der Zahler*in, das diesem*r eindeutig zugeordnet werden kann (z.B. Fingerprint, Gesichtserkennung, Iris-Scan).**

Die Elemente müssen dabei voneinander unabhängig sein. Die Nichterfüllung eines Kriteriums darf die Zuverlässigkeit der anderen nicht beeinträchtigen, und die Vertraulichkeit der Authentifizierungsdaten muss geschützt sein. Bei einem elektronischen Fernzahlungsvorgang muss die Authentifizierung zudem Elemente umfassen, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen.

Key Facts Haftungsfragen

Bei missbräuchlicher Verwendung eines Zahlungsinstruments haftet der*die Zahler*in nur, **wenn er in der Lage war, den Verlust, den Diebstahl oder die sonstige missbräuchliche Verwendung des Zahlungsinstruments zu bemerken.**

Selbst in diesem Fall ist die Haftung des*der Zahler*in auf **höchstens 50 Euro** begrenzt

Eine Ausnahme besteht für den Fall, wenn der*die Zahler*in in betrügerischer Absicht gehandelt oder die Pflicht, seine personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen, **vorsätzlich oder grob fahrlässig** verletzt hat

Es ist jedoch vorgesehen, dass Zahlungsdienstleister*innen bei Auslösen eines kontaktlosen elektronischen Zahlungsvorgangs durch den*die Zahler*in von einer starken Kund*innenauthentifizierung absehen dürfen, wenn

- **der Einzelbetrag des kontaktlosen elektronischen Zahlungsvorgangs nicht über 50 EUR hinaus geht, und**
- **die früheren kontaktlosen elektronischen Zahlungsvorgänge, die über ein mit einer kontaktlosen Funktion ausgestattetes Zahlungsinstrument ausgelöst wurden, seit der letzten Durchführung einer starken Kund*innenauthentifizierung zusammengenommen nicht über 150 € hinausgehen, oder**
- **die Anzahl der aufeinanderfolgenden kontaktlosen elektronischen Zahlungsvorgänge, die über das mit einer kontaktlosen Funktion ausgestattete Zahlungsinstrument ausgelöst wurden, seit der letzten Durchführung einer starken Kund*innenauthentifizierung nicht über fünf hinausgehen.**

Die EU-Kommission erwägt grundsätzlich eine Überarbeitung der PSD II-Richtlinie und möchte die Akzeptanz digitaler Zahlungen sowohl im öffentlichen als auch im privaten Sektor fördern; bis dato liegt jedoch noch kein konkreter Vorschlag vor. Noch im 4. Quartal 2021 sollen jedenfalls im Zuge einer Evaluierung der PSD II-Richtlinie Verbesserungspotenziale identifiziert und in weiterer Folge umgesetzt werden. Der Fokus liegt insb. auf folgenden Bereichen:

- Aktualisierung der Anforderungen an technische Lösungen, die von Zahlungsdienstleistern für eine starke Kundenauthentifizierung verwendet werden (Schwerpunkte: Stärkung personenbezogener Elemente wie Biometrie, Verringerung der Verwendung von Elementen mit geringerem Sicherheitsgrad wie statischen Kennwörtern

und Einschränkung der Verwendung älterer Technologien und Kommunikationskanäle, Verbesserung der elektronischen Identifizierung),
- Vorbeugung neuer Arten von Betrug,
- weitere Stärkung des Schutzes des Zahlers (Konsumentenschutz).

5. Bezahlen in Österreich: Verhalten der Bevölkerung

Österreich gilt seit Langem als eines der Länder der Euro-Zone, deren Bevölkerung am meisten an Bargeld hängt. Dies wird auch immer wieder durch Untersuchungen der Europäischen Zentralbank (EZB) untermauert, die zeigen, dass andere Länder in viel größerem Ausmaß die Möglichkeit des bargeldlosen Bezahlens nutzen (siehe Abbildung 1). **Österreich ist eines von nur drei Ländern, in denen laut dieser Studie das Bargeld bei über 40 Prozent der Befragten das bevorzugte Bezahlungsmittel ist**. Lediglich Deutschland und Zypern weisen noch höhere Anteile auf.

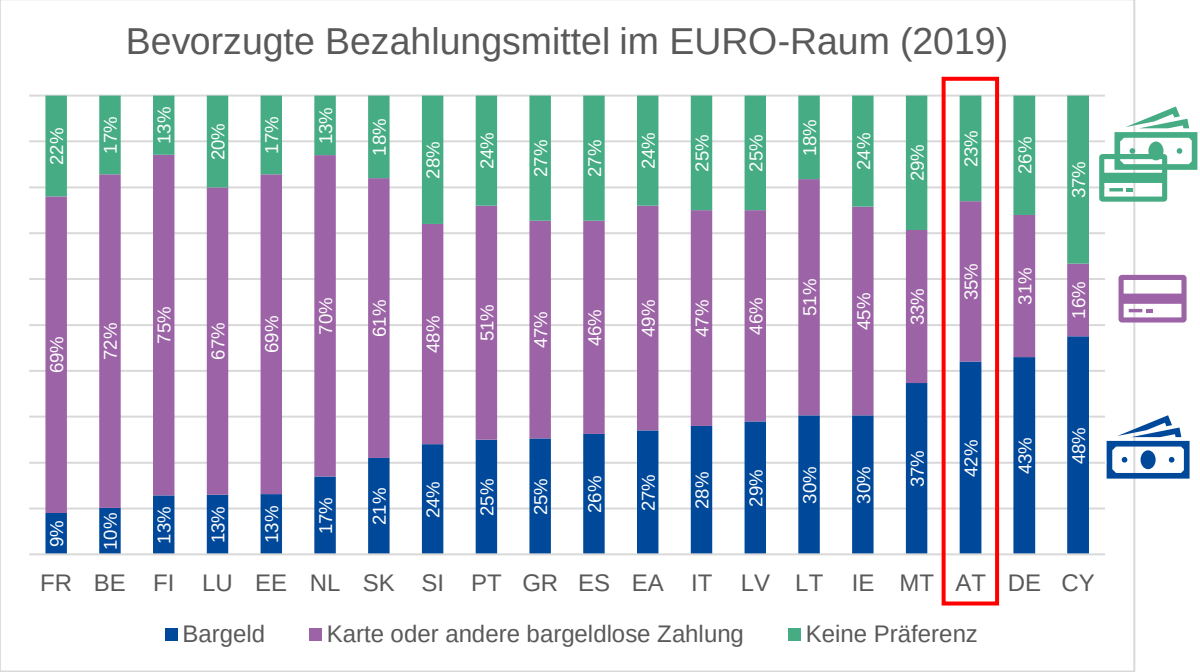


Abbildung 1: Bevorzugte Bezahlungsmittel im EURO-Raum (2019). Quelle: EZB (2021, S. 57)

Auch die Politik vertritt diese Position immer wieder. So wurde ein EZB-Vorschlag einer Obergrenze von 10.000€ bei Barbezahlungen im Mai 2021 durch den österreichischen Finanzminister Gernot Blümel (ÖVP) reflexartig abgelehnt: "Wir werden keine schleichende Abschaffung des Bargeldes akzeptieren", da das Bargeld nach wie vor das beliebteste Zahlungsmittel sei (Hahn, 2021). Sogar im türkis-grünen Regierungsprogram befindet sich ein Bekenntnis zum Bargeld.

Auch in Zeiten der Corona-Pandemie ist diese „Liebe der Österreicher*innen zum Bargeld“ zu beobachten: Laut Berechnungen der Österreichischen Nationalbank (ÖNB) werden in **österreichischen Haushalten** derzeit **zwölf bis 13 Mrd. Euro Bargeld** gehortet. Seit der Krise ist dieser Wert um rund 2,5 Mrd. Euro gestiegen (Kowalcze, 2021).

Die Gründe für die Liebe der Bürger*innen zum Bargeld sind vielfältig. So wird Bargeld nach wie vor mit Freiheit assoziiert und die Menschen schätzen die Anonymität einer Bargeldzahlung, da hier Finanzdienstleister*innen keinen Überblick erhalten, wann für was Geld ausgegeben wird. Darüber hinaus wird das Bargeld als sicherer gesehen: sollte eine Wirtschaftskrise das Geldinstitut der Wahl dahinraffen, ist das Bargeld unter dem Kopfkissen immer noch was wert, die Einlagen im Geldinstitut möglicherweise verloren.

Auch die **Verwendung von Scheck- und Kreditkarten** oder anderen bargeldlosen Bezahlformen ist in Österreich im Euro-Zonen-Schnitt **unterdurchschnittlich**. Auch Zahlen der Österreichischen Nationalbank zeigen dies: Laut der ÖNB werden 79 Prozent der Transaktionen in Österreich nach wie vor in bar durchgeführt.

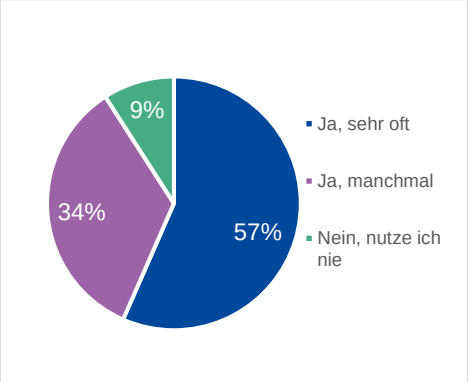
Das bargeldlose Bezahlen ist in Österreich also nach wie vor eine sekundäre Bezahlform. Über allem thront das Bargeld, durch die Krise noch einmal verfestigt auf seinem Platz an der Sonne. Doch die neuen Bezahlformen werden sich weiter Raum nehmen, nicht nur aus Komfortgründen, sondern auch, weil sich über kurz oder lang die bargeldkritische EZB-Linie auch in Österreich durchsetzen wird.

6. Ergebnisse der KFV-Bevölkerungsbefragung

6.1. Kontaktloses Bezahlen

In der vom Umfrageinstitut Spectra im Auftrag des KFV durchgeführten Bevölkerungsbefragung zeigt sich, dass das kontaktlose Bezahlen in der österreichischen Bevölkerung angekommen ist. Die Unterschiede zwischen dem kontaktlosen Zahlen mit der „guten alten“ EC-Karte und der relativ neuen Option Smartphone sind jedoch eklatant:

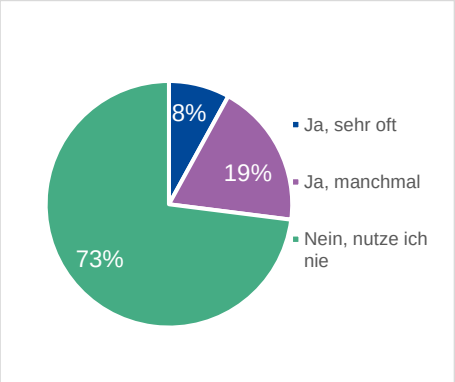
Eine deutliche Mehrheit von 90% der Bevölkerung nutzt die EC-Karte für das kontaktlose Bezahlen, davon 56% „sehr oft“ und weitere 34% „manchmal“. Hier ist, wie in vielen Bereichen der Digitalisierung, ein klarer Unterschied der Nutzung je nach Altersgruppen festzustellen: Je jünger die Befragten, umso öfter wird das kontaktlose Bezahlen mit EC-Karte genutzt (siehe Abbildung 2).



	Alter					
	18-25 Jahre	26-35 Jahre	36-45 Jahre	46-55 Jahre	56-65 Jahre	66 Jahre+
Sehr oft	68%	66%	56%	48%	51%	55%
Manchmal	25%	28%	36%	41%	38%	31%
Nie	7%	5%	8%	12%	11%	13%

Abbildung 2: Nutzung der kontaktlosen Bezahlung mit EC-Karte. Quelle: Spectra (2021).

Das Smartphone als Zahlungsmittel weist eine deutlich geringere Nutzungsquote von 27% auf. **Das heißt dass, obwohl das Bezahlen mit dem Smartphone noch relativ neu ist, haben immerhin über ein Viertel der österreichischen Bevölkerung diese Bezahlmethode bereits angewandt.** Auch hier gibt es deutliche Unterschiede nach Alter: Die 18-25-jährigen erreichen mit 44% die mit Abstand höchste Quote. Mit zunehmendem Alter geht die Nutzung deutlich zurück und liegt bei den über 66-jährigen nur mehr bei 19%. Klar zu sehen ist hier die Tendenz der älteren Generation, neueren Technologien äußerst kritisch gegenüberzustehen, wohingegen jüngere Menschen diese neuen Möglichkeiten als neue Chancen und Erleichterungen aktiver annehmen.



	Alter					
	18-25 Jahre	26-35 Jahre	36-45 Jahre	46-55 Jahre	56-65 Jahre	66 Jahre+
Sehr oft	18%	12%	8%	5%	3%	4%
Manchmal	26%	19%	17%	18%	19%	15%
Nie	56%	69%	75%	77%	78%	81%

Abbildung 3: Nutzung der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021).

Sieht man sich das Nutzungsverhalten jener Menschen an, die das Smartphone als Zahlungsmittel nutzen, so zeigt sich, dass 47% der Nutzer*innen zumindest einmal wöchentlich mit dem Handy bezahlen. **Umgerechnet auf die Gesamtbevölkerung sind dies 13%, die das Smartphone wöchentlich zum Bezahlen nutzen**. Dabei kommt am häufigsten die App der jeweiligen Hausbank zur Anwendung, wie 57% der Nutzer*innen angeben. Dies ist vor allem die App der Erste Bank/Sparkasse (38%) und jene der Raiffeisenbank (22%). 32% der Nutzer*innen verwenden Apple Pay, weitere 15% Google Pay.

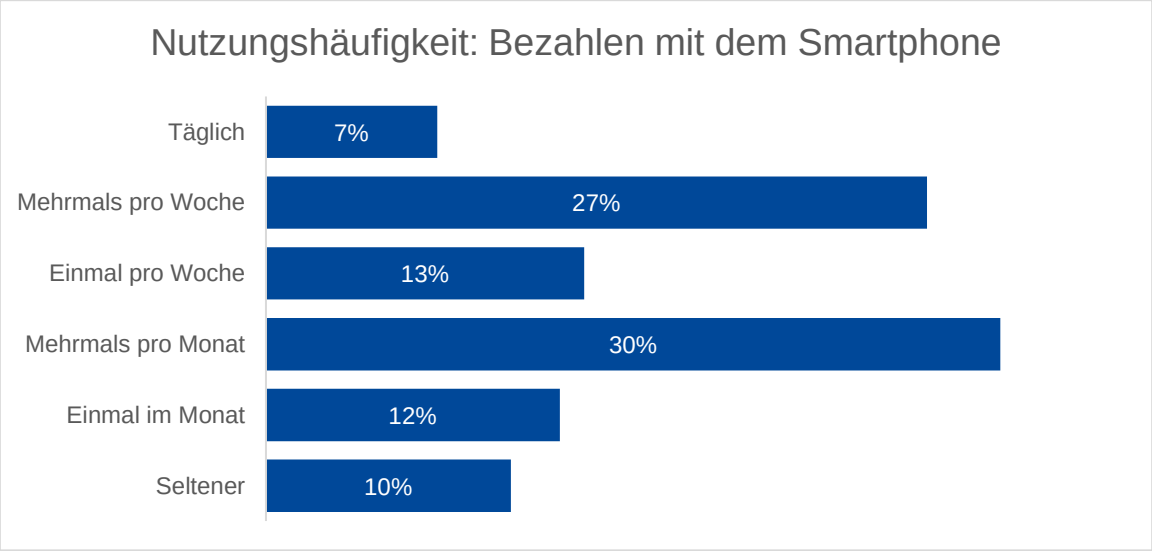


Abbildung 4: Nutzungshäufigkeit der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021).

Zwei Aspekte dominieren bei den Gründen der Bezahlung mit dem Smartphone: Es ist praktisch, weil man das Handy immer bei sich hat (78%) und es funktioniert „schnell und bequem“ (72%). Positive Nebeneffekte sind, dass man keine Geldbörse mehr braucht (27%) und das viele Kleingeld wegfällt (26%). In den Antworten versteckt ist auch einer der wichtigsten Punkte, die den Siegeszug des Smartphone beim bargeldlosen Bezahlen beschleunigen könnten: **Die Reduktion**

der mitzutragenden Gegenstände wird drastisch reduziert. Es reicht mittlerweile für fast alle Unternehmungen im öffentlichen Raum, das Handy mitzunehmen. Die dicke Geldbörse wird ebenso überflüssig wie das Scheckkartenetui.

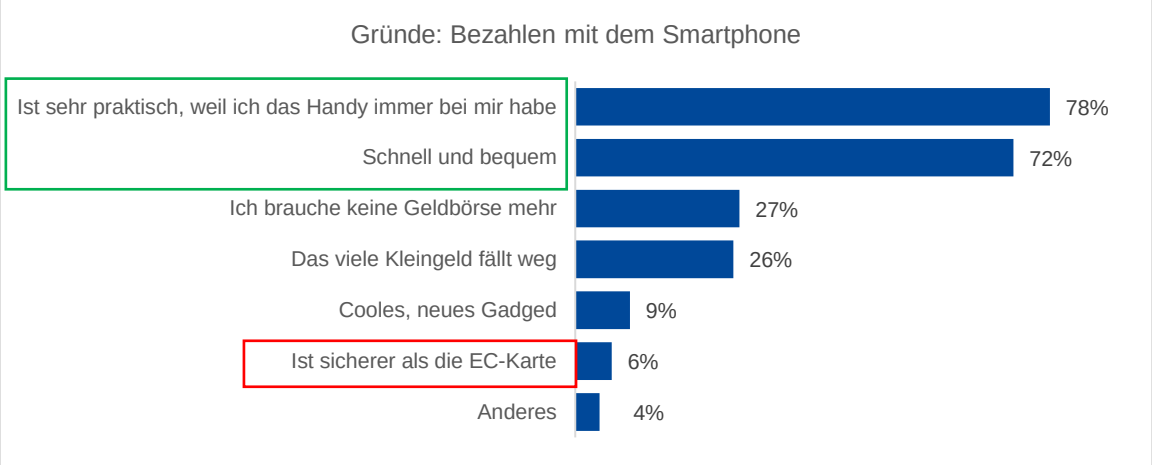


Abbildung 5: Gründe für kontaktlose Bezahlung mit Smartphone. Quelle: Spectra (2021).

Es ist klar zu sehen, dass das Smartphone als Bezahlungsmittel in Österreich noch einen weiten Weg vor sich hat. Nichtsdestotrotz ist es angekommen, und die zukünftigen Entwicklungen sowie die große Sicherheit des kontaktlosen Bezahlens mit dem Handy sollten diesen Fortschritt auch weiter antreiben. Doch wie bewerten Österreicher*innen aktuell die Sicherheit der unterschiedlichen Zahlungsmethoden?

6.2. Bewertung der Sicherheit von Zahlungsweisen

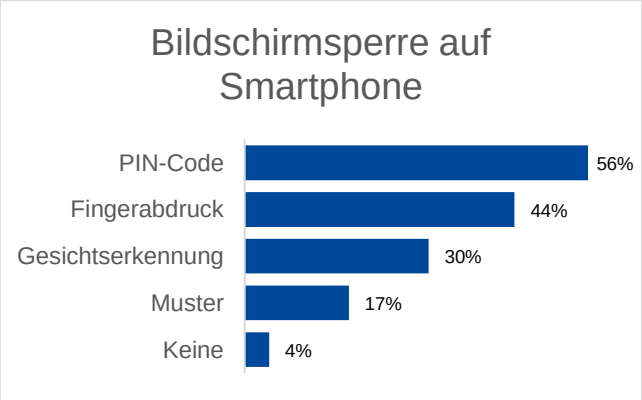


Abbildung 6: Bildschirmsperre auf Smartphone. Quelle: Spectra (2021).

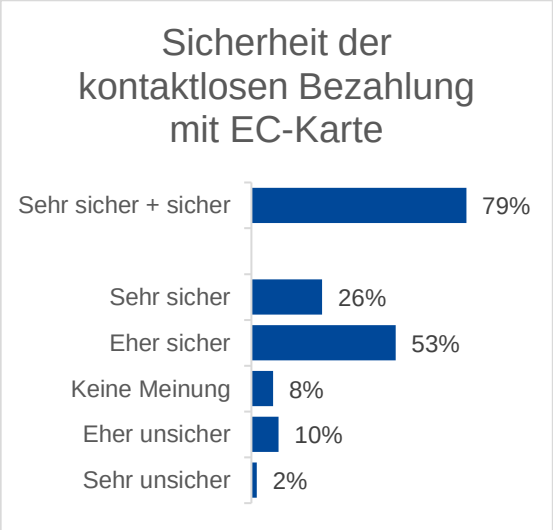
Wenn es um die Sicherheit beim kontaktlosen Bezahlen mit dem Handy geht, dann spielt unter anderem die Bildschirmsperre auf den Smartphones eine wesentliche Rolle. Dies ist der wichtigste Schutz, um das Gerät vor unbefugtem Zugriff zu schützen, und damit auch die eigenen Zahlungsinformationen. **96% der Nutzer*innen haben die Bildschirmsperre auf ihren Smartphones aktiviert.** Und zwar zu 56% mit PIN-Eingabe, zu 44% mit dem Fingerabdruck, zu 30% mittels Gesichtserkennung und zu 17% mit einem Muster zum Eingeben. Aus soziodemografischen Gesichtspunkten sind nur wenige Unterschiede festzustellen. Frauen nutzen

den PIN stärker als die Männer (63% vs 49%), Männer verwenden die Gesichtserkennung vermehrt (34% vs. 24%).

Das heißt, die weit überwiegende Mehrheit der Österreicher*innen schützt ihr Smartphone vor unbefugtem Zugriff durch Dritte. Dies ist eine gute Voraussetzung für die objektive Sicherheit des kontaktlosen Bezahlens mit dem Smartphone, da hiermit dem Missbrauch erstmal ein wichtiger Riegel vorgeschoben ist. Doch sehen das die Österreicher*innen genauso?

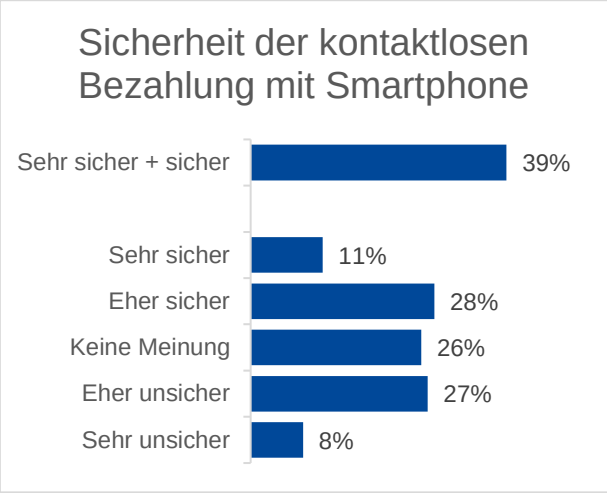
Hinsichtlich des Sicherheitsgefühls hat die EC-Karte deutliche Vorteile gegenüber dem Handy. Während 79% der Bevölkerung die EC-Karte beim kontaktlosen Bezahlen als „eher bis sehr sicher" bewerten, so sinkt dieser Wert für das Handy auf 39% ab (siehe Abbildung 7 und Abbildung 8). Hier muss allerdings auch dazu gesagt werden, dass die Zahl jener, die zum Bezahlen mit dem Smartphone „keine Meinung" haben, mit 28% mehr als dreimal so hoch ist wie bei der EC-Karte. Trotzdem ist auch die Zahl jener, die das Smartphone als „sehr oder eher unsicher" bewerten signifikant höher: Mehr als ein Drittel (35%) der Befragten bewertet die Sicherheit beim Bezahlen mit dem Smartphone auf negative Weise. Bei der EC-Karte sind es lediglich 12%.

Dieses klare Bekenntnis zur EC-Karte gilt übrigens für alle Alterskohorten und alle Bildungsschichten. Hier scheinen auch die immer wieder auftauchenden Berichte über manipulierte Kartenterminals bei Bankomaten, oder die Möglichkeit des Auslesens von EC-Karten auf kurze Distanz wenig Einfluss zu haben. Die Österreicher*innen sind davon überzeugt, dass die EC-Karte eher sicher ist. Hingegen scheint es beim Smartphone ein generelles Misstrauen gegenüber digitalen Technologien zu sein, die die Unsicherheit befeuern. Dieses Misstrauen ist in allen Bereichen der Digitalisierung zu beobachten und führt nach wie vor dazu, dass eigentlich sichere neue Technologien im ersten Moment Ablehnung erfahren, die sie nicht verdienen, speziell wenn es um Finanzen geht. So hatte auch das E-Banking lange Zeit mit großem Misstrauen und Ablehnung zu kämpfen, wie Umfragen zeigen (Härtel, 2015).



	Weitester Nutzer*innenkreis des Bezahlungsmittels	
	EC-Karte	Smartphone
Sehr sicher + sicher	83%	85%
Sehr sicher	28%	33%
Eher sicher	55%	52%
Keine Meinung	7%	6%
Eher unsicher	9%	8%
Sehr unsicher	1%	0%

Abbildung 7: Einschätzung Sicherheit der kontaktlosen Bezahlung mit EC-Karte. Quelle: Spectra (2021).



	Weitester Nutzer*innenkreis des Bezahlungsmittels	
	EC-Karte	Smartphone
Sehr sicher + sicher	40%	82%
Sehr sicher	11%	31%
Eher sicher	29%	51%
Keine Meinung	26%	10%
Eher unsicher	26%	8%
Sehr unsicher	7%	0%

Abbildung 8: Einschätzung Sicherheit der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021).

Interessant ist die Analyse auf Basis des weitesten Nutzer*innenkreises von EC-Karte und Handy, also jenen Befragten, die das jeweilige Zahlungsmittel zumindest manchmal nutzen. **Denn beide Nutzer*innengruppen sehen in der EC-Karte zu mehr als 80% eine sehr sichere Form des kontaktlosen Bezahlens (Abbildung 7). Beim Handy ist das aber deutlich anders. Nur die Handy-Nutzer stufen die Sicherheit bei der Bezahlung via Smartphone zu 82% als sicher ein, während die EC-Karten-Nutzer dies nur zu 40% tun (Abbildung 8)**. Und ein Drittel der EC-Kartennutzer*innen schätzt das Smartphone als „eher oder sehr unsicher“ ein. Auch hier scheint sich also zu bewahrheiten, dass das Misstrauen dem Smartphone gegenüber gilt, auch wenn man sich noch gar nicht mit der Bezahlform beschäftigt hat. Im umgekehrten Fall sehen sogar weniger Smartphone-Nutzer*innen die EC-Karte als unsicher an, als die Nutzer*innen der EC-Karte selbst.

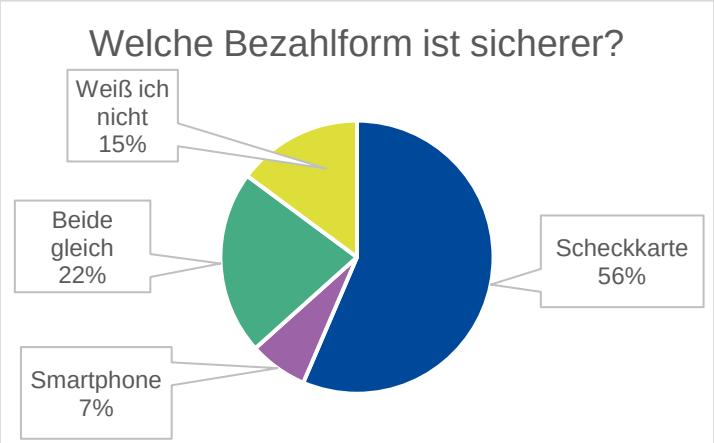


Abbildung 9: Einschätzung Sicherheit der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021).

Der Direktvergleich zeigt, dass die Scheckkarte (Bankomatkarte, Kreditkarte, Debitkarte) von 56% der Bevölkerung als wesentlich sicherer eingestuft wird als die digitale Bezahlung mittels Smartphones (nur 7%). Als gleich sicher schätzen 22% die beiden Bezahlformen ein.

Worin begründet sich die Angst vor dem Bezahlen mit dem Smartphone? Befragt nach den konkreten Bedrohungen, die die Bevölkerung mit dem Smartphone oder der Scheckkarte verknüpft, sind die Antworten durchaus ähnlich: Das größte Bedrohungsszenario stellt für die Bevölkerung das “Hacken” von EC-Karte oder Handy dar. **Mehr als die Hälfte der Österreicher*innen befürchten, dass ihre der EC-Karte gehackt werden könnte, beim Smartphone steigt dieser Anteil sogar auf über drei Viertel (Abbildung 10)**. Damit einhergehend meinen 52% (EC-Karte) bzw. 58% (Handy), dass es ein großes Risiko ist, wenn Konto-Informationen in die falschen Hände geraten. Weniger Probleme sieht die Bevölkerung darin, dass der Überblick über die Ausgaben verloren geht, wenngleich dies für immerhin 34% (bei der EC-Karte) bzw. 26% (beim Handy) ein Risiko darstellt. Konkrete Datenschutzbedenken haben zwar nur 19% bei der EC-Karte und 33% beim Handy, aber das Thema „Hacken von EC-Karte oder Handy“ impliziert ohnehin auch den Datenschutzaspekt.

Wenig überraschend ist auch die Tatsache, dass der weiteste Handy-Nutzer*innenkreis die Risiken signifikant geringer (wenngleich noch immer auf einem relativ hohen Niveau) einschätzt, als die Bevölkerung insgesamt.

Auch diese Antworten lassen vermuten, dass es vor allem ein generalisiertes, unspezifisches Misstrauen gegenüber Technologie ist, das die Österreicher*innen vor dem Handy als Bezahlungsmittel zurückschrecken lässt.

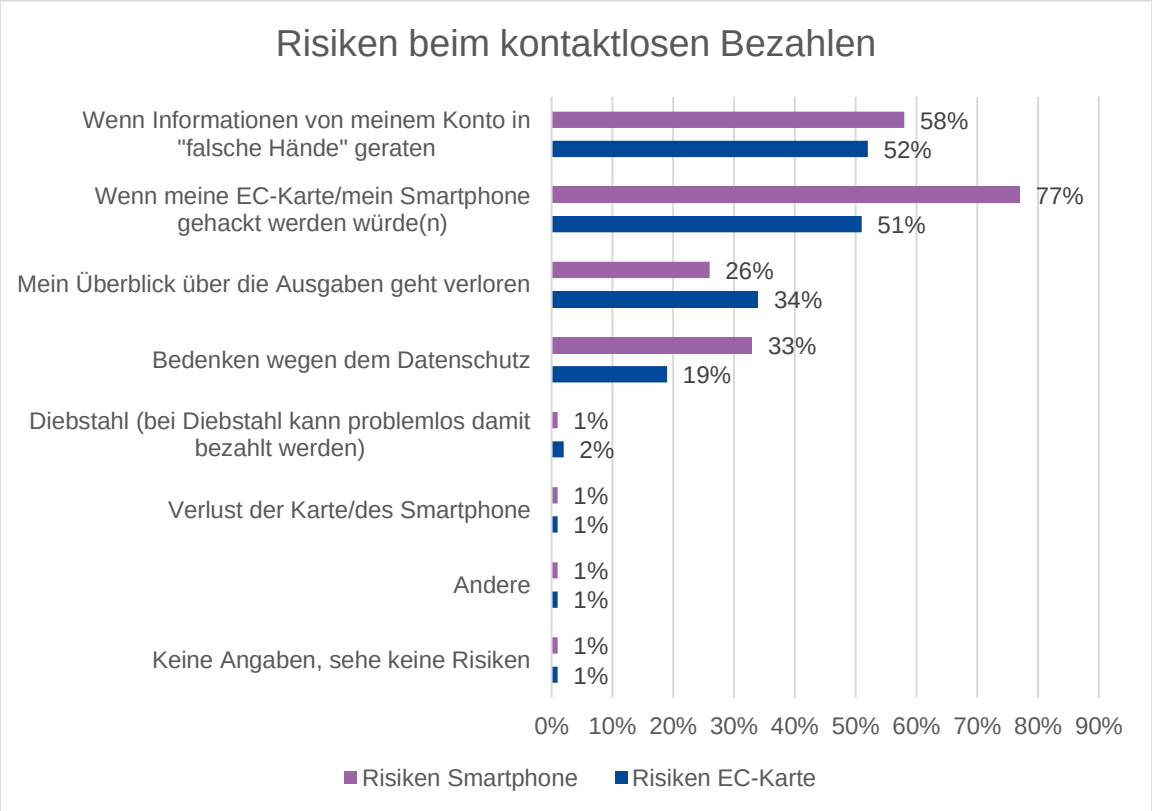


Abbildung 10: Einschätzung: Risiken des kontaktlosen Bezahlens. Quelle: Spectra (2021).

7. Fazit: Beide Bezahlungsformen sind sicher – aber Vorteil Smartphone

Smartphone		Scheckkarte
Gesendete Daten sind immer verschlüsselt		Gesendete Daten sind unverschlüsselt
Sendet Daten nur bei aktivierter App		Ist ständig sendebereit
unterschiedliche Sicherheitsstufen einstellbar		Braucht spezielle Schutzhülle für Sicherheit
gute rechtliche Absicherung für Konsument*innen		gute rechtliche Absicherung für Konsument*innen
personenbezogene Daten werden mitgesendet		personenbezogenen Daten werden **nicht** mitgesendet

Zum Abschluss bleibt zu sagen, dass beide Bezahlformen (Scheckkarte und Smartphone) insgesamt eine hohe Sicherheit aufweisen. Doch in den Feinheiten offenbart sich, dass das Smartphone auf Grund seiner Verschlüsselungen in der direkten Handhabe einen Vorsprung aufweist. In puncto Datenschutz hat das Smartphone jedoch einen kleinen Nachteil gegenüber der Scheckkarte. Denn für das Einrichten der App sind personenbezogene Daten anzugeben, die dann bei aktiver App (also während dem Bezahlvorgang) auch auslesbar sind. Bei der Scheckkarte sind es immer nur die reinen Bezahldaten, welche mitgesendet werden (Strauß, 2020).

Sollte man trotz der Sicherheit des kontaktlosen Bezahlens einmal Opfer von Kriminellen oder Missbrauch werden, so schützt hier auch zuverlässig das europäische Recht vor großem Schaden. Die EU hat es in diesem Fall geschafft, die rechtliche Absicherung einer neuen Technologie sehr schnell und sehr konsument*innenfreundlich zu gestalten, was durch die Geschwindigkeit des technischen Fortschrittes oft nicht einfach ist. Der maximale Haftungsbetrag – wenn man nicht fahrlässig handelt – ist beim kontaktlosen Bezahlen mit 50€ gedeckelt. Selbst wenn man also Opfer wird – man kommt meistens mit einem blauen Auge davon.

Das Smartphone ist also ein sehr sicheres Zahlungsmittel, vor allem, wenn man entweder die App der eigenen Hausbank oder die der zwei großen Player nutzt. **Die Daten sind fast nicht auszulesen, der Displayschutz schützt zuverlässig vor schnellem Missbrauch.**

Abschließend noch die wichtigsten Tipps, um typische Fehler zu vermeiden, damit das Smartphone sicher als Zahlungsmittel eingesetzt werden kann:

- **Achten Sie bereits beim Download der entsprechenden App darauf, welche personenbezogenen Daten Sie dort angeben müssen. Handelt die App nach dem Prinzip der Datensparsamkeit (Art. 5 DSGVO)?**
- **Achten Sie beim Einrichten des kontaktlosen Bezahlens am Smartphone darauf die „sofort bezahlen“ Option zu deaktivieren – damit stellen Sie sicher, dass die App eine Authentifizierung oder Aktivierung einfordert, bevor sie einen Zahlungsvorgang startet!**
- **Wichtig ist, stets die aktuelle Software- und Betriebssystem-Version zu nutzen**
- **Sichern Sie Ihr Smartphone durch eine PIN, damit im Falle eines Verlustes nicht auf die Pay-App zugegriffen werden kann**
- **Verleihen Sie Ihr Smartphone nicht – auch nicht mal nur kurz**
- **Schreiben Sie Ihre PIN nicht auf Ihr Smartphone (ja, auch das gibt’s immer noch…)**
- **Wählen Sie einen sicheren Code für Ihr E-Wallet.**

Abbildungsverzeichnis

Abbildung 1: Bevorzugte Bezahlungsmittel im EURO-Raum (2019). Quelle: EZB (2021, S. 57) 11
Abbildung 2: Nutzung der kontaktlosen Bezahlung mit EC-Karte. Quelle: Spectra (2021). 13
Abbildung 3: Nutzung der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021). 14
Abbildung 4: Nutzungshäufigkeit der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021). 14
Abbildung 5: Gründe für kontaktlose Bezahlung mit Smartphone. Quelle: Spectra (2021)..... 15
Abbildung 6: Bildschirmsperre auf Smartphone. Quelle: Spectra (2021). 15
Abbildung 7: Einschätzung Sicherheit der kontaktlosen Bezahlung mit EC-Karte. Quelle: Spectra (2021). 16
Abbildung 8: Einschätzung Sicherheit der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021). 17
Abbildung 9: Einschätzung Sicherheit der kontaktlosen Bezahlung mit Smartphone. Quelle: Spectra (2021). 17
Abbildung 10: Einschätzung: Risiken des kontaktlosen Bezahlens. Quelle: Spectra (2021). 18

Literaturverzeichnis

Europäische Zentralbank (EZB). (2021). *Study on the payment attitudes of consumers in the euro area (SPACE).* Frankfurt am Main: EZB. Abgerufen am 03. Mai 2021 von https://www.ecb.europa.eu/pub/pdf/other/ecb.spacereport202012~bb2038bbb6.en.pdf?05ce2c97d994fbcf1c93213ca04347dd

Hahn, A. (2021). Land der Münzen, Land der Scheine: Warum Österreicher Bargeld lieben. *der Standard*. Abgerufen am 17. Mai 2021 von https://www.derstandard.at/story/2000126601248/land-der-muenzen-land-der-scheine-warum-oesterreicher-bargeld-lieben

Härtel, U. (2015). Emnid Umfrage: Viele Deutsche misstrauen Online Banking – mehr Schutz und Informationen helfen. *IT-Finanzmagazin*. Abgerufen am 19. Mai 2021 von https://www.it-finanzmagazin.de/emnid-umfrage-viele-deutsche-misstrauen-online-banking-mehr-schutz-und-informationen-helfen-22097/

Kowalcze, K. (2021). Rekordstände bei Bargeld. *die Presse*. Abgerufen am 17. Mai 2021 von https://www.diepresse.com/5955885/rekordstande-bei-bargeld

Strauß, K. (18. Mai 2020). *Mit Sicherheit kontaktlos bezahlen*. Abgerufen am 21. Mai 2021 von Datenschutzexperte.de: https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/mit-sicherheit-kontaktlos-bezahlen/

Verbraucherzentrale. (2018). *Mobiles Bezahlen: Wie sicher ist das?* Berlin. Abgerufen am 05. Mai 2021 von https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/mobiles-bezahlen-wie-sicher-ist-das-32515#:~:text=Kurz%20gesagt%3A%20Bringt%20man%20dem,gesch%C3%BCtzt%20als%20mit%20der%20Plastikkarte.&text=Wollen%20Sie%20das%20Mobile%20Beza

KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien
T +43-(0)5 77 0 77-DW oder -0
F +43-(0)5 77 0 77-1186
E-Mail kfv@kfv.at
www.kfv.at

Medieninhaber und Herausgeber: Kuratorium für Verkehrssicherheit
Verlagsort: Wien
Herstellung: Eigendruck
Redaktion: Mag. Andrea Feymann
Grafik: Patricia Jeßner, BA
Fotos: iStock

SAFETY FIRST!