Erläuterungen:

I. Allgemeiner Teil

Die vorgeschlagenen Änderungen des Strafgesetzbuchs und des Zahlungsdienstegesetzes 2018 beinhalten vor allem Anpassungen, die sich in Umsetzung der Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates, ABl. Nr. L 123 vom 10.05.2019 S. 18, ergeben. Zentraler Zweck der Richtlinie (EU) 2019/713 ist die wirksame Vereinheitlichung der strafrechtlichen Ahndung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln in allen Mitgliedstaaten. Dazu braucht es in erster Linie einheitliche Definitionen, die durch die Umsetzung der Richtlinie (EU) 2019/713 geschaffen werden sollen.

Die Richtlinie (EU) 2019/713 löst im Bereich des gerichtlichen Strafrechts lediglich einen geringen Änderungsbedarf aus, weil die Grundlagen bereits mit dem Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl. L 149 vom 2.6.2001 S. 1, geschaffen wurden. Die gegenständlichen Änderungen bzw. Ergänzungen erfolgen zur Vereinheitlichung der Definitionen und Anpassung an moderne Instrumente, wie etwa virtuelle Währungen. Überdies soll durch die teilweise Anhebung der Strafdrohungen bzw. die Schaffung von Qualifikationstatbeständen die Ahndung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln im Einklang mit den Vorgaben von Art. 9 der Richtlinie (EU) 2019/713 sichergestellt werden.

Die Richtlinie (EU) 2019/713 ist bis 31. Mai 2021 umzusetzen.

Zudem enthält der vorliegende Entwurf gesetzliche Begleitmaßnahmen im Zusammenhang mit der Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl. Nr. L 337 vom 23.12.2015 S. 35, in der Fassung der Berichtigung, ABl. Nr. L 169 vom 28.06.2016 S. 18.

Gemäß Art. 103 der Richtlinie (EU) 2015/2366 haben die Mitgliedstaaten geeignete Verwaltungssanktionen festzulegen, die bei Zuwiderhandlungen gegen die die zur Umsetzung der Richtlinie erlassenen Vorschriften zu verhängen sind. Der Vollständigkeit halber sieht der gegenständliche Entwurf Sanktionsbestimmungen für den Zugang zu Zahlungssystemen vor.

Die überwiegende Zahl der gesetzlichen Bestimmungen zur Umsetzung der Richtlinie (EU) 2015/2366 sind mit 1. Juni 2018 in Kraft getreten.

Die gesetzlichen Bestimmungen des gegenständlichen Entwurfs sollen mit dem der Kundmachung folgenden Tag in Kraft treten.

Kompetenzgrundlage:

Der vorliegende Entwurf stützt sich auf Art. 10 Abs. 1 Z 5 und 6 B-VG (Geld-, Kredit-, Börse- und Bankwesen sowie Strafrechtswesen).

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Der Entwurf dient der Umsetzung von Unionsrecht, nämlich der Richtlinie (EU) 2019/713 sowie der Richtlinie (EU) 2015/2366.

II. Besonderer Teil

Zu Artikel 1 (Änderungen des StGB)

Zu Z 1 (§ 74 Abs. 1 Z 10 StGB):

Die vorgeschlagene Definition der unbaren Zahlungsmittel ergibt sich aus einer Kombination des Richtlinienwortlauts von Art. 2 lit. a und Art. 2 lit. b der Richtlinie (EU) 2019/713. Die bis dato geltende Rechtslage entspricht der Definition des Rahmenbeschlusses 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl. Nr. L 149 vom 2.6.2001, S. 1. Diese deckte körperliche unbare Zahlungsmittel ab. Die erweiterte Definition soll vor allem auch unkörperliche unbare Zahlungsmittel, einschließlich digitaler Zahlungsmittel, mitabdecken. Die von der Definition erfassten Vorrichtungen, Gegenstände oder Aufzeichnungen müssen vor Fälschung oder

betrügerischer Verwendung geschützt sein. Dies erfolgt iSd Art. 2 lit. b der Richtlinie (EU) 2019/713 z. B. durch das Design, eine Kodierung oder eine Unterschrift.

Ziel der Richtlinie (EU) 2019/713 ist es, auch unkörperliche unbare Zahlungsmittel zu erfassen, wobei ein technologieneutraler Ansatz verfolgt wird (Erwägungsgrund 6). Daher soll vom Abstellen allein auf körperliche Zahlungsmittel in § 74 Abs. 1 Z 10 StGB abgegangen werden.

Aus Erwägungsgrund 8 der Richtlinie (EU) 2019/713 ergibt sich, dass ein unbares Zahlungsmittel aus verschiedenen Elementen bestehen kann, die zusammenwirken, beispielsweise aus einer mobilen Zahlungsanwendung und einer entsprechenden Genehmigung, etwa durch ein Passwort. Ein unbares Zahlungsmittel ist ein Instrument, das es dem Besitzer oder Nutzer ermöglicht, tatsächlich Geld oder monetäre Werte zu übertragen oder einen Zahlungsauftrag zu erteilen. Die widerrechtliche Erlangung einer mobilen Zahlungsanwendung ohne die erforderliche Genehmigung kann in diesem Sinn nicht als widerrechtliche Erlangung eines unbaren Zahlungsinstruments betrachtet werden, da der Nutzer nicht in die Lage versetzt wird, tatsächlich Geld oder monetäre Werte zu übertragen.

Zu den unkörperlichen unbaren Zahlungsmitteln zählen insbesondere Zahlungsinstrumente wie Onlinebanking oder auch intermediäre Zahlungsabwickler, die etwa eine Bezahlung über einen entsprechenden Account zulassen, der in weiterer Folge mit einem Bankkonto oder einer Kreditkarte verknüpft ist.

Durch die Erweiterung der Definition ist auch die Übertragung mittels digitaler Tauschmittel umfasst. Unter „digitalen Tauschmitteln“ versteht Art. 2 lit. c) der Richtlinie (EU) 2019/713 E-Geld im Sinne des Art. 2 Z 2 der Richtlinie 2009/110/EG über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG, ABl. L 267 vom 10.10.2009, S. 7, oder eine virtuelle Währung. Diese Definition soll entsprechend Erwägungsgrund 10 der Richtlinie (EU) 2019/713 dem Umstand Rechnung tragen, dass digitale Brieftaschen für die Übertragung virtueller Währungen die Merkmale eines Zahlungsmittels aufweisen können, aber nicht müssen. Die Definition des Zahlungsmittels wird dadurch nicht erweitert.

E-Geld iSd Art. 2 Z 2 der Richtlinie 2009/110/EG ist jeder elektronisch — darunter auch magnetisch — gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge durchzuführen und der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird.

Eine „virtuelle Währung“ im Sinne des Art. 2 lit. d der Richtlinie (EU) 2019/713 ist eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist, die nicht den rechtlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann. Virtuelle Währungen sollen nur erfasst werden, soweit diese gemeinhin für die Leistung von Zahlungen verwendet werden können (Erwägungsgrund 10 der Richtlinie (EU) 2019/713).

Während nach § 241h StGB etwa Phishing bisher nur in Bezug auf herausgelockte Kartendaten anwendbar war, wird der Anwendungsbereich durch die erweiterte Definition des unbaren Zahlungsmittels auch auf herausgelockte Daten eines unkörperlichen, digitalen Zahlungsmittels erweitert.

Zu Z 2 bis Z 4, Z 8 und Z 9 (§§ 126c, 241c StGB):

Gemäß Art. 7 der Richtlinie (EU) 2019/713 haben Mitgliedstaaten die Vorbereitung von Straftaten im Sinne des Art. 4 lit. a) und b), Art. 5 lit. a) und b) sowie Art. 6 der Richtlinie (EU) 2019/713 zu sanktionieren. Diese Artikel sind durch die §§ 148a, 241a und 241e Abs. 1 StGB umgesetzt. Vorbereitungshandlungen iSd Art. 7 der Richtlinie (EU) 2019/713 hinsichtlich § 148a StGB sind durch § 126c StGB idgF und hinsichtlich § 241a StGB durch § 241c StGB idgF pönalisiert; solche in Bezug auf § 241e Abs. 1 StGB wären – unter den gesetzlichen Voraussetzungen – zum Teil als Beitragstäterschaft zu § 241e Abs. 1 StGB strafbar. Im Hinblick auf eine vollständige Umsetzung des Art. 7 der Richtlinie (EU) 2019/713 ist jedoch eine Erweiterung des § 241c StGB um die Vorbereitung der Entfremdung unbarer Zahlungsmittel nach § 241e Abs. 1 StGB erforderlich.

Für Vorbereitungsdelikte gem. Art. 7 der Richtlinie (EU) 2019/713 sieht Art. 9 Abs. 5 der Richtlinie (EU) 2019/713 eine Mindesthöchststrafe von zwei Jahren vor. Die Strafdrohung des Missbrauchs von Computerprogrammen oder Zugangsdaten in Bezug auf § 148a StGB (§ 126c Abs. 1a StGB) sowie der Vorbereitung der Fälschung und Entfremdung unbarer Zahlungsmittel (§ 241c StGB) war daher entsprechend anzuheben.

Zu Z 5, Z 7, Z 10 und Z 11 (§§ 147, 241b, 241f, 241h StGB):

Die vorgeschlagene Anhebung der Strafdrohungen bzw. die vorgeschlagenen Implementierungen von Qualifikationen für die Begehung als Mitglied einer kriminellen Vereinigung gehen auf Vorgaben der Richtlinie (EU) 2019/713 zurück. Die Implementierung einer Qualifikation für die Begehung als Mitglied einer kriminellen Vereinigung in §§ 147 Abs. 2a, 241b Abs. 2 und 241f Abs. 2 StGB ergibt sich aus Art. 9 Abs. 6 der Richtlinie (EU) 2019/713, korrespondierend soll auch die Strafdrohung in § 241h Abs. 2 StGB für die Begehung als Mitglied einer kriminellen Vereinigung angehoben werden. Ein – wie im Begutachtungsverfahren angeregtes – Abstellen auch auf die Mitwirkung (§ 12 StGB) eines anderen Mitglieds dieser Vereinigung würde den Richtlinienvorgaben, die diese Einschränkung nicht vorsehen, nicht entsprechen.

Die Aufnahme der Tathandlungen „Einfuhr, Ausfuhr und Verbreitung“ in §§ 241b, 241f StGB geht auf die Umsetzungsverpflichtung der Richtlinie (EU) 2019/713 zurück, nämlich auf Art. 4 lit. d). Wiewohl als Beispiel einer Verbreitung lediglich der Verkauf von Kreditkarteninformationen im Internet genannt wird (vgl. Erwägungsgrund 13 der Richtlinie (EU) 2019/713), der wohl von der bestehenden Tathandlung des Überlassens gedeckt wäre (vgl. *Tipold* in Leukauf/Steininger, StGB[4] § 241b Rz 4, der von „einvernehmlicher Übertragung an einen anderen“ spricht), ist der Begriff der Verbreitung doch insgesamt weiter als jener des Überlassens, sodass zur vollständigen RL-Umsetzung die Aufnahme auch dieser Tathandlung erfolgen soll.

Des Weiteren soll in Umsetzung von Art. 5 lit. d) der Richtlinie (EU) 2019/713 auch die Tathandlung des Bereitstellens in §§ 241b, 241f StGB ergänzt werden. Bereitstellen bedeutet, dass der Täter einem Dritten eine jederzeit effektuierbare zumindest faktische Verfügungsmacht über das falsche oder verfälschte bzw. entfremdete unbare Zahlungsmittel einräumt (vgl. hierzu *Plöchl* in Höpfel/Ratz, WK[2] StGB § 278 Rz 38 und § 278d Rz 38).

Die vorgesehene umfassende Definition des „unbaren Zahlungsmittels“ nach § 74 Abs. 1 Z 10 StGB, die sowohl körperliche als auch unkörperliche Zahlungsmittel erfasst, bringt es mit sich, dass bestimmte Tathandlungen nur in Bezug auf bestimmte Zahlungsmittel in Betracht kommen werden (idS nennt auch nur der körperliche unbare Zahlungsinstrumente betreffende Art. 4 lit. a) der Richtlinie (EU) 2019/713 die „Einfuhr und Ausfuhr“, nicht jedoch der korrespondierende Art. 5 lit. a) der Richtlinie (EU) 2019/713 in Bezug auf unbare Zahlungsmittel, während das „Bereitstellen“ nur in Art. 5 lit. d) der Richtlinie (EU) 2019/713 angesprochen ist).

Weiters erachtet die Richtlinie (EU) 2019/713 auch den bloßen Besitz, die Beschaffung oder die Verbreitung von Zahlungsinstrumenten, ohne dass eine tatsächliche betrügerische Verwendung von unbaren Zahlungsmitteln gegeben sein muss, als strafwürdig (Erwägungsgrund 13 der Richtlinie (EU) 2019/713). Dies ist anhand der geltenden Rechtslage in §§ 241e Abs. 1, 241f StGB bereits gewährleistet.

Wesentlich ist laut Erwägungsgrund 15 der Richtlinie (EU) 2019/713 auch die Strafbarkeit der Beschaffung eines widerrechtlich erlangten Zahlungsmittels zwecks betrügerischer Verwendung ohne der Notwendigkeit Feststellungen zu allen tatsächlichen Umständen der widerrechtlichen Erlangung treffen zu können. Dabei soll es auch nicht auf eine frühere oder gleichzeitige Verurteilung wegen der Vortat, die zu der widerrechtlichen Erlangung geführt hat, ankommen. Auch dieser Erleichterung der Praxis kommt die geltende Rechtslage durch § 241f bereits nach. Denn § 241f StGB kriminalisiert „nur die Aufrechterhaltung einer rechtswidrigen Gewahrsamsverschiebung“ mit entsprechendem vorgelagerten Bereicherungsvorsatz. (*Schroll* in *Höpfel/Ratz*, WK[2] StGB § 241f StGB Rz 2/1). Die Feststellung der Umstände der widerrechtlichen Erlangung ist daher – richtlinienkonform – nicht notwendig.

Nach Erwägungsgrund 11 der Richtlinie (EU) 2019/713 soll der Versand gefälschter Rechnungen um Zahlungsdaten zu erhalten, als Versuch einer rechtswidrigen Aneignung im Sinne dieser Richtlinie angesehen werden. Soweit nicht ohnehin eine Strafbarkeit nach (§ 15 iVm) §§ 241c, 241e oder § 241f StGB vorliegt, kommt eine Subsumtion unter § 241h StGB in Betracht. Wer Daten eines unbaren Zahlungsmittels mit entsprechendem Vorsatz ausspäht, macht sich nach § 241h StGB strafbar. Die bloße Versendung einer gefälschten Rechnung, die zu einer Überweisung durch den Empfänger führt, wird zwar in der Regel nicht zum Erfolg führen. Nach der Rechtsprechung ist allerdings auch der Versuch einer Geldbehebung mittels entfremdeter Bankomatkarte ohne Kenntnis der Codezahl keineswegs absolut untauglich, weil die Erfolgschance einer rechtswidrigen automatischen Geldentnahme nur minimiert, nicht aber gänzlich beseitigt ist (vgl. 12 Os 113/91). Damit kann je nach Sachverhalt beim Versenden von gefälschten Rechnungen zur Erlangung von Zahlungsdaten Strafbarkeit nach §§ 15, 241h StGB vorliegen.

Zu Z 6 (§ 148a StGB):

Eine Strafbarkeit verlangt Art. 6 lit. a) der Richtlinie (EU) 2019/713 für das vorsätzliche Durchführen oder Veranlassen einer Übertragung von Geld, monetären Werten oder virtueller Währung, durch das

einer anderen Person ein unrechtmäßiger Vermögensverlust entsteht, mit der Absicht, dem Zuwiderhandelnden oder einem Dritten einen unrechtmäßigen Vermögensvorteil zu verschaffen, wenn das Funktionieren eines Informationssystems unrechtmäßig behindert oder gestört wird.

§ 126b Abs. 1 StGB regelt die schwere Störung der Funktionsfähigkeit eines Computersystems durch Eingabe oder Übermittlung von Daten. § 126b Abs. 1 StGB erfordert jedoch keine vermögensrechtliche Komponente, insb. keinen Bereicherungsvorsatz. § 148a StGB, der zwar einen Bereicherungsvorsatz fordert, stellt nicht ausdrücklich auf das Behindern oder Stören eines Informationssystems ab. § 148a Abs. 1 StGB fordert jedoch, dass das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorganges beeinflusst wird. Es war daher zu erwägen, ob die in § 148a Abs. 1 StGB umschriebenen Tathandlungen im Ergebnis auch als Behinderung oder Störung eines Informationssystems zu werten sind. Die Definition des Informationssystems nach Art. 2 lit. e) der Richtlinie (EU) 2019/713) verweist auf Art. 2 lit. b) der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. L 218 vom 14.8.2013, S. 8. Ein Informationssystem ist demnach eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten. Informationssysteme in diesem Sinn sind von der Definition des Computersystems nach § 74 Abs. 1 Z 8 StGB erfasst.

Darauf aufbauend kann festgestellt werden, dass eine Störung eines Computersystems grundsätzlich den Wert des Computersystems herabsetzt. Eine solche Störung liegt im Falle eines Rechners dann vor, wenn ein „gesamter Rechner oder einzelne darauf laufende Dienste durch die vom Täter eingegebenen oder übermittelten Daten blockiert werden“. Gestört ist die Funktionalität aber auch schon dann, wenn die auf dem PC ablaufenden Dienste erheblich verlangsamt werden (*Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB § 126b StGB Rz 10). Unter Stören versteht man gemeinhin einen gewünschten oder herkömmlichen Zustand zu unterbrechen. Wenn also § 148a StGB davon spricht, dass das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsprozesses beeinflusst wird, so ist zu erwägen, ob nicht einige der Tathandlungen als Störung des Computersystems gewertet werden können. Nämlich jene bei welchen auf den gewöhnlichen Prozess eines Programms derart eingewirkt wird, dass die Verarbeitung nicht mehr ordnungsgemäß verläuft, das Computersystem also gestört wird.

Durch die Eingabe, Veränderung oder Löschung von Daten in der Eingabephase wird zwar das Ergebnis einer automationsunterstützten Datenverarbeitung beeinflusst, allerdings wird nicht – zwingend – die Funktionalität des Datenverarbeitungsprogramms gestört. Denn bei der „Eingabe von Daten wird das Verarbeitungsergebnis insb. dann beeinflusst, wenn es sich um unrichtige oder unvollständige Daten handelt“ (*Kirchbacher/Sadoghi* in *Höpfel/Ratz,* WK^2 StGB § 148a StGB Rz 16). Bei der Programm- und Konsolen-Manipulation geschieht hingegen eine Beeinflussung des Datenverarbeitungsergebnisses in der Verarbeitungsphase (§ 148a Abs. 1 erster und dritter Fall StGB). In Betracht kommen Manipulationen am Programm selbst (gleich ob von vornherein oder später, zB durch Hinzufügen, Verändern oder Ausschalten von Verarbeitungsschritten) und an dessen Ablauf (*Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK^2 StGB § 148a StGB Rz 21). Bei der Output-Manipulation (§ 148a Abs. 1 dritter Fall StGB) wird ebenso das Ergebnis der Datenverarbeitung beeinflusst (*Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK^2 StGB § 148a StGB Rz 22). Da daher sowohl bei der Programm- und Konsolenmanipulation als auch bei der Output-Manipulation auf den Verarbeitungsprozess an sich eingewirkt wird, kann in diesen Fällen von einer Störung des Computersystems gesprochen werden.

In diesem Sinne ist daher davon auszugehen, dass § 148a Abs. 1 erster und dritter Fall StGB, also die Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms oder sonst durch Einwirkung auf den Ablauf der Verarbeitungsprogramms, für gewöhnlich eine Störung eines Computersystems in sich birgt, sodass eine Änderung von § 126b Abs. 1 StGB oder von § 148a Abs. 1 StGB nicht erforderlich war um Art. 6 lit. a) der Richtlinie (EU) 2019/713 umzusetzen. Denn das vorsätzliche Durchführen oder Veranlassen einer Übertragung von Geld, monetären Werten oder virtueller Währung, durch das einer anderen Person ein unrechtmäßiger Vermögensverlust entsteht, mit der Absicht, dem Zuwiderhandelnden oder einem Dritten einen unrechtmäßigen Vermögensvorteil zu verschaffen, wenn das Funktionieren eines Informationssystems unrechtmäßig behindert oder gestört wird, ist unter § 148a StGB subsumierbar.

Im Begutachtungsverfahren wurde jedoch Kritik an der vorgeschlagenen Anhebung der Grundstrafdrohung in § 148a Abs. 1 StGB auf drei Jahre Freiheitsstrafe geäußert, dies vor allem im

Hinblick auf einen Wertungswiderspruch zu § 146 StGB. Des Weiteren wurde aufgezeigt, dass es für eine Strafbarkeit nach § 148a StGB bereits genügt, wenn der Vermögensschaden als unmittelbare Folge der Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung eintritt (vgl. RIS-Justiz RS 0094395; *Kirchbacher/Sadoghi* in WK StGB^2 § 148a Rz 11,16 und 31f). So seien etwa Fälle eines „Bestellbetrugs“ bei welchen im Zuge rein automationsunterstützter Online-Bestellungen vom zahlungsunwilligen Täter die eigenen Daten richtig eingegeben werden, von § 148a StGB erfasst, während die von der Richtlinie (EU) 2019/713 in Art. 6 lit. a) und lit. b) geforderte Unrechtmäßigkeit der Beeinflussung eines Informationssystems nicht gegeben sei. Die entsprechende Verpflichtung einer Mindeshöchststrafe von drei Jahren Freiheitsstrafe aus Art. 9 Abs. 4 der Richtlinie (EU) 2019/713 bezieht sich nur auf die in Art. 6 lit. a) und lit. b) genannten Fälle der *unrechtmäßigen* Behinderung oder Störung des Funktionierens eines Computersystems bzw. der *unrechtmäßigen* Eingabe, Veränderung, Löschung, Übertragung oder Unterdrückung von Computerdaten.

Diese Argumentation aufgreifend wird nunmehr vorgeschlagen, das Grunddelikt des § 148a Abs. 1 StGB – mit Ausnahme der Aufnahme der weiteren Tathandlung des „Übertragens“ (siehe dazu sogleich) – und die Qualifikation des Abs. 2 unverändert zu lassen sowie in weiterer Folge in Umsetzung von Art. 6 lit. a) und lit. b) iVm Art. 9 Abs. 4 der Richtlinie (EU) 2019/713 in einem neuen Abs. 3 festzulegen, dass mit Freiheitsstrafe bis zu drei Jahren zu bestrafen ist, wer die Tat begeht, indem er Daten *unrechtmäßig* eingibt, verändert, löscht, unterdrückt oder überträgt oder die Funktionsfähigkeit eines Computersystems *unrechtmäßig* behindert oder stört.

Nach den Erläuternden Bemerkungen anlässlich der Einführung des § 148a StGB mit dem Strafrechtsänderungsgesetz 1987, BGBl. Nr. 605/1987, wurde bewusst darauf verzichtet, die Verwendung unrichtiger oder unvollständiger Daten bzw. die unrichtige Gestaltung von Programmen in den Tatbestand aufzunehmen. Das Unrechtmäßige der Tathandlungen ergebe sich bereits durch den notwendigen Vorsatz auf unrechtmäßige Bereicherung (JAB 359 BlgNR 17. GP, S. 15 ff). Demnach erfasst der Wortlaut des § 148a Abs. 1 StGB – anders als etwa der Straftatbestand des Computerbetrugs nach § 263a des deutschen StGB – auch die Verwendung richtiger und vollständiger Daten (*Komenda/Mandl* in Sbg Kommentar zum StGB § 148a StGB Rz 16, 25 mwN; *Kirchbacher/Sadoghi* in WK StGB^2 § 148a Rz 11,16 und 31f). Angesichts der Vorgabe der Richtlinie (EU) 2019/713, die Strafdrohung (nur) in Bezug auf unrechtmäßige Tathandlungen auf mindestens drei Jahre Freiheitsstrafe zu erhöhen, soll nunmehr dennoch eine Differenzierung erfolgen.

Ob die Eingabe, Veränderung, Löschung, Unterdrückung oder Übertragung der Daten bzw. die Behinderung oder Störung der Funktionsfähigkeit eines Computersystems unrechtmäßig iSd vorgeschlagenen Abs. 3 erfolgte, wird im Einzelfall zu beurteilen sein. Zentral wird hierbei die Frage der Berechtigung zur dieser Handlung sein. So erfolgt die Eingabe von fremden Kreditkartendaten im Zuge eines Online-Bestellvorganges ohne Erlaubnis der befugten Person unrechtmäßig. Ebenso wird die Störung eines Computersystems durch eine Person, die über das Computersystem nicht oder nicht allein verfügen darf, unrechtmäßig sein. Bei einer Störung oder Behinderung der Funktionsfähigkeit eines Computersystems durch einen „freundlichen“ Hackangriff im Auftrag des (allein) Verfügungsberechtigten, durch den lediglich Sicherheitslücken aufgezeigt werden sollen, wird keine Unrechtmäßigkeit vorliegen. Zudem scheidet in einem solchen Fall eine Strafbarkeit bereits mangels Bereicherungsvorsatz und Vermögensschädigung aus. In den Konstellationen der Verwendung richtiger und vollständiger Daten wird in der Regel nicht davon auszugehen sein, dass die Eingabe der Daten unrechtmäßig erfolgte.

Die Aufnahme einer weiteren Tathandlung, nämlich jener des Übertragens, geschieht in Umsetzung von Art. 6 lit. b) der Richtlinie (EU) 2019/713, wobei aus systematischen Erwägungen bereits das Grunddelikt in Abs. 1 um diese Tathandlung erweitert werden soll.

Die Implementierung einer Qualifikation für die Begehung als Mitglied einer kriminellen Vereinigung geht auf Art. 9 Abs. 6 der Richtlinie (EU) 2019/713 zurück.

Zu Art. 2 (Änderung des Zahlungsdienstegesetzes 2018)

Zu § 86 Abs. 2 Satz 3:

Laut Art. 15 (unter Berücksichtigung von Erwägungsgrund 25) der Richtlinie (EU) 2019/713 sollen geeignete Meldekanäle zur Meldung von mutmaßlichen Straftaten im Zusammenhang mit unbaren Zahlungsmitteln, die schwerwiegende Betriebs- oder Sicherheitsvorfälle im Sinne der Richtlinie (EU) 2015/2366 darstellen können, an die Strafverfolgungsbehörden zur Verfügung stehen. Der unionsrechtlich vorgeschriebene Meldeweg ist bereits von der geltenden gesetzlichen Regelung in § 86 Abs. 2 ZaDiG 2018 gedeckt. Die FMA hat die Relevanz eines vom Zahlungsdienstleister gemeldeten Betriebs- und Sicherheitsvorfalls für andere maßgebliche Behörden der Union zu prüfen und diese im

Wege der Amts- bzw. Rechtshilfe durch Weiterleitung der Meldung entsprechend zu informieren. Durch die Einfügung der Wortfolge „einschließlich der Strafverfolgungsbehörden“ in § 86 Abs. 2 Satz 3 ZaDiG 2018 kommt es zu keiner materiellen Erweiterung der bestehenden Prüf- oder Berichtspflicht der FMA. Vielmehr soll die Klarstellung der Umsetzung des Art. 15 der Richtlinie (EU) 2019/713 dienen und im Sinne der Effizienz bestehende Systeme genutzt werden.

Zu § 99 Abs. 5:

Gemäß § 5 Abs. 1 sollen unmittelbar und mittelbar diskriminierende Praktiken von Betreibern von Zahlungssystemen unterbunden werden. Beispielsweise darf Zahlungsdienstleistern, Zahlungsdienstnutzern und anderen Zahlungssystemen der Beitritt oder die Teilnahme an anderen Zahlungssystemen nicht erschwert werden. Darüber hinaus sollen zugelassene oder registrierte Zahlungsdienstleister als Teilnehmer von Zahlungssystem nicht ohne sachlich gerechtfertigten Grund unterschiedlich behandelt werden. Letztlich sollen Beschränkungen für Zahlungsdienstleister, Zahlungsdienstnutzer oder anderen Zahlungssystemen aufgrund des institutionellen Status verhindert werden. Zudem sind Betreiber von Zahlungssystemen im Interesse der Finanzmarktstabilität und der Zahlungssystemsicherheit verpflichtet bestimmte Kriterien und Risiken gemäß § 5 Abs. 2 zu berücksichtigen, wenn sie Zahlungsdienstleistern Zugang zu Zahlungssystemen gewähren. In diesem Zusammenhang setzt Abs. 5 Art. 103 Abs. 1 der Richtlinie (EU) 2015/2366 um und normiert Sanktionen für ein Zuwiderhandeln.

Zu § 105 Abs. 1:

Hiermit soll es der FMA gemäß Art. 103 Abs. 2 der Richtlinie (EU) 2015/2366 auch in Bezug auf § 99 Abs. 5 erlaubt sein, Verwaltungssanktionen bekanntzumachen, sofern dies die Stabilität der Finanzmärkte nicht ernstlich gefährdet oder den Beteiligten unverhältnismäßigen Schaden zufügt.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-10-13T12:21:02+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	