Rat der
Europäischen Union

Brüssel, den 11. Juli 2023
(OR. en)

11761/23

CYBER 184
DROIPEN 107
IA 180
JAI 998
MI 607
TELECOM 229

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	10. Juli 2023
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2023) 363 final
Betr.:	BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT zur Bewertung, inwieweit die Mitgliedstaaten die erforderlichen Maßnahmen zur Einhaltung 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 ergriffen haben

Die Delegationen erhalten in der Anlage das Dokument COM(2023) 363 final.

Anl.: COM(2023) 363 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 10.7.2023
COM(2023) 363 final

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

zur Bewertung, inwieweit die Mitgliedstaaten die erforderlichen Maßnahmen zur Einhaltung 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 ergriffen haben

1. Einleitung

Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln wie Kredit- oder Zahlungskarten sind eine Einnahmequelle des organisierten Verbrechens und dienen zur Finanzierung anderer krimineller Aktivitäten wie Terrorismus, Drogen- und Menschenhandel. Diese Straftaten verursachen erhebliche Verluste: Der Gesamtwert der betrügerischen Geschäfte mit im Europäischen Zahlungsverkehrsraum (SEPA) ausgegebenen Karten belief sich im Jahr 2019 auf 1,87 Milliarden EUR.[1] Die überwiegende Mehrheit der betrügerischen Geschäfte steht im Zusammenhang mit Betrug, bei dem die Karte physisch nicht vorhanden ist (card-not-present, CNP): Im Jahr 2019 entfielen 80 % des Werts des Kartenbetrugs auf CNP-Geschäfte, d. h. Zahlungen via Internet, Post oder Telefon.[2] Die Verluste durch CNP-Betrug beliefen sich im Jahr 2019 auf 1,50 Mrd. EUR, was einem Anstieg um 4,3 % gegenüber dem Vorjahr entspricht.[3]

Es besteht eindeutig eine grenzüberschreitende Dimension: Mehr als die Hälfte des Gesamtwerts des Betrugs im Jahr 2019 betraf grenzüberschreitende Geschäfte innerhalb des Europäischen Zahlungsverkehrsraums. Was die geografische Verteilung angeht, so machten im Jahr 2019 inländische Geschäfte 89 % des Werts aller Kartentransaktionen aus, aber nur 35 % der betrügerischen Geschäfte. Grenzüberschreitende Geschäfte innerhalb des SEPA machten wertmäßig 9 % aller Kartentransaktionen aus, jedoch 51 % der gemeldeten Betrugsfälle.[4]

Um diese Straftaten wirksam zu bekämpfen, müssen die Mitgliedstaaten gemeinsam definieren, welche Handlungen als Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln zu erachten sind. Sie müssen ferner Art und Umfang ihrer Sanktionen angleichen und über entsprechende operative Mittel verfügen, um Straftaten melden und Informationen zwischen Behörden austauschen zu können. Vor diesem Hintergrund haben das Europäische Parlament und der Rat am 17. April 2019 die Richtlinie (EU) 2019/713 (im Folgenden „Richtlinie“) zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates erlassen.[5] Mit diesem Bericht wird der Anforderung gemäß Artikel 21 der Richtlinie entsprochen.

1.1. Ziele und Anwendungsbereich der Richtlinie

Zu den Zielen der Richtlinie zählen die Angleichung des Strafrechts der Mitgliedstaaten[6] im Bereich des Betrugs und der Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und

---

[1] Europäische Zentralbank, Seventh report on card fraud (Siebter Bericht über Kartenbetrug), abrufbar unter: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html.

[2] Ebenda.

[3] Ebenda.

[4] Ebenda.

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019L0713&lang1=DE&from=EN&lang3=choose&lang2=DE&_csrf=936ca0cc-00e2-485c-8fa6-2c2ac621be21

[6] Sofern nicht ausdrücklich etwas anderes angegeben ist, bezieht sich im Folgenden der Begriff „Mitgliedstaaten“ oder „alle Mitgliedstaaten“ auf die Mitgliedstaaten, die durch die Richtlinie gebunden sind, d. h. auf alle Mitgliedstaaten mit Ausnahme Dänemarks und Irlands, die sich nach dem Protokoll über die Position Dänemarks, das dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der

die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden. Zu diesem Zweck werden in der Richtlinie Mindestvorschriften zur Definition von Straftaten und die Festlegung einschlägiger Strafen festgelegt. Der Geltungsbereich der Richtlinie ist weit gefasst und deckt gemäß „nichtkörperliche oder körperliche geschützte Vorrichtungen, geschützte Gegenstände oder geschützte Aufzeichnungen oder deren Kombination, ausgenommen gesetzliche Zahlungsmittel, die beziehungsweise der für sich oder in Verbindung mit einem oder mehreren Verfahren dem Inhaber oder Nutzer ermöglicht, Geld oder monetäre Werte zu übertragen, auch mittels digitaler Tauschmittel“ ab (Artikel 2 Buchstabe a).[7] So würde beispielsweise eine mobile Zahlungsanwendung in Verbindung mit dem Genehmigungsverfahren (z. B. PIN) unter diese Definition fallen. Die Richtlinie deckt gemäß Artikel 2 Buchstabe d und Artikel 6 auch virtuelle Währungen ab.

In der Richtlinie werden spezifische Straftaten definiert, insbesondere:

- betrügerische Verwendung von unbaren Zahlungsinstrumenten (Artikel 3),
- Straftaten im Zusammenhang mit der betrügerischen Verwendung körperlicher unbarer Zahlungsinstrumente (Artikel 4),
- Straftaten im Zusammenhang mit der betrügerischen Verwendung nichtkörperlicher unbarer Zahlungsinstrumente (Artikel 5),
- Betrug im Zusammenhang mit Informationssystemen (Artikel 6),
- rechtswidrige Bereitstellung von Tatwerkzeugen zur Begehung der genannten Straftaten (Artikel 7).

Darüber hinaus weitet die Richtlinie die **strafrechtliche Verantwortung** auf die Anstiftung und Beihilfe zur Begehung einer der oben genannten Straftaten sowie auf den Versuch zur Begehung dieser Straftaten seitens einer natürlichen und/oder juristischen Person aus (Artikel 8).

Artikel 9 macht Mindestvorgaben hinsichtlich der **Höchststrafen** für die Straftaten im Sinne der Richtlinie.

Die darauffolgenden Artikel machen Mindestvorgaben in Bezug auf die **Verantwortlichkeit juristischer Personen** (Artikel 10) und Sanktionen, zu denen Geldstrafen oder Geldbußen gehören, und listen Beispiele für sonstige Sanktionen gegen diese Personen auf (Artikel 11).

Mit Artikel 12 soll sichergestellt werden, dass die in der Richtlinie genannten Straftäter wegen der Straftaten nach den Artikeln 3 bis 8 der Richtlinie strafrechtlich verfolgt werden. Die **gerichtliche Zuständigkeit** eines Mitgliedstaats muss begründet werden, wenn a) die Straftat ganz oder teilweise in seinem Hoheitsgebiet begangen wurde, und/oder b) es sich beim Straftäter um einen seiner Staatsangehörigen handelt. Mit anderen Worten legt Artikel 12 Absatz 1 Buchstabe a der Richtlinie das Territorialitätsprinzip fest, während Buchstabe b auf den Grundsatz der aktiven Staatsangehörigkeit verweist.

Gemäß Artikel 13 Absatz 1 der Richtlinie müssen **Ermittlungsinstrumente** für die Ermittlung und die strafrechtliche Verfolgung von Straftaten nach den Artikeln 3 bis 8 wirksam und verhältnismäßig sein und den zuständigen Personen, Stellen und Diensten zur

---

Europäischen Union (AEUV) beigefügt ist, bzw. gemäß dem Protokoll Nr. 21 über die Position des Vereinigten Königreichs und Irlands nicht an der Annahme der Richtlinie beteiligen.

[7] Bei allen genannten Artikeln handelt es sich um Artikel der Richtlinie, sofern nichts anderes angegeben ist.

Verfügung stehen. Informationen zu den in den Artikeln 3 bis 8 genannten Straftaten sollten gemäß Artikel 13 Absatz 2 der Richtlinie die Behörden, die mit der Ermittlung oder strafrechtlichen Verfolgung dieser Straftaten befasst sind, unverzüglich erreichen.

Was den Informationsaustausch betrifft, müssen Mitgliedstaaten laut Artikel 14 sicherstellen, dass sie über operative nationale **Kontaktstellen** verfügen, die sieben Tage pro Woche 24 Stunden täglich zur Verfügung stehen, damit sie in der Lage sind, bei dringenden Ersuchen ausländischer Behörden binnen acht Stunden zu reagieren.

Darüber hinaus sind die Mitgliedstaaten nach Artikel 15 Absatz 1 der Richtlinie verpflichtet, geeignete Meldekanäle einzurichten, damit die **Meldung von Straftaten** im Sinne von Artikel 3 bis 8 an die Behörden unverzüglich erfolgen kann. Insbesondere werden Finanzinstitute aufgefordert, den Strafverfolgungs- und Justizbehörden mutmaßliche Betrugsfälle zu melden (Artikel 15 Absatz 2). Die Meldung ist häufig der Ausgangspunkt für strafrechtliche Ermittlungen (Erwägungsgrund 27).

Schließlich befassen sich die Artikel 16 und 17 der Richtlinie mit **Hilfe und Unterstützung für Opfer** bzw. mit **Prävention**.

1.2 Zweck und Methodik dieses Berichts

Nach Artikel 20 müssen die Mitgliedstaaten die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft setzen, um der Richtlinie bis zum 31. Mai 2021 nachzukommen, und der Kommission den Wortlaut der Maßnahmen übermitteln.

Mit diesem Bericht erfüllt die Kommission ihre Verpflichtung aus Artikel 21 der Richtlinie, dem Europäischen Parlament und dem Rat einen Bericht darüber vorzulegen, inwieweit die Mitgliedstaaten die zur Einhaltung der Richtlinie erforderlichen Maßnahmen ergriffen haben. Der Bericht – der erste Bericht gemäß Artikel 21 – gibt einen Überblick über die wichtigsten Umsetzungsmaßnahmen, die von den Mitgliedstaaten ergriffen wurden.

Im Zuge der Umsetzung der Richtlinie in den Mitgliedstaaten mussten Informationen über die einschlägigen Rechtsvorschriften und Verwaltungsmaßnahmen erhoben und analysiert sowie neue Rechtsvorschriften oder – in den meisten Fällen – Änderungsrechtsakte erarbeitet, bis zu ihrer Verabschiedung weiterverfolgt und schließlich der Kommission mitgeteilt werden.

Bis zum Ablauf der Umsetzungsfrist (31. Mai 2021) hatten 9 Mitgliedstaaten die Kommission über die vollständige Umsetzung der Richtlinie unterrichtet und ihre Umsetzungsmaßnahmen mitgeteilt. Im Juli 2021 leitete die Kommission gegen die übrigen 16 Mitgliedstaaten Vertragsverletzungsverfahren wegen Nichtmitteilung nationaler Umsetzungsmaßnahmen ein: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO und SI.[8] Inzwischen haben 15 Mitgliedstaaten ihre Umsetzungsmaßnahmen mitgeteilt. Stand 30. April 2023 ist ein Vertragsverletzungsverfahren wegen Nichtmitteilung nationaler Umsetzungsmaßnahmen gegen BG noch anhängig.[9]

[8] Die diesem Bericht verwendeten Länderkürzel richten sich nach den folgenden Vorgaben: http://publications.europa.eu/code/de/de-5000600.htm.

[9] Informationen über die Beschlüsse der Kommission in Bezug auf Vertragsverletzungsverfahren können abgerufen werden unter: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=de.

Die nachfolgenden Beschreibungen und Analysen in diesem Bericht basieren auf den Informationen über nationale Umsetzungsmaßnahmen, die von den Mitgliedstaaten bis zum 31. Januar 2023 vorgelegt wurden. Die nach diesem Tag eingegangenen Mitteilungen wurden nicht berücksichtigt. Dagegen wurden alle Maßnahmen berücksichtigt, die zu nationalen Rechtsvorschriften und Gerichtsentscheidungen sowie – gegebenenfalls – zur allgemein anerkannten Rechtstheorie mitgeteilt wurden. Darüber hinaus hat die Kommission die Mitgliedstaaten im Zuge der Analyse direkt kontaktiert, sofern zusätzliche Informationen oder Klarstellungen angemessen schienen. Alle Informationen, die zusammengetragen wurden, wurden in die Analyse einbezogen.

Infolgedessen ist es möglich, dass in diesem Bericht weitere Probleme bei der Umsetzung und andere Bestimmungen, die der Kommission nicht mitgeteilt wurden, sowie weitere legislative und nicht legislative Entwicklungen nicht erfasst sind. Daher behält sich die Kommission vor, ungeachtet dieses Berichts einige Bestimmungen weiter zu evaluieren und die Mitgliedstaaten auch weiterhin bei der Umsetzung der Richtlinie zu unterstützen.

2. Umsetzungsmaßnahmen

2.1 Begriffsbestimmungen

Artikel 2 enthält die Definitionen der wichtigsten Begriffe, die in der Richtlinie verwendet werden, nämlich: unbares Zahlungsinstrument, geschützte Vorrichtung, geschützter Gegenstand oder geschützte Aufzeichnung, digitales Tauschmittel, virtuelle Währung, Informationssystem, Computerdaten, juristische Person.

Die Mitgliedstaaten haben die Begriffsbestimmungen im Allgemeinen umgesetzt, indem sie sich auf Rechtsvorschriften stützen, die vor oder nach dem Inkrafttreten der Richtlinie erlassen wurden. In einigen Fällen gibt es zwar keine Bestimmungen, die Definitionen enthalten, doch sind die Straftaten durch allgemeine Bestimmungen des Strafgesetzbuchs abgedeckt, die einen breiteren Anwendungsbereich haben, z. B. Bestimmungen über Diebstahl. Die Nichtmitteilung einer wörtlichen Umsetzung der Definition bedeutet daher nicht notwendigerweise die unvollständige Umsetzung oder die Nichteinhaltung.

Darüber hinaus verweisen mehrere der Begriffsbestimmungen auf in anderen Richtlinien erläuterte Begriffsbestimmungen.

a) Unbare Zahlungsinstrumente

Bei der Bewertung wurde mindestens ein Fall unvollständiger Umsetzung festgestellt, da die Definition im Rahmenbeschluss 2001/413/JI des Rates nicht aktualisiert worden war. Dieser betrifft daher nur körperliche Zahlungsinstrumente und nicht „geschützte Vorrichtungen, geschützte Gegenstände oder geschützte Aufzeichnungen oder deren Kombination“, wie in der Definition der Richtlinie vorgesehen.

b) Geschützte Vorrichtung, geschützter Gegenstand oder geschützte Aufzeichnung

Mehrere Mitgliedstaaten haben diese Definition nicht umgesetzt (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). Dies gilt nicht unbedingt als Verstoß, da die Bedeutung in der Regel selbsterklärend ist oder aus dem Wortlaut der Definition des Begriffs „unbare Zahlungsinstrumente“ abgeleitet werden kann. In einigen Ländern wird das Konzept in vorbereitenden Arbeiten erläutert.

c) Digitale Tauschmittel und virtuelle Währung

Diese beiden Definitionen sind von zentraler Bedeutung für die Richtlinie (EU) 2019/713, laut deren wichtigstem Ziel der Tatsache Rechnung getragen werden sollte, dass der Rahmenbeschluss 2001/413/JI die aktuellen Gegebenheiten nicht mehr widerspiegelt und nicht ausreichend auf neue Herausforderungen und technologische Entwicklungen wie virtuelle Währungen und mobile Zahlungen eingeht. Diese mussten aufgenommen werden, um eine umfassende Reaktion auf das Phänomen zu gewährleisten und unbeabsichtigte Lücken bezüglich einer Kriminalisierung zu schließen.

Das Hauptproblem bei der Umsetzung ist die Erfassung virtueller Währungen im Sinne von Artikel 2 Buchstabe d der Richtlinie. Während E-Geld in allen Mitgliedstaaten definiert wurde, häufig infolge der Umsetzung der E-Geld-Richtlinie[10], ist die Definition und Erfassung von virtuellem Geld nicht immer einfach.

[10] Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 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).

In HU gelten virtuelle Währungen als Vermögen und elektronische Daten und können Gegenstand der Einziehung von Vermögensgegenständen und der Beschlagnahme sein. In PL ist virtuelle Währung in den Rechtsvorschriften nicht definiert, und es besteht ein gewisses Maß an Unsicherheit darüber, ob sie unter die verschiedenen für die Umsetzung der Richtlinie relevanten Straftaten fallen würde, wenngleich einige Autoren der Ansicht sind, dass virtuelle Währungen unter die Bestimmungen des Strafgesetzbuchs fallen könnten, die Straftaten im Zusammenhang mit Informationen, Datenträgern oder Informationsdaten regeln.

Viele Mitgliedstaaten haben diese Definitionen durch Finanzvorschriften und nicht im Strafrecht umgesetzt (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). Allerdings gibt es nicht in allen diesen Fällen einen Querverweis auf die einschlägigen Bestimmungen in den nationalen Rechtsvorschriften, in denen die Straftaten festgelegt sind. In drei Mitgliedstaaten (IT, MT, RO) wurden beide Definitionen in das Strafgesetzbuch übernommen.

d) Informationssystem

In Artikel 2 Buchstabe e wird „Informationssystem“ als ein Informationssystem im Sinne des Artikels 2 Buchstabe a der Richtlinie 2013/40/EU definiert. Alle Mitgliedstaaten haben die Definition im Einklang mit der Richtlinie umgesetzt.

e) Computerdaten

Computerdaten werden in Artikel 2 Buchstabe f als Computerdaten im Sinne des Artikels 2 Buchstabe b der Richtlinie 2013/40/EU definiert. Alle Mitgliedstaaten haben Artikel 2 Buchstabe f im Einklang mit der Richtlinie umgesetzt.

f) Juristische Person

Schließlich wird in Artikel 2 Buchstabe g der Begriff „juristische Person“ definiert. Fast alle Mitgliedstaaten haben diesen Begriff in ihren Rechtsvorschriften umgesetzt. Die einzige Ausnahme bildet SE, wo der Begriff „juristische Person“ nicht definiert ist. Bei der Umsetzung wird die Bezeichnung „Unternehmen“ verwendet, die dem genannten Begriff am nächsten kommt. Diese Bezeichnung ist weder in einem Rechtstext noch in Rechtslehre oder Rechtsprechung definiert.

2.2 Spezifische Straftaten

a) Betrügerische Verwendung von unbaren Zahlungsinstrumenten

Nach Artikel 3 Buchstabe a der Richtlinie treffen die Mitgliedstaaten die erforderlichen Maßnahmen, um sicherzustellen, dass die vorsätzliche betrügerische Verwendung gestohlener oder anderweitig widerrechtlich angeeigneter oder erlangter unbarer Zahlungsinstrumente als Straftat geahndet werden kann.

25 Mitgliedstaaten haben Artikel 3 Buchstabe a der Richtlinie umgesetzt. Von den 25 Ländern haben 14 die Richtlinie durch eine Bestimmung über die betrügerische Verwendung unbarer Zahlungsinstrumente umgesetzt (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). Die übrigen Mitgliedstaaten verwiesen auf allgemeinere Straftaten wie Betrug und Computerfälschung oder Betrug im Zusammenhang mit Zahlungsmitteln, die nicht auf unbare Zahlungsinstrumente beschränkt sind (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

Das Gesetz von HR bezieht sich nicht auf die Verwendung gestohlener oder anderweitig rechtswidrig angepasster Zahlungsinstrumente. Die Umsetzungsbestimmung in HU bezieht sich nur auf elektronische unbare Zahlungsinstrumente.

Nach Artikel 3 Buchstabe b der Richtlinie treffen die Mitgliedstaaten die erforderlichen Maßnahmen, um sicherzustellen, dass die vorsätzliche betrügerische Verwendung gefälschter oder verfälschter unbarer Zahlungsinstrumente als Straftat geahndet werden kann.

Artikel 3 Buchstabe b wurde im Allgemeinen vollständig umgesetzt.

Zur Umsetzung der Richtlinie verweisen 15 Mitgliedstaaten auf nationale Bestimmungen über unbare Zahlungsinstrumente (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), während in zehn Mitgliedstaaten die nationalen Umsetzungsvorschriften allgemeinere Straftaten wie Diebstahl oder Betrug oder Straftaten im Zusammenhang mit Zahlungsinstrumenten abdecken, nicht aber speziell unbare Instrumente (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Straftaten im Zusammenhang mit der betrügerischen Verwendung körperlicher unbarer Zahlungsinstrumente

Artikel 4 der Richtlinie verpflichtet die Mitgliedstaaten, die erforderlichen Maßnahmen zu treffen, um sicherzustellen, dass die in den Unterabsätzen des Artikels aufgeführten vorsätzlich begangenen Handlungen als Straftat geahndet werden können. Die Unterabsätze umfassen a) den Diebstahl oder eine andere widerrechtliche Aneignung eines körperlichen unbaren Zahlungsinstruments, b) die betrügerische Fälschung oder Verfälschung eines körperlichen unbaren Zahlungsinstruments, c) den Besitz von gestohlenen oder in anderer Weise widerrechtlich angeeigneten oder gefälschten oder verfälschten körperlichen unbaren Zahlungsinstrumenten zwecks betrügerischer Verwendung, d) die Beschaffung für sich selbst oder einen Dritten, einschließlich der Annahme, der Aneignung, des Erwerbs, der Weitergabe, der Einfuhr, der Ausfuhr, des Verkaufs, der Beförderung oder der Verbreitung eines gestohlenen, gefälschten oder verfälschten körperlichen unbaren Zahlungsinstruments zwecks betrügerischer Verwendung.

Während Artikel 4 offenbar mehr oder weniger wörtlich umgesetzt wurde, wirft die nationale Umsetzung in einigen Fällen Fragen auf, wenn es um die konkrete Beschaffung eines gestohlenen, gefälschten oder verfälschten körperlichen unbaren Zahlungsinstruments zur betrügerischen Verwendung für sich selbst oder einen Dritten geht.

c) Straftaten im Zusammenhang mit der betrügerischen Verwendung nichtkörperlicher unbarer Zahlungsinstrumente

In Artikel 5 der Richtlinie werden Verhaltensweisen im Zusammenhang mit der betrügerischen Verwendung nichtkörperlicher unbarer Zahlungsinstrumente unter Strafe gestellt. Die Analyse ergab, dass dieser Artikel offenbar keine Herausforderungen bei der Umsetzung mit sich brachte. In den meisten Fällen gilt die nationale Bestimmung sowohl für körperliche als auch für nichtkörperliche unbare Zahlungsinstrumente. Etwa die Hälfte der Mitgliedstaaten hat Artikel 5 der Richtlinie durch allgemeinere Bestimmungen umgesetzt (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK) und mehr als die Hälfte von ihnen hat Artikel 5 durch eine Bestimmung umgesetzt, die sich speziell auf die betrügerische Verwendung unbarer Zahlungsinstrumente bezieht (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Betrug im Zusammenhang mit Informationssystemen

Artikel 6 der Richtlinie verpflichtet die Mitgliedstaaten die erforderlichen Maßnahmen zu treffen, um sicherzustellen, dass 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, als Straftat geahndet wird, wenn das Funktionieren eines Informationssystems unrechtmäßig behindert oder gestört wird (Artikel 6 Buchstabe a) oder Computerdaten unrechtmäßig eingegeben, verändert, gelöscht, übertragen oder unterdrückt werden (Artikel 6 Buchstabe b). Alle Mitgliedstaaten haben Artikel 6 umgesetzt.

e) Tatwerkzeuge

Artikel 7 verpflichtet die Mitgliedstaaten, die erforderlichen Maßnahmen zu treffen, um sicherzustellen, dass die Herstellung, die Beschaffung für sich selbst oder einen Dritten oder die Bereitstellung einer Vorrichtung oder eines Instruments, von Computerdaten oder anderer Mittel, die eigens dafür konzipiert oder angepasst worden sind, eine Straftat im Sinne des Artikels 4 Buchstaben a und b, des Artikels 5 Buchstaben a und b oder des Artikels 6 zu begehen, zumindest dann als Straftat geahndet werden, wenn dabei der Vorsatz besteht, dass diese Mittel Verwendung finden.

Die überwiegende Mehrheit der Mitgliedstaaten hat Artikel 7 der Richtlinie umgesetzt (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Sechs Länder haben Artikel 7 der Richtlinie durch Bestimmungen umgesetzt, die sich auf umfassendere Bestimmungen beziehen, entweder zu allgemeinen Straftaten wie Diebstahl oder zu Finanzinstrumenten und Zahlungsmitteln (BG, FI, FR, LV, SE, SK). 17 Länder haben die Richtlinie durch eine spezifische Bestimmung zu Instrumenten umgesetzt, die zur Begehung der verschiedenen Straftaten der Richtlinie im Zusammenhang mit körperlichen oder nichtkörperlichen unbaren Zahlungsinstrumenten verwendet werden (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Fünf Mitgliedstaaten (BE, BG, HU, PL, PT) hatten offenbar Schwierigkeiten bei der Umsetzung.

2.3 Allgemeine Vorschriften zu den betreffenden Straftaten

a) Anstiftung, Beihilfe und Versuch

Gemäß Artikel 8 Absatz 1 der Richtlinie stellen die Mitgliedstaaten sicher, dass die Anstiftung oder Beihilfe zu einer der in den Artikeln 3 bis 7 genannten Straftaten als Straftat geahndet wird.

Alle Mitgliedstaaten haben diese Bestimmung umgesetzt. Die überwiegende Mehrheit der Mitgliedstaaten hat die Richtlinie mithilfe eines bestehenden Artikels zur Anstiftung und Beihilfe im Allgemeinen umgesetzt (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). Zwei Mitgliedstaaten haben jedoch beschlossen, eine neue Bestimmung zu erlassen, die nur im Zusammenhang mit den Straftaten der Richtlinie gilt (CY, MT).

Artikel 8 Absatz 2 Satz 1 verpflichtet die Mitgliedstaaten, sicherzustellen, dass der Versuch der Begehung einer Straftat im Sinne des Artikels 3, des Artikels 4 Buchstaben a, b oder d, des Artikels 5 Buchstaben a oder b sowie des Artikels 6 als Straftat geahndet wird. Mit Ausnahme von BE, LU und SI scheinen alle Mitgliedstaaten diese Bestimmung vollständig umgesetzt zu haben.

Die überwiegende Mehrheit der Mitgliedstaaten hat auch in diesem Fall die Richtlinie mithilfe einer bestehenden Bestimmung zum Versuch im Allgemeinen umgesetzt (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). Die anderen Mitgliedstaaten haben die Bestimmung in eine besondere Umsetzungsmaßnahme aufgenommen (CY, DE, FI, MT, RO).

Die Mitgliedstaaten müssen zudem sicherstellen, dass zumindest die versuchte betrügerische Beschaffung eines widerrechtlich erlangten, gefälschten oder verfälschten nichtkörperlichen unbaren Zahlungsinstruments für sich selbst oder einen Dritten (Artikel 5 Buchstabe d) als Straftat geahndet wird (Artikel 8 Absatz 2 Satz 2).

Die Bewertung ergab, dass die Kriminalisierung des Versuchs in zwei Mitgliedstaaten (HR, SI) Beschränkungen unterworfen werden kann, die in der Richtlinie nicht vorgesehen sind.

Alle übrigen Mitgliedstaaten haben die einschlägigen Bestimmungen der Richtlinie umgesetzt. Dies geschah entweder durch einen Artikel zum Versuch im Allgemeinen (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK) oder durch eine besondere Umsetzungsmaßnahme (CY, DE, FI, MT, RO).

b) Strafen

In Artikel 9 ist festgelegt, dass Straftaten im Sinne der Artikel 3 bis 8 mit wirksamen, angemessenen und abschreckenden Strafen geahndet werden. Darüber hinaus gibt der Artikel die Höchstmaße für Freiheitsstrafen für die verschiedenen Straftaten vor.

Während die Mitgliedstaaten Artikel 9 der Richtlinie im Allgemeinen umgesetzt haben, wurden bei der Bewertung mögliche Probleme im Zusammenhang mit dem Anwendungsbereich der Definition in Bezug auf Artikel 9 Absatz 2 in HR und Artikel 9 Absatz 6 in BE, CZ, HR und HU ermittelt.

Der Vergleich der von den Mitgliedstaaten für die verschiedenen Straftaten festgelegten Sanktionen ist kompliziert, da die Straftaten sowohl von allgemeinen als auch von spezifischen Bestimmungen abgedeckt werden. Bei der Umsetzung der Richtlinie durch Bestimmungen über allgemeine Straftaten haben sich die Mitgliedstaaten auf verschiedene nationale Vorschriften gestützt, um eine Handlung unter Strafe zu stellen, die nach der Richtlinie verboten ist. Dies führt zu verschiedenen Höchststrafen, die für diesen konkreten Verstoß gelten, und bedeutet, dass die tatsächliche Höchststrafe vom konkreten Fall, von der Vorgehensweise der Gerichte und von den nationalen Vorschriften über die gleichzeitige Verhängung von Strafen abhängen würde. In PL beispielsweise gilt die Regel, dass eine Handlung nur eine Straftat darstellen kann. Weist eine Handlung Merkmale von zwei oder mehr strafrechtlichen Bestimmungen auf, muss das Gericht eine bestimmte Straftat wählen. In BG hingegen bestimmt das Gericht in Fällen, in denen der Besondere Teil des Strafgesetzbuchs die Verhängung von zwei oder mehr Strafen gleichzeitig für eine bestimmte Straftat vorsieht, den Umfang jeder einzelnen Strafe so, dass die Summe den allgemeinen Zielen der Strafe entspricht.

Darüber hinaus können die Bestimmungen erschwerende Umstände enthalten, die die Höchststrafe anheben und zu höheren Strafen führen können. Die Höchststrafe hängt daher von der Art und Weise ab, wie die Straftat begangen wird. So sieht beispielsweise die allgemeine Bestimmung über missbräuchliche Verwendung in HR eine Freiheitsstrafe von höchstens fünf Jahren vor. Wendet der Täter jedoch Gewalt an, so beträgt die Höchststrafe zehn Jahre, und wenn die Tat zu einem erheblichen materiellen Gewinn geführt hat, drohen dem Täter bis zu 12 Jahre Freiheitsentzug. In DE zieht die Fälschung von körperlichen unbaren Zahlungsinstrumenten eine Freiheitsstrafe von höchstens fünf Jahren nach sich. Wenn der Täter jedoch gewerbsmäßig handelt, beträgt die Höchststrafe zehn Jahre.

Die Bewertung ergab auch, dass die in den nationalen Rechtsvorschriften vorgesehenen Schwellenwerte in den meisten Fällen strenger sind als die in der Richtlinie festgelegten Schwellenwerte. Der Unterschied kann erheblich sein: Auf Geldfälschung stehen in BG und LU bis zu 15 Jahre und in PL bis zu 25 Jahre Freiheitsentzug. In nur zwei Mitgliedstaaten (AT, MT) sind die gleichen Höchststrafen vorgesehen wie in der Richtlinie bzw. Höchststrafen, die diesen nahekommen.

c) Verantwortlichkeit juristischer Personen

Die Bewertung ergab, dass 16 Mitgliedstaaten Artikel 10 der Richtlinie durch eine bereits bestehende allgemeine Bestimmung ihres Strafgesetzbuchs umgesetzt haben (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), während neun Mitgliedstaaten den Artikel durch ein Gesetz über die Verantwortlichkeit juristischer Personen im Zusammenhang mit der Richtlinie umgesetzt haben (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sanktionen gegen juristische Personen

Artikel 11 der Richtlinie verpflichtet die Mitgliedstaaten, wirksame, verhältnismäßige und abschreckende Sanktionen in Form von Geldstrafen oder Geldbußen auch gegen juristische Personen festzulegen. Alle Mitgliedstaaten haben solche Sanktionen festgelegt.

Artikel 11 sieht für die Mitgliedstaaten die Möglichkeit vor, verschiedene spezifische Sanktionen gegen juristische Personen zu erlassen, wie z. B. den Ausschluss von öffentlichen Zuwendungen oder die gerichtlich angeordnete Auflösung. Sechs Mitgliedstaaten (AT, BG, EE, FI, NL, SE) haben von der Möglichkeit nach Artikel 11 der Richtlinie überhaupt keinen Gebrauch gemacht. Die übrigen 19 Mitgliedstaaten haben Artikel 11 entweder vollständig oder teilweise umgesetzt (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Gerichtliche Zuständigkeit

Dieser Artikel, der die Mitgliedstaaten verpflichtet, ihre gerichtliche Zuständigkeit für Straftaten zu begründen, die in ihrem Hoheitsgebiet oder von einem ihrer Staatsangehörigen begangen wurden, wird in allen Mitgliedstaaten in den allgemeinen Bestimmungen des nationalen Strafgesetzbuchs oder der Strafprozessordnung umgesetzt. Daher sind das Territorialitätsprinzip und der Grundsatz der aktiven Staatsangehörigkeit allgemein anwendbar und nicht spezifisch für die in dieser Richtlinie geregelten Straftaten. Darüber hinaus wurde Artikel 12 auch von CY in das nationale Gesetz über die Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln und von PT in das Gesetz zur Bekämpfung der Cyberkriminalität umgesetzt.

Alle Mitgliedstaaten haben Artikel 12 Absatz 1 Buchstaben a und b umgesetzt.

Nach Artikel 12 Absatz 3 kann der Mitgliedstaat die gerichtliche Zuständigkeit für eine außerhalb ihres Hoheitsgebiets begangene Straftat im Sinne der Artikel 3 bis 8 der Richtlinie begründen, wenn unter anderem a) die Straftat von einer Person begangen wird, deren gewöhnlicher Aufenthalt in seinem Hoheitsgebiet liegt, b) die Straftat zugunsten einer in seinem Hoheitsgebiet niedergelassenen juristischen Person begangen wurde oder c) es sich bei dem Opfer der Straftat um einen seiner Staatsangehörigen handelt oder um eine Person, die ihren gewöhnlichen Aufenthalt in seinem Hoheitsgebiet hat. 14 Mitgliedstaaten (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) haben von der in Artikel 12 Absatz 3 Buchstabe a vorgesehenen Möglichkeit Gebrauch gemacht, 12 Mitgliedstaaten (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) haben Artikel 12 Absatz 3 Buchstabe b umgesetzt, und 16 Mitgliedstaaten (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) haben ihre Zuständigkeit gemäß Artikel 12 Absatz 3 Buchstabe c ausgeweitet. In Bezug auf Buchstabe c wurde in BG, DE, EE, HU, RO und SI die gerichtliche Zuständigkeit für eine Straftat begründet, die außerhalb ihrer Hoheitsgebiete begangen wurde, wenn die Straftat (nur) gegen einen ihrer Staatsangehörigen verübt wurde, womit Personen mit gewöhnlichem Aufenthalt im Hoheitsgebiet nicht erfasst werden. AT sieht vor, dass im Ausland begangene Straftaten von der österreichischen Strafjustiz verfolgt werden, wenn Täter und Opfer Österreicher sind. CY, CZ, EL, FI, LV und MT haben von allen drei fakultativen Bestimmungen des Artikels 12 Absatz 3 Gebrauch gemacht.

2.4 Operative Angelegenheiten

a) Wirksame Ermittlungen und Zusammenarbeit

In allen Mitgliedstaaten sind Ermittlungsinstrumente für die Ermittlung und strafrechtliche Verfolgung der in den Artikeln 3 bis 8 genannten Straftaten nicht ausdrücklich in den Rechtsvorschriften zur Umsetzung der Richtlinie enthalten, sondern eher in allgemeineren Rechtsvorschriften wie der Strafprozessordnung. In der Regel steht die Möglichkeit, in einem bestimmten Fall ein Ermittlungsinstrument einzusetzen, im Zusammenhang mit der Sanktion für die betreffende Straftat. Wie bereits in der Bestimmung der Richtlinie dargelegt, stehen die Ermittlungsinstrumente, die bei der Bekämpfung der organisierten Kriminalität oder in anderen Fällen schwerer Kriminalität eingesetzt werden, auch für die Ermittlung und Verfolgung der in dieser Richtlinie genannten Straftaten zur Verfügung. Der Ausnahmecharakter einiger Ermittlungsinstrumente und die Notwendigkeit der Verhältnismäßigkeit in Bezug auf die Straftat sind am häufigsten in den einschlägigen Rechtsvorschriften und/oder in der Verfassung enthalten.

Informationen zu den in den Artikeln 3 bis 8 genannten Straftaten sollten gemäß Artikel 13 Absatz 2 der Richtlinie die Behörden, die mit der Ermittlung oder strafrechtlichen Verfolgung dieser Straftaten befasst sind, unverzüglich erreichen. Anders ausgedrückt sollten Strafverfolgungsbehörden und sonstige zuständige Behörden zum Zwecke der Ermittlung und strafrechtlichen Verfolgung der in dieser Richtlinie (Erwägung 22) genannten Straftaten zügig Zugang zu einschlägigen Informationen erhalten. Die Strafprozessordnung sieht häufig verschiedene Meldesysteme vor, damit Straftaten (im Sinne der Artikel 3 bis 8 der Richtlinie) effizient und schnell gemeldet werden können. Zu diesen Meldesystemen gehören: eine Pflicht zur Meldung an öffentliche Stellen und Behörden, ein System für Hinweisgeber, ein Beschwerdeverfahren, eine Verpflichtung der Zahlungsdienstleister zur Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle und das Recht von Privatpersonen, Vorfälle zu melden. Darüber hinaus kann mit einigen spezifischeren Rechtsvorschriften sichergestellt werden, dass Meldungen über Sicherheitsvorfälle (einschließlich Meldungen über schwerwiegende Straftaten, wie unbefugter Erwerb, Fälschung und Änderung eines Zahlungsmittels) den zuständigen Behörden so schnell wie möglich gemeldet werden. Solche Gesetze wurden von AT, CZ, LT, FI, MT und PT gemeldet.

Die Bedingung, dass die übermittelten Informationen die zuständigen Behörden unverzüglich erreichen sollten, wird in den meisten Fällen nicht ausdrücklich umgesetzt.

b) Austausch von Informationen

Der Austausch von Informationen zwischen den nationalen Strafverfolgungsbehörden zum Zwecke der Ermittlung und strafrechtlichen Verfolgung von Straftaten, einschließlich der in den Artikeln 3 bis 8 der Richtlinie genannten Straftaten, kann durch operative Kontaktstellen erleichtert werden (Erwägungsgrund 26). Artikel 14 Absatz 1 Satz 1 der Richtlinie stellt sicher, dass die Mitgliedstaaten diese Kontaktstellen tatsächlich einrichten und dass sie rund um die Uhr zur Verfügung stehen. Zudem verpflichtet Satz 2 die Mitgliedstaaten, dafür zu sorgen, dass Verfahren vorhanden sind, mit denen dringende Ersuchen um Unterstützung umgehend bearbeitet werden und binnen acht Stunden nach Eingang des Ersuchens zumindest mitgeteilt wird, ob das Ersuchen beantwortet wird, in welcher Form die Antwort erfolgen und wann diese voraussichtlich gesendet werden wird.

Die folgenden Mitgliedstaaten haben beschlossen, eine bestehende operative Kontaktstelle für die in dieser Richtlinie beschriebenen Zwecke zu nutzen: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

Tabelle 1 gibt einen Überblick über die eingerichteten Kontaktstellen. In BG, CZ, LU, SI und HR wurden keine Kontaktstellen benannt.

Tabelle 1 Operative Kontaktstellen

Mitgliedstaat	Kontaktstelle	Mitgliedstaat	Kontaktstelle
AT	Bundeskriminalamt	**EE**	Justizministerium
BE	Direktion für operative polizeiliche Informationen	**FI**	Nationales Ermittlungsbüro
BG	k. A.	**FR**	Abteilung für internationale Beziehungen der Zentraldirektion der Kriminalpolizei
CY	Zyprische Polizei	**HR**	k. A.
CZ	k. A.	**HU**	Zentrum für internationale Zusammenarbeit in Strafsachen (NEBEK)
DE	16 Landeskriminalämter und ein Bundeskriminalamt – Zentrale	**MT**	Maltesische Polizei

	Kontaktstellen für Cyberkriminalität		
EL	Griechische Polizei (Abteilung für internationale polizeiliche Zusammenarbeit)	**ES**	Notfallkoordinierungszelle
IT	Internationale Operationszentrale des Dienstes für internationale polizeiliche Zusammenarbeit	**NL**	Nationales Zentrum für internationale Rechtshilfe (LIRC)
LT	Zweite Abteilung der Polizeidirektion des Polizeidepartements am Innenministerium der Republik Litauen und der Rat für internationale Beziehungen des litauischen Kriminalpolizeiamts	**PL**	Polizeihauptpräsidium
LV	Nationale Polizei	**PT**	Kriminalpolizei
RO	Abteilung für Strafverfolgung und strafrechtliche Ermittlungen der Generalstaatsanwaltschaft	**SE**	Polizeibehörde
SI	k. A.	**SK**	Kriminalpolizeiamt des Polizeipräsidiums der Slowakischen Republik

Artikel 14 Absatz 1 Satz 2 der Richtlinie wurde in einigen Mitgliedstaaten praktisch umgesetzt. Informationen zu den Verfahren für dringende Ersuchen konnten in BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE, SK nicht ermittelt werden.

c) Meldung von Straftaten

Die Mitgliedstaaten sind auch verpflichtet, geeignete Meldekanäle einzurichten. Solche Kanäle zur Meldung von Betrugsverdachtsfällen oder allgemein zur Meldung mutmaßlicher Straftaten können in Rechtsakten festgelegt werden. Häufig haben die Mitgliedstaaten die Meldung einer Straftat als Verpflichtung für bestimmte Kategorien von (natürlichen und juristischen) Personen festgelegt (weitgehend entsprechend Artikel 15 Absatz 2), während Opfern und anderen anwesenden Personen die Möglichkeit (nicht aber die Pflicht) eingeräumt wird, die Straftat zu melden. Diese Rechtsvorschriften werden in der Regel durch praktische Umsetzungsmaßnahmen ergänzt.

In allen Mitgliedstaaten können schriftliche oder mündliche Berichte an die Polizei und/oder die Justiz gerichtet werden. Darüber hinaus haben einige Mitgliedstaaten zusätzliche Meldekanäle eingerichtet:

Das österreichische Bundesgesetz sieht verschiedene Meldesysteme vor, damit Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie effizient und schnell gemeldet werden können: 1) die Pflicht zur Meldung an öffentliche Stellen und Behörden, 2) das System für Hinweisgeber der Staatsanwaltschaft für Wirtschaft und Korruption, 3) das System für Hinweisgeber der Finanzmarktbehörde, 4) die Verpflichtung der Zahlungsdienstleister zur Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle. Beim Bundeskriminalamt wurde eine spezielle Meldestelle für Cyberkriminalität eingerichtet. Darüber hinaus arbeitet das Bundesministerium für Inneres mit der Wirtschaftskammer zusammen. Infolgedessen finden verschiedene Informationsaktionen und Kampagnen statt, mit denen die Öffentlichkeit motiviert und ermutigt wird, einschlägige Gesetzesverstöße zu melden.

In BE betreibt das Wirtschaftsministerium eine einheitliche Anlaufstelle für Opfer von Betrug und Täuschung. Darüber hinaus wurde ein Meldekanal für Hinweisgeber eingerichtet, der von der Finanzdienstleistungs- und Marktaufsichtsbehörde für alle Beschwerden im Zusammenhang mit Kredit- oder Anlageprodukten und -dienstleistungen eingerichtet wurde.

In CY wurden die zyprische Polizei zusammen mit der Zentralbank Zyperns und der nationalen Behörde für die Sicherheit von Netz- und Informationssystemen im Wege einer gesetzlichen Maßnahme förmlich als die zuständigen nationalen Behörden benannt, die für die Einrichtung geeigneter Melde- und Kommunikationskanäle zuständig sind.

Das tschechische Strafrecht verpflichtet die staatlichen Behörden zur Meldung.

In DE müssen die Verpflichteten verdächtige Handlungen unverzüglich melden. Darüber hinaus wurden auf Bundesebene nichtlegislative Maßnahmen wie eine institutionalisierte öffentlich-private Partnerschaft zum Zwecke der Aufdeckung, Verhütung, Ermittlung oder strafrechtlichen Verfolgung von Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie und eine Plattform für den Informationsaustausch eingerichtet.

In EL hat die griechische Regierung zusätzlich zu den allgemeinen Meldekanälen einen staatlichen Online-Dienst eingerichtet, über den Bürger direkt Beschwerden wegen online begangener Straftaten einreichen können. Zudem müssen Kreditinstitute und andere Anbieter von Zahlungsdiensten der Bank von Griechenland (die für solche Beschwerden zuständig ist) unverzüglich alle Betrugsfälle melden, wenn sie auf solche stoßen.

In ES bietet die Bank von Spanien neben den allgemeinen Kanälen für die Meldung von Straftaten einen Meldekanal in Zusammenarbeit mit dem nationalen Institut für Cybersicherheit an.

In den italienischen Rechtsvorschriften wird die zeitnahe Meldung einer Straftat durch die Kriminalpolizei an die Staatsanwaltschaft sichergestellt, wenn diese von Amts wegen oder aufgrund einer Beschwerde oder eines Rechtsstreits Kenntnis davon erlangt hat. Der Informationsaustausch wird auch über digitale Plattformen gefördert.

LT verfügt über mehrere Kanäle für die Meldung von Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie, nämlich über eine Website (e-Police-Portal), über die allgemeine Notrufnummer 112 sowie persönlich, per E-Mail, per Textnachricht und über die mobile e-Police-Anwendung sowie über andere automatisierte Mittel. Zahlungsdienstleister, Finanzinstitute und andere Verpflichtete, die Bank von Litauen und die Ermittlungsstelle für Finanzkriminalität sind verpflichtet, den zuständigen Strafverfolgungsbehörden einen begründeten Verdacht auf kriminelle und/oder sonstige rechtswidrige Handlungen zu melden.

In LU wird auf einer Website erläutert, wie Betrugsfälle gemeldet werden können. Die Aufsichtskommission des Finanzsektors legte Leitlinien zur Aufdeckung von Finanzbetrug fest, fordert aber auch alle ihrer Aufsicht unterstehenden Einrichtungen auf, alle Betrugsfälle und alle Vorfälle im Zusammenhang mit Computerangriffen von außen möglichst zeitnah zu melden.

In RO besteht eine Meldepflicht für Beamte und Personen in Führungspositionen in Behörden, Personen, die Dienstleistungen von öffentlichem Interesse erbringen, sowie Personen, die in Kontroll- und Aufsichtsorganen tätig sind.

In SI besteht für alle staatlichen Behörden und Organisationen mit hoheitlichen Befugnissen die Pflicht, eine Straftat zu melden.

Die Plattform Perceval in FR, die durch einen Rechtsakt eingerichtet wurde, ermöglicht Opfern die Meldung von Bankkartenbetrug und -fälschung. Eine ähnliche Plattform gibt es für die Meldung von Cyberstraftaten. Darüber hinaus gelten Sanktionen für jede (natürliche oder juristische) Person, die nicht durch ihr sofortiges Handeln eine Straftat verhindert, was einer allgemeinen Meldepflicht entspricht.

In HU ist die Pflicht zur Anzeige einer Straftat nur für die Mitarbeiter der Behörde, Beamte und gesetzliche Berufsorganisationen festgelegt. Die ungarische Nationalbank fordert die Finanzinstitute auf ihrer Website auf, mutmaßliche Betrugsfälle in Form einer Stellungnahme zu melden.

In MT fördert die nationale Kontaktstelle die Meldung, insbesondere durch Finanzinstitute, von Verdachtsfällen von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln.

Neben dem in PT gesetzlich eingerichteten Meldekanal für Hinweisgeber gibt es ein „Ein-Klick“-System zur Meldung von Cyberkriminalität, bei dem über einen Link umgehend eine E-Mail an die zuständigen Behörden geöffnet wird.

In SE können bestimmte Arten von Straftaten wie Kreditkartenbetrug auch über den elektronischen Dienst der Polizeibehörde gemeldet werden. Darüber hinaus sind Akteure, die im Bereich Banken und Finanzierungen tätig sind, verpflichtet, verdächtige Aktivitäten im Zusammenhang mit potenziellen Fällen von Geldwäsche oder Terrorismusfinanzierung oder auf andere Weise aus einer Straftat erzieltes Vermögen der Polizeibehörde zu melden. Zudem wird ein ständiger Dialog zwischen der Bank- und Finanzwirtschaft und dem nationalen Betrugsbekämpfungszentrum der Polizeibehörde geführt.

Die Rechtsvorschriften in SK verpflichten die Behörden und andere juristische Personen zur unverzüglichen Meldung von Straftaten an die Strafverfolgungsbehörden (und geben Verfahren dafür vor). Ferner bestehen für Verpflichtete und insbesondere für Banken Meldepflichten bezüglich Geldwäsche.

Alternativ wurden in NL und PL nichtlegislative Maßnahmen zur Umsetzung von Artikel 15 der Richtlinie ergriffen. Über die Rufnummern des Polizeidienstes und die Website der Polizei werden geeignete Kanäle für die Meldung von Betrugsfällen im Zusammenhang mit unbaren Zahlungsinstrumenten an die Behörden bereitgestellt. Darüber hinaus hat sich die niederländische Regierung verpflichtet, Finanzinstitute und andere juristische Personen aufzufordern, jeden Betrugsverdacht zu melden. Die Bemühungen zeigen sich z. B. am Bestehen einer Dienststelle für Finanzbetrug, die in allen Polizeieinheiten in den Niederlanden eingerichtet wurde. Außerdem haben vier große Banken und Herausgeber von ICS-Karten eine Vereinbarung mit der Polizei unterzeichnet, um gemeinsam gegen (Banken-)Betrug und Phishing vorzugehen. In PL werden Meldungen von Straftaten rund um die Uhr von allen Polizeidienststellen entgegengenommen. Zudem ist es aufgrund der Art der unter Einsatz von Computertechnologien begangenen Straftaten möglich, sich direkt an eine spezialisierte Organisationseinheit des Polizeihauptpräsidiums zu wenden. Um eine möglichst rasche Zusammenarbeit mit dem Bankensektor sicherzustellen, wurde außerdem ein Kooperationskanal zwischen dem Büro für die Bekämpfung von Cyberkriminalität des Polizeihauptpräsidiums und dem Zentrum für Bankensicherheit des polnischen Bankenverbands eingerichtet.

Artikel 15 Absatz 2 der Richtlinie wurde in BG, EE und HR nicht umgesetzt.

2.5 Unterstützung für Opfer und Prävention

a) Hilfe und Unterstützung für Opfer

Hilfe und Unterstützung für natürliche und juristische Personen, deren personenbezogene Daten missbräuchlich verwendet wurden, werden durch Artikel 16 Absatz 1 der Richtlinie gewährleistet. Die Maßnahmen umfassen: a) das Angebot von einschlägigen Informationen und Beratung, wie sie sich vor den negativen Folgen solcher Straftaten schützen können, und b) das Bereitstellen einer Liste spezieller Einrichtungen, die verschiedene Aspekte der Identitätskriminalität und der Opferhilfe abdecken.

In gleicher Weise sollten juristische Personen, die Opfer einer Straftat im Sinne der Artikel 3 bis 8 dieser Richtlinie sind, Zugang zu Informationen über a) die Verfahren zur Erstattung einer Strafanzeige, b) das Recht, Informationen über den Fall zu erhalten, c) die verfügbaren Beschwerdeverfahren für den Fall, dass die zuständige Behörde die Rechte des Opfers im Strafverfahren verletzt, und d) die Kontaktangaben für den Fall betreffende Mitteilungen (Artikel 16 Absatz 3 der Richtlinie) haben.

Die Strafprozessordnung der meisten Mitgliedstaaten enthält Vorschriften zu Opfern und deren Rechten, darunter einige spezifische Bestimmungen zum Recht der Opfer auf Information und Unterstützung während des Verfahrens, das Recht auf Beratung und das Recht auf Beschwerde. Ein spezifischer Rechtsakt zur Umsetzung der Richtlinie ergänzt oft das, was bereits in der Strafprozessordnung vorgesehen ist. Juristische Personen werden in der Regel in gesonderten Rechtsvorschriften in der Strafprozessordnung oder an anderer Stelle behandelt. Darüber hinaus stehen verschiedene Informationskampagnen, Faltblätter, spezielle Websites, Rundschreiben usw. zur Verfügung, um Opfer von Straftaten im Sinne der Artikel 3 bis 8 der Richtlinie zu unterstützen. Dies ist in AT, BE (hinsichtlich Artikel 16 Absatz 1), CY, CZ, DE, IT, LT, LU (hinsichtlich Artikel 16 Absatz 1), LV (hinsichtlich Artikel 16 Absatz 3), RO, SI (hinsichtlich Artikel 16 Absatz 3), EE, FI (hinsichtlich Artikel 16 Absatz 1), FR (hinsichtlich Artikel 16 Absatz 1), HR, HU, NL, PL (hinsichtlich Artikel 16 Absatz 3), PT, SE und SK der Fall. Artikel 16 Absatz 1 und/oder Artikel 16 Absatz 3 der Richtlinie wurden in keinem Mitgliedstaat wörtlich oder fast wörtlich umgesetzt, mit Ausnahme von MT.

Die Liste der akkreditierten Beratungseinrichtungen, die Opferhilfe leisten, gemäß Artikel 16 Absatz 1 Buchstabe b der Richtlinie, ist in der Regel online verfügbar und wird somit in der Praxis umgesetzt.

b) Prävention

Gemäß Artikel 17 über Prävention ergreifen die Mitgliedstaaten geeignete Maßnahmen, wie beispielsweise Informations- und Sensibilisierungskampagnen sowie Forschungs- und Bildungsprogramme. Dieser Abschnitt stützt sich auf eine Bewertung der Informationen, die die Mitgliedstaaten der Kommission übermittelt haben, sowie auf eine Recherche der offen im Internet verfügbaren Informationen, in deren Rahmen das Bestehen von Präventionsmaßnahmen untersucht wurde. Wie in Tabelle 2 beschrieben, befassen sich die ermittelten Präventionsmaßnahmen hauptsächlich mit Cyberkriminalität und Online-Betrug. In einigen Ländern werden jedoch auch Informationen über die Betrugsprävention bereitgestellt, in der Regel von der Polizei.

Tabelle 2 Präventionsmaßnahmen

Mitgliedstaat	Maßnahmen
AT	Die Bundespolizei informiert regelmäßig auf ihrer Website und in sozialen Netzwerken über Möglichkeiten, sich vor Betrug zu schützen. Die Zusammenarbeit mit Interessenträgern wie der Handelskammer wird im Rahmen von E-Commerce-Projekten unterstützt und umgesetzt.
BE	Verschiedene Websites mit Materialien zur Beratung/Sensibilisierung, z. B. vom Zentrum für Cybersicherheit von Belgien (Centre for Cybersecurity Belgium, CCB). Im Rahmen der Internetrecherche konnte eine gewisse Zusammenarbeit mit Interessenträgern festgestellt werden, z. B. arbeitete die den Finanzsektor vertretende Organisation mit der Brüsseler Staatsanwaltschaft (Parquet de Bruxelles) zusammen, um Materialien zur Sensibilisierung zu entwickeln.
BG	In Bulgarien wurde im Jahr 2021 eine vom Bankenverband organisierte Kampagne zur Bekämpfung von sogenannten „Money Mules“ (dt.: Geldesel, Finanzagenten) gestartet und gemeinsam mit der Generaldirektion für die Bekämpfung der organisierten Kriminalität und der Staatsanwaltschaft durchgeführt. Die Generaldirektion hat auch eine Kampagne zum Thema Phishing gestartet.
CY	Die Unterabteilung der Polizei für Cyberkriminalität stellt auf ihrer Website Informationen und Ratschläge zu Themen wie digitalem Betrug sowie Informationen über bevorstehende Veranstaltungen, wie Sensibilisierungskampagnen, bereit. Ein Beispiel hierfür ist die Informationskampagne zur Informationssicherheit, die von der Polizei, den Zentralbanken, dem Bankenverband und der Behörde für digitale Sicherheit durchgeführt wird.
DE	Das Bundeskriminalamt (BKA) bietet auf seiner Website einen Überblick über die Maßnahmen für institutionalisierte öffentlich-private Partnerschaften zum Zwecke der Aufdeckung,

	Verhütung, Ermittlung oder Verfolgung der unter die Richtlinie fallenden Straftaten, z. B. die Partnerschaft zwischen dem Bundeskriminalamt (BKA), dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem „German Competence Centre against Cyber Crime“ (Deutsches Kompetenzzentrum zur Bekämpfung von Cyberkriminalität, G4C), einem Verband mit Finanzinstituten und Unternehmen des IT-Sicherheitssektors. Das BKA hat auch die Cybercrime Conference C³ ins Leben gerufen, eine Plattform für den Austausch zwischen Behörden, Unternehmen, Wissenschaft und Politik. Das G4C erstellt auch Informationsbroschüren und entwickelt Schulungen. Schließlich beteiligt sich das BKA auch an Präventionsmaßnahmen im Bereich der Cyberkriminalität auf Länderebene. Auf Bundesebene ist das BKA zudem mit anderen Polizei- und Nichtpolizeibehörden und -organisationen (Interessenträger) vernetzt und intensiviert die Zusammenarbeit insbesondere bei Trendthemen.
FR	Das Innenministerium veröffentlicht Informationen zur Prävention von Cyberkriminalität. Auf den Plattformen, die für die Meldung von Cyberkriminalität zur Verfügung stehen, sind auch Informationen über Prävention enthalten sowie ein Kontakt zum Informations- und Kommunikationsdienst der nationalen Polizei (SICoP). Weitere Beispiele sind die von der Bank von Frankreich herausgegebenen Leitlinien oder der von der nationalen Task Force für die Betrugsbekämpfung veröffentlichte Leitfaden, in dem verschiedene Verwaltungs- und Durchsetzungsbehörden zusammengefasst sind.
EL	Die Abteilung für Cyberkriminalität und das Polizeihauptpräsidium bemühen sich sehr aktiv darum, die Öffentlichkeit zu informieren, zu sensibilisieren und das Risiko, Opfer von Betrug zu werden, durch Fernsehkampagnen, Vorträge und Online-Informationen zu verringern.
ES	Das nationale spanische Institut für Cybersicherheit und die Steuerbehörde stellen auf ihrer Website einschlägige Informationen zur Verhinderung von Phishing, dem Einsatz von Ransomware usw. in Geschäftsumgebungen bereit.
HR	Das Innenministerium stellt online Informationen über Internetbetrug bereit und betreibt einen YouTube-Kanal, der sich mit Betrug und Computersicherheit befasst und Videos über Cyberbetrug enthält.
IT	Das Finanzministerium ist für die Verhinderung von Betrug im Zusammenhang mit Zahlungsmitteln zuständig und fördert bereits eine Reihe von Initiativen auf lokaler Ebene in Zusammenarbeit mit den lokalen Verwaltungen und dem Hochschulsystem und veranstaltet Seminare und Workshops, die sich an die Personenkategorien aber auch an Bürger richten, die mit der Bekämpfung von Geldfälschung befasst sind.
LT	Auf der Website der für Kommunikation zuständigen Regulierungsbehörde finden sich Informationen zur Prävention im Zusammenhang mit Online-Betrug und auf der Website der Polizei Informationen über die häufigsten Arten von Cyberbetrug. Darüber hinaus besteht eines der Ziele der nationalen Strategie zur Bekämpfung der Cyberkriminalität darin, die Prävention und Kontrolle der Cyberkriminalität zu stärken, insbesondere durch die Entwicklung einer wirksamen Zusammenarbeit zwischen den Strafverfolgungsbehörden und anderen Interessenträgern.
LV	Die Finanz- und Kapitalmarktkommission hat verschiedene internetbasierte Werkzeuge entwickelt, mit denen Informationen und Leitlinien im Bereich finanzielle Sicherheit und Betrug bereitgestellt werden. Darüber hinaus wurden in Zusammenarbeit mit der Staatspolizei und dem Verbraucherschutzzentrum verschiedene Kampagnen organisiert.
NL	Es gibt Maßnahmen wie den „Fraudehelpdesk“ (Notrufnummer bei Betrugsfällen), eine Organisation, die von der niederländischen Regierung gefördert wird. Der Fraudehelpdesk, an den betrügerische Handlungen gemeldet werden können, ist der Teil der SAFECIN-Stiftung (Stiftung zur Bekämpfung der Finanz- und Wirtschaftskriminalität in den Niederlanden), einer Stiftung mit staatlicher Beteiligung.
SE	Zwischen der Bank- und Finanzwirtschaft und dem nationalen Betrugsbekämpfungszentrum der Polizeibehörde (NBC) wird ein ständiger Dialog geführt. Darüber hinaus arbeitet das NBC auch zu Zwecken der Verbrechensprävention u. a. mit Akteuren im elektronischen Handel zusammen. Bei diesen Kontakten wird betont, wie wichtig die Meldung von Betrugsfällen an die Polizei ist.

In zehn Mitgliedstaaten (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK) wurden keine Informationen über geeignete Präventionsmaßnahmen und die praktische Umsetzung ermittelt, wenngleich sich die Rechtsvorschriften in MT und RO sehr genau an den Wortlaut der Richtlinie halten und diese Verpflichtung widerspiegeln.

3. Schlussfolgerung und nächste Schritte

Die Richtlinie hat erhebliche Fortschritte bei der Angleichung der Einstufung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln als Straftaten in den Mitgliedstaaten bewirkt, wodurch eine grenzüberschreitende Zusammenarbeit der Strafverfolgungsbehörden, die diese Art von Straftaten untersuchen, ermöglicht wird. Die Mitgliedstaaten haben Strafgesetzbücher und andere einschlägige Rechtsvorschriften geändert, Verfahren gestrafft und Regelungen für die Zusammenarbeit eingeführt oder verbessert. Die Kommission erkennt die erheblichen Anstrengungen der Mitgliedstaaten zur Umsetzung der Richtlinie an.

Es besteht allerdings noch Spielraum, um das Potenzial der Richtlinie durch vollständige Umsetzung aller Bestimmungen durch die Mitgliedstaaten voll auszuschöpfen. Die bisherige Analyse deutet darauf hin, dass einige der wichtigsten von den Mitgliedstaaten zu erreichenden Verbesserungen die folgenden Artikel betreffen: Artikel 2 Buchstabe d, in dem die Definition der virtuellen Währung festgelegt ist, Artikel 7 über Straftaten im Zusammenhang mit den Tatwerkzeugen und Artikel 8 Absatz 2 über den Versuch, Artikel 9 Absatz 6 über Strafen für natürliche Personen, wenn die Straftat im Rahmen einer kriminellen Vereinigung begangen wurde, Artikel 14 über den Austausch von Informationen und Artikel 16 über Hilfe und Unterstützung für Opfer.

Die Kommission wird die Mitgliedstaaten auch weiterhin bei der Umsetzung der Richtlinie unterstützen. Insbesondere wird im Jahr 2023 eine spezielle Aufforderung zur Einreichung von Vorschlägen veröffentlicht.

Die Kommission ist bestrebt zu gewährleisten, dass die Umsetzung der Richtlinie in allen Mitgliedstaaten abgeschlossen wird und ihre Bestimmungen korrekt umgesetzt werden. Dies schließt die Kontrolle der Vereinbarkeit der nationalen Maßnahmen mit den entsprechenden Bestimmungen der Richtlinie ein. Gegebenenfalls wird die Kommission von den ihr aus den Verträgen erwachsenden Durchsetzungsbefugnissen Gebrauch machen, indem sie Vertragsverletzungsverfahren einleitet.