MASTER THESIS | MASTER'S THESIS

Titel | Title

Identitätsmissbrauch in der Telekommunikation

verfasst von | submitted by

Mag.iur. Tanja Fuchs

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 992 942
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von | Supervisor:	Univ.-Prof. Mag. Dr. Farsam Salimi Privatdoz.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABl	Amtsblatt der Europäischen Union, Reihe L: Rechtsvorschriften
Abs	Absatz
Art	Artikel
BAO	Bundesabgabenordnung BGBl 1961/194
BGBl	Bundesgesetzblatt
BlgNR	Beilage(n) zu den stenographischen Protokollen des Nationalrats
bspw	beispielsweise
bzw	beziehungsweise
dh	das heißt
dTKG	deutsches Telekommunikationsgesetz
DSB	Datenschutzbehörde
DSG	Datenschutzgesetz BGBl I 1999/165
DSGVO	Datenschutz-Grundverordnung
EECC	Europäischer Kodex für elektronische Kommunikation
Erläut	Erläuterung, -en
ff	und der, die folgenden
EGMR	Europäischer Gerichtshof für Menschenrechte
E-Evidence VO	Verordnung über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren
E-GovG	E-Government-Gesetz BGBl I 2004/10
EMRK	Europäische Menschenrechtskonvention BGBl 1958/210
ErläutRV	Erläuterungen zur Regierungsvorlage
ePrivacy-RL	Datenschutzrichtlinie für elektronische Kommunikation
FM-GwG	Finanzmarkt-Geldwäschegesetz BGBl I 2016/118
GlBG	Gleichbehandlungsgesetz BGBl I 2004/66
GSMA	GSM Association
IA	Initiativantrag
IKT	Informations- und Kommunikationstechnik
iSd	im Sinne des, - der
iVm	in Verbindung mit
IVO	Identifikationsverordnung BGBl II 2019/7
KEM-V 2009	Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 BGBl II 2009/212

mE	meines Erachtens
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
RTR-GmbH	Rundfunk und Telekom Regulierungs-GmbH
StGB	Strafgesetzbuch BGBl 1974/60
StPO	Strafprozeßordnung 1975 BGBl 1975/631
TKG 2021	Telekommunikationsgesetz 2021 BGBl I 2021/190
ua	unter andere, -s, unter anderem
UGB	Unternehmensgesetzbuch BGBl I 2005/120
WFA	Wirkungsorientierte Folgenabschätzung
VfGH	Verfassungsgerichtshof
VoIP	Voice Over IP
Z	Ziffer
zB	zum Beispiel

Sämtliche im Rahmen gegenständlicher Master Thesis verwendete Personenbezeichnungen sollen ausdrücklich alle Personen einschließen. Allein zur besseren Lesbarkeit werden nicht stets alle grammatikalischen Geschlechterformen aufgelistet.

1. Einführung

Die Kriminalität im Rahmen der Telekommunikation – sei es durch Handlungen über herkömmliche Anrufe und SMS oder Nachrichten durch Messengerdienste wie WhatsApp – hat verschiedenste Facetten.

Beispielsweise verfälscht die Täterschaft bei Betrugsanrufen ihre Rufnummer, wodurch bei den Empfängern der Anrufe eine falsche Rufnummer aufscheint (Call-ID Spoofing).[1] Das vorrangige Ziel davon ist, dass die tatsächlichen Täter ihre wahre Identität verschleiern, um sich der Strafverfolgung zu entziehen.[2] Im Endeffekt werden aber oftmals existierende Rufnummern missbräuchlich verwendet[3], womit schwerwiegende negative Folgen für den tatsächlichen Inhaber der Rufnummer, die missbraucht wird, verbunden sind. Dieser kann unter anderem Ermittlungen ausgesetzt werden, obwohl er die Straftat nicht begangen hat.[4] Damit kann schlussendlich eine erhebliche psychische Belastung einhergehen.[5]
Zudem bestehen eine Reihe an weiteren kriminellen Begehungsweisen, bei denen fremde Identitäten unberechtigterweise verwendet werden.[6]
Allein im Jahr 2023 wurden der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), die eine Meldestelle für Rufnummernmissbrauch betreibt, insgesamt 31.832 Betrugsanrufe, Betrugs-SMS sowie Missbräuche der eigenen Rufnummer gemeldet.[7]

In diesem Zusammenhang stellt sich die Frage, ob in der österreichischen Rechtsordnung ein wirksamer Schutz gegen das unbefugte Sichverschaffen fremder Identitätsdaten und die Verwendung dieser Daten besteht. In gegenständlicher Master Thesis werden diese beiden Handlungen, nämlich einerseits die Erlangung der Kenntnis über fremde Identitätsdaten und andererseits der unbefugte Gebrauch dieser Daten als Identitätsmissbrauch definiert und näher er-

---

1 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023: Lagebericht über die Entwicklung von Cybercrime (2024) 71.
2 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 71.
3 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 71.
4 *Österreichisches Institut für angewandte Telekommunikation (ÖIAT*), Identitätsdiebstahl: Die Folgen für Betroffene und wie ihnen geholfen werden kann (April 2022) 15.
5 *Österreichisches Institut für angewandte Telekommunikation (ÖIAT),* Identitätsdiebstahl 15.
6 Siehe dazu näher Kapitel 4 der gegenständlichen Master Thesis.
7 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT der Schlichtungsstellen 2023 (2024) 29.

läutert.[8] Der Fokus wird dabei auf Identitätsmissbrauch im Zusammenhang mit der Nutzung von Kommunikationsdiensten (worunter elektronische Dienste fallen, die gewöhnlich gegen Entgelt über Kommunikationsnetze erbracht werden[9]) gelegt. Im folgenden Kapitel wird dargelegt, auf welche Arten von Kommunikationsdiensten im Rahmen gegenständlicher Arbeit eingegangen wird.
Darüber hinaus wird der für die betreffende Master Thesis relevante Begriff „Identität" zunächst näher erörtert.
Sodann werden ausgewählte Kriminalitätsformen von Identitätsmissbrauch, wie Spoofing, einige Formen von betrügerischen Anrufen und Nachrichten sowie Phishing, dargestellt.

Anschließend erfolgt die Betrachtung der für den Identitätsmissbrauch einschlägigen Straftatbestände. In diesem Zusammenhang wird auch auf die Frage eingegangen, über welche Möglichkeiten die ermittelnden Behörden verfügen, beschuldigte Personen ausfindig zu machen.

Neben den strafrechtlichen Aspekten des Identitätsmissbrauchs wird analysiert, ob andere Rechtsgebiete, wie im Besonderen das Telekommunikations- und Datenschutzrecht, Bestimmungen vorsehen, die Identitätsmissbrauch erschweren oder unmöglich machen, sodass das Strafrecht letztendlich nicht zur Anwendung kommen muss.

Im Zuge der telekommunikationsrechtlichen Aspekte wird unter anderem herausgearbeitet, ob die im Telekommunikationsgesetz 2021 (TKG 2021)[10] verankerte Verpflichtung der Identitätserhebung und Registrierung von Stammdaten von Nutzern einen Beitrag zum Schutz von Identitätsdaten und somit gegen Identitätsmissbrauch leisten kann. Weiters wird thematisiert, welche weiteren Regelungen das Telekommunikationsgesetz vorsieht, um einzelne kriminelle Erscheinungsformen (wie insbesondere Call-ID Spoofing) zu unterbinden.
Zudem wird bei der Analyse datensicherheitsrechtlicher Aspekte unter anderem darauf eingegangen, ob Anbieter von Kommunikationsdiensten durch das Ergreifen von entsprechenden technischen und organisatorischen Maßnahmen nach der Datenschutz-Grundverordnung[11] (DSGVO) und dem TKG 2021 Identitätsmissbrauch vorbeugen können.

---

8 Siehe zur Definition von Identitätsmissbrauch zB *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112 (114*); Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 26, 27 (Stand 15.8.2023, rdb.at).

9 § 4 Z 4 Telekommunikationsgesetz 2021 BGBl I 2021/190 (TKG 2021).

10 BGBl I 2021/190.

11 VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

Die Erörterung dieser Themenbereiche und die entsprechende Untersuchung der einschlägigen Bestimmungen erfolgt unter Anwendung der juristischen Interpretationsmethoden sowie durch Literatur- und Judikaturrecherche.

2. Begriff „Kommunikationsdienst“

Vom Begriff „Kommunikationsdienste“ sind nach § 4 Z 4 TKG 2021 folgende „*gewöhnlich gegen Entgelt über Kommunikationsnetze erbrachte elektronische Dienste*“ umfasst: Internetzugangsdienste, interpersonelle Kommunikationsdienste und Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen (wie zB Dienste für die Maschine-Maschine-Kommunikation).[12]

Im Rahmen der gegenständlichen Master Thesis wird ausschließlich auf die Nutzung von interpersonellen Kommunikationsdiensten sowie die Nutzung von Internetzugangsdiensten eingegangen.
Interpersonelle Kommunikationsdienste werden in nummerngebundene interpersonelle Kommunikationsdienste (§ 4 Z 7 TKG 2021) und in nummernunabhängige interpersonelle Kommunikationsdienste (§ 4 Z 8 TKG 2021) unterteilt. Zu nummerngebundenen interpersonellen Kommunikationsdiensten sind vor allem Sprachkommunikationsdienste (über die eingehende und ausgehende Gespräche unter Nutzung von Nummern eines Nummerierungsplans geführt werden) und SMS-Dienste zuzuordnen.[13] Dagegen gehören etwa E-Mail-Dienste, nummernunabhängige VoIP-Dienste, Chatdienste, Nachrichtendienste und Videochatdienste zu nummernunabhängigen interpersonellen Kommunikationsdiensten.[14] Ein prominentes Beispiel für einen nummernunabhängigen Dienst ist WhatsApp, da die Nutzung des Dienstes auch ohne Rufnummer als Adressierungselement möglich ist.[15] Auch der Facebook Messenger, Telegram Messenger, Snapchat und G-Mail zählen zu den nummernunabhängigen interpersonellen Kommunikationsdiensten.[16]

---

12 § 4 Z 4 TKG 2021.
13 §§ 4 Z 4 lit b, 4 Z 6 und 7 TKG 2021; ErläutRV 1043 BlgNR 27. GP 3.
14 ErläutRV 1043 BlgNR 27. GP 3.
15 *Feiel*, Das Telekommunikationsgesetz 2021 – ein Überblick, MR 2021, 310.
16 *Abazagic*, Handbuch Telekomrecht: Regelungen des TKG 2021 für das Massengeschäft und EU-Vorgaben für Netzneutralität und Roaming, Kapitel 2 „Begriffsbestimmungen“ (2025) Rz 49.

3. Begriff „Identität“ und „Identitätsdaten“

Um in den nachstehenden Kapiteln auf das Phänomen Identitätsmissbrauch genauer eingehen zu können, werden in diesem Abschnitt zunächst die Fragen „Was ist die Identität?“ bzw „Wie kann eine Person identifiziert werden?“ erörtert.
Diese Fragen können nicht allgemeingültig beantwortet werden. Vielmehr bestehen je nach Disziplin (sei es in der Informationstechnologie, Philosophie, Mathematik oder in den Sozialwissenschaften) divergierende Beschreibungen der Identität.[17]

Im Folgenden wird die Erörterung im rechtlichen Sinn vorgenommen. Zunächst ist vorwegzunehmen, dass der Terminus „Identität“ kein Synonym der „Identifizierung“ darstellt. So stimmt der Begriff Identität mit der Person überein – die Identität einer Person stellt somit immer die konkrete Person selbst dar.[18] Dagegen wird bei der Identifizierung einer Person stets auf gewisse Merkmale abgestellt, die einer einzelnen Person zugeordnet werden können. Diese individuellen Merkmale können auch als Identitätsdaten bezeichnet werden.
Im österreichischen Recht besteht keine einheitliche Definition des Begriffs „Identitätsdaten“. In den einzelnen Materiengesetzen sind unterschiedliche Begriffsdefinitionen vorhanden. Nachstehend wird hinsichtlich der Art der Identifizierung von Personen auf einige ausgewählte Rechtsnormen näher eingegangen.

3.1. Telekommunikationsgesetz 2021 (TKG 2021)[19]

§ 166 Abs 2 TKG 2021 nimmt auf die Erhebung der Identität sowie Registrierung von Daten zur Identifizierung von Personen beim Abschluss eines Vertrags über die Bereitstellung von Kommunikationsdiensten (wie zB Prepaid Mobilfunkdienste) Bezug. So haben Anbieter von Kommunikationsdiensten gemäß § 166 Abs 2 TKG 2021 vor Durchführung des Vertrages die Identität der Nutzer zu erheben und die zur Identifizierung der Nutzer erforderlichen Stammdaten, nämlich den Namen, den akademischer Grad und das Geburtsdatum anhand geeigneter Identifizierungsverfahren zu registrieren.[20] Vom Begriff „Nutzer“ sind sowohl natürliche als auch juristische Personen erfasst.[21]

---

17 Siehe dazu *Borges/Schwenk/Stuckenberg/Wegener*, Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche Aspekte und technische Aspekte (2011) 14-16; näher *Bartz*, Identitätsdiebstahl: Zur Frage der Strafbarkeit des Identitätsdiebstahls und der Notwendigkeit eines eigenen Straftatbestands im deutschen Recht (2017) 19-34.

18 Siehe dazu auch *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 26, wonach der Begriff Identität „*an sich vollkommene Übereinstimmung in Bezug auf Dinge oder Personen bedeutet*“.

19 BGBl I 2021/190.

20 § 166 Abs 2 TKG 2021.

21 § 4 Z 13 TKG 2021.

Das Ziel ist, dass die Kundschaft von Kommunikationsdiensteanbietern im Anlassfall identifizierbar ist, damit die effektive Strafverfolgung sowie Gefahrenabwehr möglich sind.[22] Mithilfe dieser Identifizierung sollte den sicherheits- und kriminalpolizeilichen Bedürfnissen Rechnung getragen werden.[23]

Die auf Basis des TKG 2021 erlassene Identifikationsverordnung[24] (IVO) listet einzelne Identifizierungsverfahren, mit denen die Identität von natürlichen als auch juristischen Personen erhoben werden kann.
Als konkrete Verfahren zur Erhebung der Identität von natürlichen Personen werden (i) die persönliche Vorlage eines amtlichen Lichtbildausweises im Shop, in dem die SIM-Karte erworben wurde, (ii) die Bestätigung durch ein Kredit- oder Finanzinstitut, das die Person bereits zuvor identifiziert hat, sowie (iii) das Photoident-Verfahren (im Rahmen dessen über die Webcam eines internetfähigen Geräts ein amtlicher Lichtbildausweis vorzulegen ist und eine Aufnahme des Gesichts einer Person angefertigt wird) aufgelistet.[25]
Dementsprechend findet die Erhebung der Identität bei diesen drei Verfahren stets durch Vorlage eines amtlichen Lichtbildausweises, dessen Lichtbild mit der den Ausweis vorlegenden Person abgeglichen wird, statt.[26] Dokumente bzw Ausweise gelten als amtliche Lichtbildausweise, sofern sie von einer staatlichen Behörde ausgestellt wurden sowie *„mit einem nicht austauschbaren erkennbaren Kopfbild der betreffenden Person versehen sind, und den Namen, das Geburtsdatum und die Unterschrift der Person sowie die ausstellende Behörde enthalten“*.[27] Ebendiese auf einem Lichtbildausweis angeführten Daten kennzeichnen also einen Menschen, weswegen sie als Identitätsdaten bezeichnet werden können.
Hinsichtlich juristischer Personen zählen die auf einem Registerauszug enthaltenen Daten, nämlich Name, Rechtsform, Vertretungsbefugnis sowie aufrechter Bestand der juristischen Person, zu den Identitätsdaten.[28] Darüber hinaus können andere Identifizierungsverfahren angewendet werden, wenn sie im Hinblick auf die Erfassungsgenauigkeit den aufgelisteten Verfahren zumindest gleichwertig sind.[29]

Nachdem der Anbieter eines Kommunikationsdienstes die Identität durch ein Verfahren erhoben hat, hat er weiters einzelne Stammdaten der Kundschaft zu registrieren und in seiner Kun-

22 ErläutRV 15 BlgNR 26. GP 5; Vorblatt und WFA 15 BlgNR 26. GP 3.
23 ErläutRV 15 BlgNR 26. GP 5; Vorblatt und WFA 15 BlgNR 26. GP 3.
24 BGBl II 2019/7.
25 §§ 3 bis 5 IVO.
26 §§ 3 bis 5 IVO.
27 § 6 Abs 2 Z 1 Finanzmarkt-Geldwäschegesetz BGBl I 2016/118 (FM-GwG).
28 § 6 IVO.
29 § 2 IVO.

dendatenbank zu hinterlegen.[30] Dabei sind durch den Anbieter eines Kommunikationsdienstes gemäß § 166 Abs 2 TKG 2021 zu einer Rufnummer bloß der Titel, der Name und das Geburtsdatum einer Person zu registrieren. Eine Verpflichtung zur Speicherung des obig erwähnten Lichtbildausweises sieht weder § 166 Abs 2 TKG 2021 noch die IVO vor.

Demnach sollten der Titel, der Name, das Geburtsdatum und die vom Anbieter zugeteilte Rufnummer ausreichend sein, um eine Person (sei es von dem Anbieter selbst oder von einer zum Erhalt einzelner Stammdaten ermächtigten Behörde zum Zweck der Strafverfolgung oder Gefahrenabwehr) eindeutig identifizieren zu können.[31] Weitere Stammdaten, wie ua die Wohnadresse, sind nach dem Gesetzgeber für die Identifizierung von Personen nicht notwendig.[32] Hierzu ist allerdings anzumerken, dass möglicherweise zwei oder mehrere Menschen mit genau demselben Namen und demselben Geburtsdatum existieren. Somit können die Daten auch zu einer Verwechslung von Personen führen. In diesem Fall müssen weitere Attribute, wie zB die beim Anbieter eines Kommunikationsdienstes hinterlegte Wohnadresse oder eine verifizierte E-Mail-Adresse zu einer Rufnummer, herangezogen werden, um letztlich die den Anschluss innehabende Person eindeutig eruieren zu können.

Zusammengefasst sind nach dem TKG 2021 im Wesentlichen der akademische Grad, der Name und das Geburtsdatum sowie die vom Anbieter einer Person zugeteilte Rufnummer jene Merkmale, anhand derer eine Person identifiziert werden kann und daher insgesamt als Identitätsdaten iSd TKG 2021 zu subsumieren.

3.2. Strafprozessordnung[33] (StPO)

Auch in der StPO besteht mit § 118 eine Rechtsgrundlage, die die Feststellung der Identität zur Aufklärung einer Straftat zum Inhalt hat. Nach dieser Bestimmung können zum Zweck der Identitätsfeststellung seitens der Kriminalpolizei insbesondere der Name, das Geschlecht, das Geburtsdatum, der Geburtsort, der Beruf und die Wohnanschrift eines Menschen (durch Personenbefragung oder Einsicht in Ausweisdokumente) ermittelt werden.[34] Darüber hinaus sind nach der genannten Rechtsgrundlage die Größe eines Menschen, Fotografien, die Stimme sowie Papillarlinienabdrücke geeignete Attribute, um die Identität einer Person feststellen zu können.[35]

Im Gegensatz zu den im TKG 2021 aufgelisteten Stammdaten, die vom Anbieter eines Kommunikationsdienstes zur Rufnummer eines Nutzers zwingend zu registrieren sind (Titel, Name

---

30 § 166 Abs 2 TKG 2021.
31 ErläutRV 15 BlgNR 26. GP 5.
32 *Forgó* in *Steinmaurer*, TKG 2021 § 166 Rz 11 (Stand 1.9.2024, rdb.at).
33 BGBl 1975/631.
34 *Kollmann/Moser* in *Birklbauer/Haumer/Nimmervoll/Wess*, StPO - Linzer Kommentar zur Strafprozessordnung § 118 Rz 6 (Stand 11.2020, lexisnexis.at).
35 § 118 Abs 2 StPO.

und Geburtsdatum), sind die in § 118 StPO genannten Identitätsdaten um einiges umfangreicher ausgestaltet. Daher ist die Kombination dieser Daten jedenfalls besser geeignet, um einen Menschen im Anlassfall zweifellos bestimmen zu können.

3.3. E-Government-Gesetz[36] (E-GovG)

Zudem enthält das E-GovG, das die elektronische Kommunikation zwischen Bürgern und Behörden regelt, auch eine Begriffsbestimmung der „Identität".[37] Diese stellt darauf ab, dass ein Betroffener durch Merkmale derart bezeichnet werden muss, dass er von anderen unterschieden werden kann.[38] Die entsprechenden Merkmale, die diese Anforderung erfüllen, werden in der Begriffsbestimmung demonstrativ aufgelistet und umfassen beispielsweise den Namen, das Geburtsdatum sowie eine nummerische Bezeichnung.[39]

3.4. Datenschutz-Grundverordnung[40] (DSGVO)

Weiters wird in Art 4 Z 1 DSGVO sowie in Art 12 DSGVO auf Identifizierbarkeit von Menschen Bezug genommen.

Art 4 Z 1 DSGVO definiert „personenbezogene Daten" als „*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen*".
Eine natürliche Person gilt dann als identifiziert, wenn gewisse Attribute gegeben sind, die sich ausschließlich auf ein einzelnes Individuum beziehen.[41]
Identifizierbar ist eine Person dann, wenn sie „*direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann*".[42]
Von der DSGVO wird hinsichtlich der Identifizierbarkeit demnach auch auf besondere (nicht abschließend aufgezählte) Merkmale abgezielt, die auf ein Individuum zutreffen. Beispiele von Kennzeichen zur Identifizierung von Personen sind der Name, das Geburtsdatum, die Sozialversicherungsnummer, die Telefonnummer sowie Online-Kennungen wie IP-Adressen.[43] Für die

---

36 BGBl I 2004/10.
37 ErläutRV 252 BlgNR 22. GP 1; § 1 und § 2 Z 1 E-GovG.
38 § 2 Z 1 E-GovG.
39 § 2 Z 1 E-GovG.
40 DSGVO 2016/679 ABl L 2016/119, 1.
41 *Bergauer* in *Jahnel* (Hrsg), Kommentar zur Datenschutz-Grundverordnung (2021) Art 4 Z 1 Rz 14.
42 Art 4 Z 1 DSGVO.
43 *Bergauer* in *Jahnel* (Hrsg), Datenschutz-Grundverordnung Art 4 Z 1 Rz 21.

Identifizierbarkeit genügt es grundsätzlich, dass irgendjemand mit rechtlich zulässigen Mitteln sowie vertretbarem und zumutbarem Aufwand die Zuordnung der Merkmale zu einer konkreten Person vornehmen kann.[44]

Ferner hat Art 12 DSGVO die Überprüfung der Identität zum Inhalt. Demnach hat ein Verantwortlicher iSd DSGVO die Möglichkeit, im Zusammenhang mit der Ausübung der nach der DSGVO zustehenden Rechte betroffener Personen deren Identität zu überprüfen.[45] Dadurch soll Missbrauch verhindert werden und somit sichergestellt werden, dass nur die tatsächlich berechtige Person ihre Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung sowie Datenübertragbarkeit ihrer Daten wahrnehmen und Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten erheben kann.[46]
Je nach konkretem Fall kann zur Feststellung der Identität bspw die Vorlage einer Kundennummer oder Personalnummer ausreichend sein.[47] Weiters kann die Identität zB durch eine Kopie eines amtlichen Lichtbildausweises oder durch eine qualifizierte elektronische Signatur nachgewiesen werden.[48]

Folglich können jedenfalls die in diesem Punkt demonstrativ aufgelisteten Daten als Identitätsdaten iSd DSGVO bezeichnet werden.

3.5. Ergebnis

Die obigen Ausführungen beziehen sich im Wesentlichen auf die Mittel zur Identifizierung von Personen. Diese sind je nach Rechtsgrundlage verschieden. So werden in den Rechtsgrundlagen jeweils unterschiedliche Daten genannt, die Rückschlüsse zu einer Person zulassen und somit eine Person ausmachen.
Meines Erachtens ist die Begriffsdefinition im E-GovG am treffendsten ausgestaltet – denn eine Person wird durch jene Attribute charakterisiert, die sie von allen anderen Menschen unterscheidet. Dementsprechend sind davon alle Merkmale umfasst, die stets ausschließlich einem Individuum zweifelsfrei zugeordnet werden können.[49]
Je nach Umstand ist für die zweifelsfreie Identifikation einer Person die Zuordnung von einzelnen Merkmalen oder eine Kombination an Merkmalen erforderlich. So kann für die Identifizie-

---

44 *Bergauer* in *Jahnel* (Hrsg), Datenschutz-Grundverordnung Art 4 Z 1 Rz 20; DSB 22.12.2021, D155.027 2021-0.586.257.
45 Art 12 DSGVO.
46 *Illibauer* in *Knyrim,* DatKomm Art 12 DSGVO Rz 73/1(Stand 1.7.2024, rdb.at).
47 *Datenschutzbehörde*, Formulare https://dsb.gv.at/eingabe-an-die-dsb/formulare (Antrag gemäß Art. 15 DSGVO auf Auskunft / Request for Access (Article 15 GDPR), Stand 4.2020).
48 *Illibauer* in *Knyrim,* DatKomm Art 12 DSGVO Rz 76.
49 *Büchel/Hirsch,* Internetkriminalität: Phänomene – Ermittlungshilfen – Prävention^2 (2020) 8.

rung schon ein Name ausreichend sein. Bei Namensgleichheit werden aber zusätzliche Merkmale zu erheben sein, damit die betreffende Person eindeutig von anderen abgegrenzt werden und somit identifiziert werden kann.[50]

Darüber hinaus sollte bei der Begriffsdefinition von Identitätsdaten auch auf folgende Frage abgestellt werden:
Welche Daten, die sich auf eine Person beziehen, können missbräuchlich verwendet werden, womit im Endeffekt negative Folgen für die tatsächlich zur Nutzung der Daten berechtigte Person verbunden sind?
Dies wird auf alle Attribute zutreffen, die auf eine konkrete Person hinführen, wie unter anderem der Name einer natürlichen oder juristischen Person, die Ausweisnummer, die Rufnummer sowie die Kontonummer. All jene personenbezogenen Daten, durch deren missbräuchliches und somit unbefugtes Verwenden durch Dritte der tatsächlich berechtigten Person ein Schaden zugefügt werden kann (sei es zB die Schädigung des Vermögens oder der Reputation[51]), charakterisieren meiner Auffassung nach die Identitätsdaten.

4. Formen von Identitätsmissbrauch

Bereits im Jahr 2019 gab knapp die Hälfte der Österreicher an, sie seien besorgt, dass jemand ihre persönlichen Daten erlangt und sodann mit ihrer Identität auftritt.[52]

Es existieren unterschiedliche Auffassungen hinsichtlich der Definition von Identitätsmissbrauch. Einige nehmen eine Trennung zwischen Identitätsdiebstahl (womit die unbefugte Beschaffung fremder Identitätsdaten gemeint ist) und Identitätsmissbrauch (worunter der unberechtigte Gebrauch dieser fremden Identitätsdaten fällt) vor.[53]
Es ist jedenfalls jener Auffassung zuzustimmen, wonach das unbefugte Sichverschaffen fremder Identitätsdaten und der Gebrauch dieser Daten zeitlich getrennte Handlungen darstellen.[54] Dennoch ist die Verwendung des Begriffs „Identitätsdiebstahl“ für die zuvor genannte erste Handlung aus juristischer Sicht unzutreffend. In dieser Hinsicht ist ua *Reindl-Krauskopf* zu folgen, die zutreffend darlegt, dass bei der Verschaffung von Identitätsdaten kein Diebstahl iSd

---

50 *Bergauer* in *Jahnel* (Hrsg), Datenschutz-Grundverordnung Art 4 Z 1 Rz 15.
51 *Büchel/Hirsch,* Internetkriminalität[2] 9.
52 *Statista GmbH*, Wie besorgt sind Sie, dass Sie im Internet Opfer eines Identitätsdiebstahls werden könnten? https://de.statista.com/statistik/daten/studie/542843/umfrage/grad-der-besorgnis-der-eu-buerger-in-bezug-auf-identitaetsdiebstahl-im-internet/#statisticContainer (abgefragt am 3.4.2025).
53 *Bartz*, Identitätsdiebstahl 91-94; siehe dazu auch *Borges/Schwenk/Stuckenberg/Wegener*, Identitätsdiebstahl und Identitätsmissbrauch im Internet 22-24.
54 *Bartz*, Identitätsdiebstahl 94.

StGB vorliegt.[55] Für eine Subsumierung unter § 127 StGB scheitert es unter anderem an der geforderten Körperlichkeit des Gegenstandes, da es sich bei Identitätsdaten nicht um Sachen, sondern um Datensätze bzw Informationen handelt.[56] Identitätsdaten stellen somit kein taugliches Tatobjekt dar.[57] Zudem liegt keine Wegnahme iSd § 127 StGB vor, da auch die vom Missbrauch betroffene Person ihre Identitätsdaten selbst weiter gebraucht und unter ihrer Identität auftritt.[58]

Dementsprechend wird der Begriff „Identitätsdiebstahl" in gegenständlicher Arbeit nicht weiter herangezogen. Vielmehr werden im Folgenden sowohl die Erlangung der Kenntnis von Identitätsdaten als auch die Verwendung dieser Daten als „Identitätsmissbrauch" bezeichnet.[59]

Es gibt verschiedenartige Motive, weshalb versucht wird, an die Identitätsdaten von Opfern zu gelangen und sodann deren Identität anzunehmen. So kann das Ziel davon beispielsweise das Lukrieren von Vermögen oder die Diskreditierung des vom Missbrauch betroffenen Individuums sein.[60]
In der heutigen Zeit kann nahezu jede Person Identitätsmissbrauch im Rahmen der Telekommunikation erfahren, da laut einer Studie im Jahr 2023 bereits rund 90% der Österreicher ab 15 Jahren über ein Smartphone verfügten.[61] Anfang 2024 stecken in Österreich rund 13,7 Millionen SIM-Karten in mobilen Endgeräten.[62] Weiters ergab eine Studie der RTR-GmbH vom Juli 2022, dass rund 90% der Befragten klassische Telefonie-Dienste sowie Messengerdienste (wie WhatsApp oder Facebook Messenger) privat zumindest monatlich nutzen.[63] Auch E-Mail-Dienste werden von den Betroffenen zu 97% zumindest monatlich privat genutzt.[64]
Dieser Umstand eröffnet der Täterschaft die Möglichkeit, mit einer Vielzahl an potenziellen Opfern in Kontakt zu treten (dies wird oftmals mit der Versendung von Massen-Nachrichten erreicht).[65]

---

55 *Reindl-Krauskopf*, ÖJZ 2015/19, 112 (114).
56 *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 26; *Salimi* in *Triffterer/Rosbaud/Hinterhofer* StGB: Salzburger Kommentar zum StGB § 127 Rz 24 (27. Lfg, Stand 11.2012, lexisnexis.at).
57 *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 26.
58 *Reindl-Krauskopf*, ÖJZ 2015/19, 112 (114); siehe dazu auch *Borges/Schwenk/Stuckenberg/Wegener*, Identitätsdiebstahl und Identitätsmissbrauch im Internet 202.
59 *Reindl-Krauskopf*, ÖJZ 2015/19, 112 (114).
60 *Büchel/Hirsch,* Internetkriminalität² 9; *Reindl-Krauskopf*, ÖJZ 2015/19, 112 (114).
61 *Statista GmbH*, Anteil der Smartphone-Besitzer sowie Nutzung von Mobile Commerce in Österreich von 2013 bis 2023 https://de.statista.com/statistik/daten/studie/568185/umfrage/smartphone-besitz-und-smartphone-nutzung-in-oesterreich/ (abgefragt am 3.4.2025).
62 *Rundfunk und Telekom Regulierungs-GmbH*, 5G-SIM-Karten setzen sich immer mehr durch: Österreicher:innen upgraden auf neueste Netztechnik https://www.rtr.at/TKP/presse/pressemitteilungen/presseinformationen_2024/pinfo10102024tkp.de.html (Stand 10.10.2024).
63 *Rundfunk und Telekom Regulierungs-GmbH*, Nutzung von Kommunikationsdiensten im Internet (2022) 12, 36.
64 *Rundfunk und Telekom Regulierungs-GmbH*, Nutzung von Kommunikationsdiensten im Internet (2022) 12.
65 Siehe dazu beispielsweise *Bundeskriminalamt*, Prävention: Tochter-Sohn-Trick https://www.bundeskriminalamt.at/news.aspx?id=582B3033474E43655243633D (Stand 11.11.2022).

Im Folgenden werden einzelne Begehungsweisen näher dargestellt, bei denen Identitätsdaten erlangt werden und diese fremden Daten sodann unbefugt für eigene Handlungen herangezogen werden.[66] Die betreffenden Handlungen können auch als Cybercrime-Delikte bzw Straftaten der Computerkriminalität[67] bezeichnet werden. Zwar werden die Begriffe und demnach die Zuordnung der Straftaten kontrovers diskutiert[68], die Abgrenzung des Bundeskriminalamts erscheint aber meiner Ansicht nach am treffendsten. Dieses unterscheidet Cybercrime im engeren Sinne und Cybercrime im weiteren Sinne. Im Rahmen von Cybercrime im engeren Sinn wird die Informations- und Kommunikationstechnik (IKT) als Angriffsziel betrachtet – dh, dass die Straftraten grundsätzlich „*gegen die Netzwerke selbst oder aber gegen Geräte, Daten oder Dienste in diesen Netzwerken gerichtet*" sind (als Beispiel kann hier die Datenfälschung genannt werden).[69] Dagegen sind vom Cybercrime im weiteren Sinn Straftaten umfasst, bei denen die IKT „*als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten*" eingesetzt wird.[70] Dies kann unter anderem bei Betrugsdelikten der Fall sein.[71]

Cornelia Koller, ehemalige Präsidentin der Vereinigung österreichischer Staatsanwältinnen und Staatsanwälte, wies darauf hin, dass Cybercrime-Delikte *„[...] regelmäßig mit starkem Auslandsbezug, komplexen Sachverhalten und hohem technischen Know-how verbunden [...]",* sind.[72]

4.1. Spoofing

Identitätsmissbrauch kann unter anderem durch sogenanntes Spoofing durchgeführt werden.[73] Aus dem Englischen ins Deutsche wird der Terminus Spoofing mit „Manipulation", „Verschleierung" bzw „Vortäuschung" übersetzt.[74]
In der Praxis existieren unterschiedliche Varianten von Spoofing, wobei es sich im Rahmen der Telekommunikation zB auf Rufnummern oder E-Mail-Adressen beziehen kann.[75]

---

66 *Meyer*, Identität und virtuelle Identität natürlicher Personen im Internet (2011) 39.
67 Siehe dazu *Spornberger*, IT-Strafrecht – IT-Strafrecht im Überblick, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021) Rz 16.2, der darauf hinweist, dass die „Convention of Cybercrime" vom 31.11.2001 mit „Übereinkommen über Computerkriminalität" übersetzt wird.
68 Siehe dazu unter anderem *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht: Cyberdelikte und Ermittlungsbefugnisse (2018) 1; *Bergauer*, Computerstrafrecht, in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht: Profiwissen für die Praxis[2] (2022) Rz 11.1 ff.
69 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 24-25.
70 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 26.
71 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 26.
72 *Moser,* Evaluierung des Rückgangs der Anfallszahlen bei Gericht, Österreichisches Anwaltsblatt 2019/194, 461 (467).
73 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 71.
74 *Borges/Schwenk/Stuckenberg/Wegener*, Identitätsdiebstahl und Identitätsmissbrauch im Internet 30.
75 *Bartz*, Identitätsdiebstahl 94-95; *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

Die Täterschaft verfälscht dabei mit technischen Mitteln ihre Kennung (Rufnummer oder E-Mail-Adresse), um ihre Identität zu verdecken.[76] Dadurch tritt sie gegenüber denjenigen Personen, die die Nachricht oder den Anruf erhalten, unter einer falschen Identität auf.[77] Bei den Empfängern wird der Eindruck erweckt, dass der reale Inhaber einer Rufnummer oder E-Mail-Adresse für das Versenden der betreffenden Nachricht bzw das Tätigen des Anrufs verantwortlich ist, obwohl dies nicht der Fall ist.[78]

Spoofing wird oftmals im Zusammenhang mit betrügerischen Handlungen verübt (siehe dazu bspw den Polizisten-Trick und CEO-Fraud unter den Punkten 4.2.1 und 4.2.2). Die technische Manipulierung der Kennungen kann meist ohne großen Aufwand erfolgen – eine Reihe solcher Spoofing-Tools können im Internet aufgerufen oder heruntergeladen werden.[79]

Sofern dabei eine tatsächlich existierende Rufnummer oder E-Mail-Adresse, die jemandem vom Anbieter zugeteilt wurde, verwendet wird, kann dies für den Eigentümer dieser Identitätsdaten schwerwiegende Folgen nach sich ziehen. Hierbei ist zu erwähnen, dass die Rufnummer jedenfalls seit der unter Punkt 3.1 beschriebenen zwingenden Identifizierung von Personen und Registrierung von Stammdaten gemäß § 166 Abs 2 TKG 2021 als Identitätsdatum anzusehen ist. Mit Einführung dieser Verpflichtung ist für den Anbieter eines Kommunikationsdienstes stets nachvollziehbar, welche Person hinter der zugeteilten Rufnummer steht – eine Rufnummer ist somit in jedem Fall auf ein Individuum rückführbar.
Allem voran wird durch Spoofing der tatsächliche Rufnummerninhaber Ermittlungen von Strafverfolgungsbehörden ausgesetzt werden, obwohl er die betreffende Straftat nicht begangen hat.[80] Mit der notwendigen Entkräftung der Anschuldigungen gehen vor allem auch psychische Belastungen einher.[81] Sofern das Tatsubjekt mit der gefälschten Rufnummer zahlreiche missbräuchliche Anrufe getätigt hat, besteht weiters die Möglichkeit, dass die Person, die der wahre Rufnummerninhaber ist, zahlreiche Rückrufe erhält.[82]
Auch für jene Person, die Empfänger des Anrufs oder der Nachricht ist und der hinter dem Anruf/der Nachricht stehenden Person ihr Vertrauen entgegenbrachte, können negative Konsequenzen verbunden sein. Dies soll anhand einzelner Beispiele im nächsten Punkt veranschaulicht werden.

---

76 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 71.
77 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 71.
78 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 71.
79 Siehe dazu beispielsweise https://emkei.cz/.
80 Siehe dazu *Österreichisches Institut für angewandte Telekommunikation (ÖIAT)*, Identitätsdiebstahl 15.
81 Siehe dazu *Österreichisches Institut für angewandte Telekommunikation (ÖIAT)*, Identitätsdiebstahl 15.
82 *Rundfunk und Telekom Regulierungs-GmbH*, Manipulation von Rufnummern https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/spam-unerwuenschte_anrufe_und_nachrichten/manipulation_von_telefonnummern.de.html (abgefragt am 3.4.2025).

4.2. Arten von betrügerischen Anrufen oder Nachrichten

In diesem Punkt werden gängige Handlungen aufgelistet, bei denen kriminelle Personen im Rahmen von Anrufen oder Nachrichten unter einer fremden Identität auftreten. Das englische Wort für „Betrug“ lautet „Scam“, weswegen die nachfolgenden Handlungen auch als Scam-Anrufe oder Scam-Nachrichten bezeichnet werden.[83]

4.2.1. Polizisten-Trick

Laut dem Jahresbericht der Schlichtungsstellen 2022 der RTR-GmbH sind die Meldungen von Betrugsanrufen im Jahr 2022 im Gegensatz zu den vorherigen Jahren drastisch gestiegen.[84] Am häufigsten wurden Betrugsanrufe, bei denen sich die Betrüger als Polizisten ausgaben, wahrgenommen und gemeldet.[85]

Im Rahmen der Anrufe schienen – aufgrund der Anwendung von Spoofing – wiederum vertrauenswürdige österreichische Telefonnummern auf.[86] Diese Art von Anrufen wurde in einigen Fällen mittels Call-Bots verübt.[87] Das bedeutet, dass nach Abheben des Telefonats eine Tonbandstimme erklingt, die den Empfänger des Anrufs auffordert, eine bestimmte Tastenkombination zu drücken.[88] Daraufhin werden die Opfer zu vermeintlichen Polizisten weitergeleitet, die ihnen beispielsweise mitteilen, es wären verdächtige Aktivitäten auf ihrem Bankkonto vorgenommen worden oder sie hätten an strafbaren Handlungen mitgewirkt.[89] Im Zuge dessen werden die

---

83 *Rundfunk und Telekom Regulierungs-GmbH*, Scam-Anrufe/Phishing-Anrufe https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/information/informationen_fuer_konsumenten/TKKS_Spam.de.html (abgefragt am 3.4.2025).

84 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT Schlichtungsstellen 2022 (2023) 29.

85 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT Schlichtungsstellen 2022 (2023) 30.

86 *Rundfunk und Telekom Regulierungs-GmbH*, Betrugsanrufe vom "Austrian Police Department" schlagen derzeit hohe Wellen: einfach ignorieren und auflegen! https://www.rtr.at/TKP/presse/pressemitteilungen/pressemitteilungen/pinfo26072022tkp.de.html (Stand 26.7.2022).

87 *Rundfunk und Telekom Regulierungs-GmbH*, Betrugsanrufe vom "Austrian Police Department" schlagen derzeit hohe Wellen: einfach ignorieren und auflegen! https://www.rtr.at/TKP/presse/pressemitteilungen/pressemitteilungen/pinfo26072022tkp.de.html (Stand 26.7.2022); *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021: Lagebericht über die Entwicklung von Cybercrime (2022) 15.

88 *Rundfunk und Telekom Regulierungs-GmbH*, Betrugsanrufe vom "Austrian Police Department" schlagen derzeit hohe Wellen: einfach ignorieren und auflegen! https://www.rtr.at/TKP/presse/pressemitteilungen/pressemitteilungen/pinfo26072022tkp.de.html (Stand 26.7.2022); *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 15.

89 *Rundfunk und Telekom Regulierungs-GmbH*, Betrugsanrufe vom "Austrian Police Department" schlagen derzeit hohe Wellen: einfach ignorieren und auflegen! https://www.rtr.at/TKP/presse/pressemitteilungen/pressemitteilungen/pinfo26072022tkp.de.html (Stand 26.7.2022); *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 15.

Opfer meist aufgefordert, Geldtransfers zu veranlassen.[90]
Im September 2022 gelang es dem Bundeskriminalamt, Interpol und der indischen Polizeibehörde CBI ein für den Betrug verantwortliches Call-Center ausfindig zu machen und die dafür zuständigen Personen festzunehmen.[91] Im Jahr 2022 ist insgesamt ein Schaden von 15 Millionen Euro im Zusammenhang mit dem Trick der falschen Polizeibeamten entstanden.[92]

4.2.2. CEO-Fraud

Ein weiteres stets wiederkehrendes Phänomen, im Rahmen dessen E-Mail-Spoofing angewendet wird, ist der sogenannte CEO-Fraud. Dabei fälschen die Absender einer Nachricht ihre E-Mail-Adresse und verwenden eine, einer Führungsposition eines Unternehmens zugehörige, existierende E-Mail-Adresse. Die Täterschaft versendet sodann an einzelne relevante Beschäftigte eines Unternehmens (insbesondere an Beschäftigte der Buchhaltung) eine E-Mail. In dieser gibt sie sich als Führungskraft aus und fordert die Beschäftigten auf, rasch Überweisungen – meist an ausländische Konten – zu tätigen. Dadurch wird bei den zuständigen Personen eine Drucksituation erzeugt, die in einzelnen Fällen auch zum Tätigen der Überweisungen führt.[93]

4.2.3. Tochter-Sohn-Trick

In jüngster Vergangenheit wurde von der Täterschaft die Tochter-Sohn-Masche angewendet.[94] Bei dieser Methode erhalten Opfer SMS oder WhatsApp-Nachrichten über eine ihnen unbekannte Rufnummer, in denen sich Betrüger als Angehörige der potenziellen Opfer ausgeben.[95] Dabei wird vorgegeben, dass sie Hilfe benötigen, beispielsweise, dass das Mobiltelefon des Kindes kaputt gegangen sei oder das Online-Banking nicht funktioniere.[96] So werden die Opfer verleitet, Überweisungen für ihre vermeintlichen Kinder zu tätigen, um ihnen aus der vorgespielten Notsituation zu helfen.[97]

---

90 *Rundfunk und Telekom Regulierungs-GmbH*, Betrugsanrufe vom "Austrian Police Department" schlagen derzeit hohe Wellen: einfach ignorieren und auflegen! https://www.rtr.at/TKP/presse/pressemitteilungen/pressemitteilungen/pinfo26072022tkp.de.html (Stand 26.7.2022); *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 15.

91 *Bundesministerium für Inneres*, Bundeskriminalamt: Ermittlungserfolg gegen „falsche Polizisten“ am Telefon https://www.bundeskriminalamt.at/news.aspx?id=63346C2B366B75663968773D (Stand 17.11.2022).

92 *Salzburger Nachrichten Medien GmbH & Co. KG*, Fast jeder zweite Betrug wird im Internet verübt https://www.sn.at/panorama/oesterreich/fast-jeder-zweite-betrug-wird-im-internet-veruebt-143270104 (Stand 7.8.2023).

93 Siehe zum betreffenden Absatz insgesamt *Teichmann/Falker*, CEO-Fraud: Empfehlungen für das Legal Risk Management, GRCaktuell 2021, 48; *Spornberger*, IT-Strafrecht – IT-Strafrecht im Überblick, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021) Rz 16.90.

94 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 28.

95 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 28.

96 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 28.

97 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 28.

Zwischen Oktober und Dezember 2022 wurden österreichweit monatlich rund 880 derartige Fälle angezeigt.[98] Die Dunkelziffer wurde vom Bundeskriminalamt als weit höher eingeschätzt.[99] Die Auswirkungen dieser Welle an betrügerischen Nachrichten war beträchtlich – im Jahr 2022 soll ein Schaden von 6 Millionen Euro entstanden sein.[100]

Das Szenario setzte sich auch im Jahr 2023 fort.[101] So war die Anzahl der Meldungen zu Betrugs-SMS 2023 im Vergleich zum Jahr 2022 um einiges höher.[102] Die Steigerung wurde vor allem durch den Tochter-Sohn-Trick sowie durch die vorgetäuschte Kontaktaufnahme von Banken, Postdiensteanbietern und Behörden erwirkt.[103]

Diese betrügerischen Mitteilungen sowie die zuvor genannten Methoden werden auch als „Social Engineering" bezeichnet, da menschliche Schwachstellen ausgenutzt werden. So werden im Rahmen der Betrugsmaschen Personen über die Identität und die Absicht des Tatsubjekts getäuscht. Dabei wird das Vertrauen oder die Autorität ausgenutzt, wodurch die Opfer größtenteils dazu verleitet werden, vertrauliche Informationen zu übermitteln oder Überweisungen zu tätigen.[104]

4.3. Phishing

Als eine weitere Erscheinungsform von Identitätsmissbrauch ist Phishing (welches eine Kombination der Wörter „Password" und „Fishing" darstellt) zu nennen.[105]
Es gibt verschiedenste Formen von Phishing, dessen Ziel es ist, sich Kenntnis von fremden Passwörtern und weiteren persönlichen Informationen zu verschaffen.[106] Eine klassische Vari-

---

98 *Standard Verlagsgesellschaft m.b.H*, Eklatant steigende Fallzahlen von „Tochter-Sohn-Betrug" https://www.derstandard.at/story/2000141679885/eklatant-steigende-fallzahlen-von-tochter-sohn-betrug (Stand 10.12.2022).

99 *Standard Verlagsgesellschaft m.b.H*, Eklatant steigende Fallzahlen von „Tochter-Sohn-Betrug" https://www.derstandard.at/story/2000141679885/eklatant-steigende-fallzahlen-von-tochter-sohn-betrug (Stand 10.12.2022).

100 Siehe dazu *Salzburger Nachrichten Medien GmbH & Co. KG*, Fast jeder zweite Betrug wird im Internet verübt https://www.sn.at/panorama/oesterreich/fast-jeder-zweite-betrug-wird-im-internet-veruebt-143270104 (Stand 7.8.2023).

101 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT Schlichtungsstellen 2023 (2024) 28.

102 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT Schlichtungsstellen 2023 (2024) 29.

103 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT Schlichtungsstellen 2023 (2024) 28.

104 Siehe zum betreffenden Absatz insgesamt *Bundesamt für Sicherheit in der Informationstechnik*, Social Engineering – der Mensch als Schwachstelle https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html (abgefragt am 3.4.2025); *Akinlade*, Grundlagen der Informatik und IT-Security – Security als Managementfunktion, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021) Rz 3.25.

105 *Bergauer*, Das materielle Computerstrafrecht (2016) 404.

106 Siehe dazu unter anderem *Spornberger*, IT-Strafrecht – IT-Strafrecht im Überblick, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021) Rz 16.89 ff.

ante davon ist Phishing per E-Mail.[107] Bei dieser Methode werden Nachrichten von vermeintlich echten Unternehmen oder staatlichen Einrichtungen an zahlreiche Personen versendet, in denen unterschiedlichste Umstände vorgetäuscht werden (zB das E-Mail-Postfach sei voll, weswegen umgehend zusätzlicher Speicher freizuschalten wäre).[108]

Im Zuge der Nachricht wird dem Empfänger nahegelegt, auf einen Link zu klicken, damit das behauptete Problem, wie zB das vorgetäuschte volle Postfach, behoben werden kann. Der entsprechende Link führt jedoch auf eine von der Täterschaft manipulierte Seite. Dies ist für das Opfer oftmals schwer ersichtlich, da die graphische Darstellung der offiziellen Webseite des echten Unternehmens nahezu gleicht. Als Folge dessen werden die Empfänger auf der manipulierten Webseite zur Eingabe ihrer Daten verleitet, zB um sich in ihr vermeintlich echtes Nutzerkonto einzuloggen, um weiteren Speicherplatz für ihr E-Mail-Postfach zu kaufen. Diese Zugangsdaten werden aber an die dahinterstehende Täterschaft weitergeleitet, wodurch sich diese Zugriff auf die einzelnen Nutzerkonten und die dort hinterlegten Daten verschafft. In diesem Zusammenhang werden fallweise auch weitere Daten, wie Bankdaten, abgefragt. Dadurch besteht die Möglichkeit, dass der Täterschaft zahlreiche Identitätsdaten offengelegt werden.[109]

Eine weitere Form von Phishing ist „Smishing", worunter Phishing durch das Versenden von SMS zu verstehen ist.[110] Phishing-Nachrichten im Rahmen von Instant Messaging Diensten (zB WhatsApp) werden „SPIM", das eine Kombination von Spam und Instant Messaging Diensten darstellt, genannt.[111] Die Vorgehensweise bei Smishing und SPIM gleicht jener, wie der zuvor beschriebenen beim Phishing via E-Mail. Als weitere Methode werden Empfänger bei Smishing und SPIM zur Installation von Malware verleitet.[112]

---

[107] *Bartz*, Identitätsdiebstahl 95.

[108] *Österreichisches Institut für angewandte Telekommunikation (ÖIAT)*, Gefälschtes A1-Mail im Umlauf https://www.watchlist-internet.at/news/gefaelschtes-a1-mail-im-umlauf/ (Stand 31.10.2022); aktuelle Phänomene siehe weiters unter www.watchlist-internet.at/warnungen-tipps/phishing-smishing-vishing.

[109] Siehe zum betreffenden Absatz insgesamt *Bartz*, Identitätsdiebstahl 95-96; *Österreichisches Institut für angewandte Telekommunikation (ÖIAT)*, Gefälschtes A1-Mail im Umlauf https://www.watchlist-internet.at/news/gefaelschtes-a1-mail-im-umlauf/ (Stand 31.10.2022).

[110] *Rundfunk und Telekom Regulierungs-GmbH*, Unerwünschte Nachrichten per SMS, Whatsapp & Co https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/spam-unerwuenschte_anrufe_und_nachrichten/unerwuenschte_sms.de.html (abgefragt am 3.4.2025).

[111] *Rundfunk und Telekom Regulierungs-GmbH*, Unerwünschte Nachrichten per SMS, Whatsapp & Co https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/spam-unerwuenschte_anrufe_und_nachrichten/unerwuenschte_sms.de.html (abgefragt am 3.4.2025).

[112] *Rundfunk und Telekom Regulierungs-GmbH*, Unerwünschte Nachrichten per SMS, Whatsapp & Co https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/spam-unerwuenschte_anrufe_und_nachrichten/unerwuenschte_sms.de.html (abgefragt am 3.4.2025); siehe dazu näher das Phänomen „Flubot" unter Punkt 4.4 der gegenständlichen Master Thesis.

Daneben ist im Rahmen der Telekommunikation das sogenannte „Vishing“ relevant. Dabei wird darauf abgezielt, per Anruf an relevante Daten zu gelangen (Voice-Phishing).[113]

Die beschriebenen Angriffsformen von Phishing sind sehr eng mit der unter Punkt 4.1 beschriebenen Manipulation von Kennungen verbunden. So ist es möglich, dass die Täterschaft ihre potenziellen Opfer über ihre Identität durch das Fälschen der Rufnummernanzeige oder der Anzeige der E-Mail-Adresse täuscht. Dadurch wird das Vertrauen der Empfänger in die Nachricht bzw den Anruf noch weiter gestärkt, weshalb diese unwissend zum Tätigen von für sie nachteiligen Handlungen verleitet werden.[114]

4.4. Schadsoftware am Beispiel von Flubot

Ein Beispiel von Smishing ist der sogenannte Flubot-Virus, auf den im Jahr 2021 nahezu 33.000 Beschwerden bei der Meldestelle für Nummernmissbrauch zurückzuführen sind.[115]
Dabei wird in einer SMS unter anderem die Lieferung eines Pakets vorgetäuscht.[116] In dieser SMS ist ein Hinweis zu einem Link enthalten, der die Opfer auffordert, eine App auf ihrem Smartphone zu installieren.[117] Sofern der Installationsvorgang durchgeführt wird, wird eine Malware, die sich auf Android-Betriebssysteme bezieht, installiert.[118] Dadurch hat die Täterschaft Zugriff auf das Mobiltelefon.[119] Dieses befindet sich mit weiteren infizierten Geräten in einem von den Tätern gesteuerten Bot-Netz, dh, dass die Geräte von Kriminellen ferngesteuert werden und zu bestimmten Aktionen missbraucht werden.[120] Die Malware veranlasst einerseits die unbemerkte massenhafte Versendung weiterer SMS zur Weiterverbreitung des Links im Hintergrund (Smishing).[121] Dadurch können den Opfern zum Teil hohe Kosten bei ihren Kommunikationsanbietern entstehen.[122] Andererseits kann die Täterschaft durch die Schadsoftware die auf dem Mobiltelefon gespeicherten Daten sowie die vom Benutzer des Mobiltelefons durchgeführ-

---

113 *Bartz*, Identitätsdiebstahl 105.
114 Siehe zum betreffenden Absatz insgesamt *Rundfunk und Telekom Regulierungs-GmbH*, Tipps bei Phishing SMS https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/tippsgegenspam/tipps_phishing-sms.de.html (abgefragt am 3.4.2025); siehe beispielsweise *Österreichisches Institut für angewandte Telekommunikation (ÖIAT)*, Post E-Mail „Dein Paket wartet!“ ist fake! https://www.watchlist-internet.at/news/post-e-mail-dein-paket-wartet-ist-fake/ (Stand 2.2.2022).
115 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT der Schlichtungsstellen 2021 (2022) 31.
116 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 12-15.
117 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 12-15.
118 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 12-15.
119 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 13.
120 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 13; *Bundesamt für Sicherheit in der Informationstechnik*, Botnetze-Auswirkungen und Schutzmaßnahmen https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/botnetze_node.html (abgefragt am 3.4.2025).
121 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 12-13.
122 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT Schlichtungsstellen 2021, 28-29.

ten Aktionen ausspähen und so an zahlreiche persönliche Daten, wie Zugangsdaten für Online-Banking, gelangen.[123]

4.5. SIM-Swapping

Sofern der Täter mit seiner Phishing- bzw Social Engineering-Attacke erfolgreich war und dadurch an personenbezogene Daten der Opfer gelangt ist, besteht für die betroffenen Personen mit dem sogenannten „SIM-Swapping" ein weiteres erhebliches Risiko von Identitätsmissbrauch. Bei dieser Methode geben sich Kriminelle unter Angabe der ausgespähten Daten ihrer Opfer gegenüber dem Kommunikationsdiensteanbieter des Opfers als Vertragspartner aus und beantragen für die Rufnummer ihres Opfers eine neue SIM-Karte. Aufgrund des Umstands, dass SMS-Nachrichten oftmals für Zwei-Faktor-Authentifizierungen (beispielsweise für Onlinebanking oder Onlineshops) eingesetzt werden, können Täter nach erfolgreichem SIM-Swapping Zugriff zu den Konten des Opfers erhalten, wodurch die Opfer einen finanziellen Schaden erleiden können.[124]

4.6. Ergebnis

Seitens der Bevölkerung werden jährlich zahlreiche Betrugsanrufe und Betrugs-SMS gemeldet.[125] Es ist jedoch davon auszugehen, dass nicht jede betroffene Person eine Meldung vornimmt. Dies mag daran liegen, dass die Meldestelle für Nummernmissbrauch nicht Jedem bekannt ist oder auch daran, dass der Empfang von betrügerischen Anrufen/Nachrichten von der Bevölkerung bereits als immer gewöhnlicher angesehen wird.[126]
Die gemeldeten Phänomene können sich schlagartig ändern. Beispielsweise wurde im Jahr 2021 der Höhepunkt der Flubot SMS-Welle erreicht, im Jahr 2022 sind demgegenüber massenweise Betrugsanrufe aufgetreten.[127] Im Jahr 2023 wurden über 10.000 Meldungen des Missbrauchs der eigenen Rufnummer erfasst.[128] Künftig könnte bei der Verübung der Straftaten vermehrt künstliche Intelligenz, zB für die Programmierung von Malware oder beim Phishing,

---

123 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2021, 13.
124 Siehe zum betreffenden Absatz insgesamt *Bundesministerium für Soziales, Gesundheit, Pflege und* Konsumentenschutz, Rufnummernmissbrauch über eSIM-Karten https://www.konsumentenfragen.at/konsumentenfragen/Aktuelles/Konsumentenfragen/Rufnummernmissbrauch-ueber-eSIM-Karten.html (Stand 6.2.2024).
125 *Rundfunk und Telekom Regulierungs-GmbH*, Jahresbericht der Schlichtungsstellen 2023 (2024) 29.
126 *Rundfunk und Telekom Regulierungs-GmbH*, Jahresbericht der Schlichtungsstellen 2023 (2024) 29.
127 *Rundfunk und Telekom Regulierungs-GmbH*, Jahresbericht der Schlichtungsstellen 2022 (2023) 28, 29.
128 *Rundfunk und Telekom Regulierungs-GmbH*, Jahresbericht der Schlichtungsstellen 2023 (2024) 29.

zum Einsatz kommen.[129] Mithilfe von künstlicher Intelligenz ist ua die Erstellung und das Versenden von personalisierten Betrugsnachrichten im Schreibstil eines Bekannten oder das Nutzen der Stimme eines Bekannten möglich.[130] Durch den Einsatz von künstlicher Intelligenz für Social Engineering wird das Opfer noch mehr dazu verleitet, vertrauliche Informationen zu übermitteln oder Überweisungen zu tätigen.[131]

Aus den dargestellten Beispielen zeigt sich, dass Identitätsmissbrauch grundsätzlich in zwei Gruppen unterteilt werden kann: Zum einen werden – beispielsweise beim Spoofing oder Phishing – die rechtmäßigen Identitätseigentümer durch das unbefugte Verwenden ihrer Datensätze direkt geschädigt. Andererseits sind vom Missbrauch – wie etwa beim Polizisten-Trick oder Tochter-Sohn-Trick – auch Dritte betroffen. Dies sind jene Personen, die dem Gegenüber, das unbefugterweise eine fremde Identität angenommen hat, ihr Vertrauen entgegenbrachten.

5. Strafrechtliche Beurteilung

In diesem Abschnitt wird untersucht, unter welche Strafrechtsnormen die zuvor beschriebenen kriminellen Handlungen subsumiert werden können.

Einleitend ist hierbei anzumerken, dass kein eigener Straftatbestand des Identitätsmissbrauchs im österreichischen Strafrecht existiert. Zwar stellte die Europäische Kommission vor einigen Jahren in einer Mitteilung hinsichtlich der allgemeinen Politik zur Bekämpfung der Internetkriminalität die Einführung eines europaweit gemeinsamen Straftatbestandes für Identitätsdiebstahl zur Diskussion.[132] Allerdings wurde ein solcher bisher nicht eingeführt. Daher kommen für das Phänomen Identitätsmissbrauch – je nach konkretem Sachverhalt – verschiedene Strafrechtsnormen in Betracht.[133] Aufgrund des weitreichenden strafrechtlichen Schutzes von Identitäts-

---

[129] *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 28; *A-SIT Zentrum für sichere Informationstechnologie – Austria*, KI-basierte Cyberangriffe: Aktuelle Trends und Gefahren https://www.onlinesicherheit.gv.at/Services/News/KI-Cyberattacken-Risiken-Trends.html (Stand 14.11.2023); *A-SIT Zentrum für sichere Informationstechnologie – Austria*, Audio-Deepfakes und Voice-Cloning: So schützen Sie sich vor Betrug https://www.onlinesicherheit.gv.at/Services/News/Audio-Deepfake-Voice-Cloning.html (Stand 12.10.2023).

[130] *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 28; *A-SIT Zentrum für sichere Informationstechnologie – Austria*, KI-basierte Cyberangriffe: Aktuelle Trends und Gefahren https://www.onlinesicherheit.gv.at/Services/News/KI-Cyberattacken-Risiken-Trends.html (Stand 14.11.2023); *A-SIT Zentrum für sichere Informationstechnologie – Austria*, Audio-Deepfakes und Voice-Cloning: So schützen Sie sich vor Betrug https://www.onlinesicherheit.gv.at/Services/News/Audio-Deepfake-Voice-Cloning.html (Stand 12.10.2023).

[131] *A-SIT Zentrum für sichere Informationstechnologie – Austria*, Audio-Deepfakes und Voice-Cloning: So schützen Sie sich vor Betrug https://www.onlinesicherheit.gv.at/Services/News/Audio-Deepfake-Voice-Cloning.html (Stand 12.10.2023).

[132] *Meyer*, Identität und virtuelle Identität natürlicher Personen im Internet (2011) 38; Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen: „Eine allgemeine Politik zur Bekämpfung der Internetkriminalität", KOM (2007) 267 endgültig (22.5.2007) 9-10.

[133] *Reindl-Krauskopf*, ÖJZ 2015/19, 112 (115, 116).

missbrauch durch das geltende materielle Strafrecht wird auch gegenwärtig keine Änderung des Strafrechts durch Einführung einer eigens der Bestrafung von Identitätsmissbrauch dienenden Norm angedacht.[134]

Im Folgenden werden einige für das Phänomen Identitätsmissbrauch einschlägigen Normen, konkret die Datenfälschung gemäß § 225a StGB, der Betrug gemäß § 146 StGB und der schwere Betrug gemäß § 147 Abs 1 Z 1 StGB, die üble Nachrede gemäß § 111 StGB, der besondere Erschwerungsgrund gemäß § 33 Abs 1 Z 8 StGB sowie die Datenverarbeitung in Gewinn- oder Schädigungsabsicht gemäß § 63 DSG näher analysiert. Wie bereits im vorherigen Kapitel erwähnt, kann Identitätsmissbrauch nicht unter das Delikt Diebstahl gemäß § 127 StGB subsumiert werden, weshalb im Folgenden darauf nicht nochmals genauer eingegangen wird.[135]

Die Voraussetzung für die Verfolgung von Taten im Zusammenhang mit Identitätsmissbrauch und somit für die Strafbarkeit ist zunächst, dass das österreichische Strafrecht anwendbar ist. Diese Bedingung ist insbesondere vor dem Hintergrund relevant, dass Cybercrime-Delikte auch vom Ausland aus begangen werden.[136]
So gelten die österreichischen Strafgesetze grundsätzlich für Taten, die im Inland begangen wurden (Territorialitätsprinzip gemäß § 62 StGB).[137] Gemäß § 67 Abs 2 StGB begeht das Tatsubjekt eine mit Strafe bedrohte Handlung im Inland, sofern die Handlung im Inland stattgefunden hat bzw hätte sollen oder der Erfolg eingetreten ist bzw nach den Vorstellungen des Tatsubjekts hätte eintreten sollen. Somit ist beispielsweise im Falle eines Betrugs inländische Gerichtsbarkeit gegeben, wenn der Vermögensschaden in Österreich eintritt.[138]

5.1. Datenfälschung gemäß § 225a StGB

Gemäß § 225a StGB ist jene Person, die „*durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden*“, zu bestrafen (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bis zu 720 Tagessätze).

---

[134] Siehe dazu insbesondere Anfragebeantwortung durch die Bundesministerin für Justiz Dr. Alma Zadić, LL.M. vom 30.5.2023 zu der schriftlichen Anfrage (14796/J) der Abgeordneten Mag. Christian Drobits, Kolleginnen und Kollegen an die Bundesministerin für Justiz betreffend Identitätsdiebstahl https://www.parlament.gv.at/gegenstand/XXVII/AB/14309.
[135] Siehe dazu näher Punkt 4 „Formen des Identitätsmissbrauchs“ der gegenständlichen Master Thesis.
[136] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 4.1.
[137] *Salimi* in *Höpfel/Ratz*, WK² StGB Vor §§ 62 - 67 Rz 6 (Stand 1.3.2022, rdb.at).
[138] *Salimi* in *Höpfel/Ratz*, WK² StGB § 67 Rz 30 (Stand 1.3.2022, rdb.at).

5.1.1. Objektiver Tatbestand

a) Daten

Tatobjekt des gegenständlichen Delikts sind Daten iSd § 74 Abs 2 StGB, worunter sowohl personenbezogene als auch nicht personenbezogene Daten sowie Programme zu verstehen sind.[139] Der Datenbegriff ist somit gesetzlich weit gefasst und inkludiert nach dem Wortlaut grundsätzlich eine Vielzahl an Dokumenten.[140] Laut *Bergauer* wird sich der Tatbestand der Datenfälschung jedoch auf „*automationsunterstützt verarbeitete, übermittelte oder überlassene Daten"* beschränken, da ansonsten auch Daten auf Papier, die im Grunde dem Tatbestand der Urkundenfälschung unterliegen, umfasst wären.[141] Folglich fallen unter Daten iSd § 225a StGB jene Informationen, die „ *in elektronischer oder computertechnisch sonst bearbeitbarer Form vorliegen*".[142]

Die erste Voraussetzung der Verwirklichung des Straftatbestandes ist die Herstellung von falschen oder die Verfälschung von echten automationsunterstützt verarbeiteten Daten.[143]

Im Rahmen der Herstellung von falschen Daten erzeugt das Tatsubjekt neue Daten.[144] Unter den Begriff falsche Daten fallen jene Daten, die über die Identität des Ausstellers täuschen.[145] Der Täter zieht somit eine fremde Identität heran, wodurch er für Dritte den Anschein erweckt, die betreffenden Daten stammen vom eigentlichen Identitätseigentümer.[146] Tatsächlich stammen die Daten jedoch nicht von derjenigen Person, die als Aussteller angegeben ist.[147] Dieser Umstand trifft beispielsweise beim Spoofing von Rufnummern oder E-Mail-Adressen zu, bei dem eine Nachricht gefälscht wird, da sie nicht von dem Aussteller stammt, der in der Nachricht angeführt ist.[148]

Unter die Handlung des Verfälschens von Daten fällt dagegen die Veränderung von bereits vorhandenen echten Daten, wobei es für den Erklärungsadressaten wiederum so erscheint, als würde der Dateninhalt vom tatsächlich ursprünglichen Aussteller der Daten

---

139 *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 3 (Stand 1.1.2017, rdb.at).
140 *Bergauer*, Computerstrafrecht (2016) 393.
141 *Bergauer*, Computerstrafrecht (2016) 393, 394.
142 *Jerabek/Ropper/Reindl-Krauskopf/Schroll/Oberressl* in *Höpfel/Ratz*, WK² StGB § 74 Rz 65 (Stand 1.5.2024, rdb.at).
143 § 225a StGB.
144 *Tipold* in *Leukauf/Steininger*, StGB⁴ § 225a Rz 6 (Stand 1.10.2016, rdb.at).
145 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.210; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 4, 5.
146 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.210; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 4, 5.
147 *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.240.
148 *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.240.

herkommen.[149] Davon kann unter anderem der Austausch des Namens oder Fotos eines digitalen Ausweises umfasst sein, da es sich hierbei um eine echte elektronische Urkunde handelt, die verfälscht wird.[150]

Neben der Herstellung von falschen Daten bzw der Verfälschung von echten Daten ist die sogenannte Perpetuierungsfunktion von Relevanz. Das bedeutet, dass die betreffenden Daten nicht sofort wieder gelöscht werden können, sondern längerfristig verkörpert sein müssen.[151]

Darüber hinaus verlangt § 225a StGB die Rechtserheblichkeit von Erklärungen. So muss das elektronische Dokument rechtserheblich sein und dementsprechend Beweisfunktion haben.[152] Dies wäre beispielsweise bei einer Nachricht, mit der um die dringende Überweisung eines Geldbetrags mit einer gespooften Rufnummer (und somit um eine Schenkung) ersucht wird (zB Tochter-Sohn-Trick) der Fall.[153]

Letztlich hat der Aussteller des betreffenden Dokuments ersichtlich zu sein (sogenannte Garantiefunktion).[154] Dieser kann unter anderem durch die (elektronische) Signatur eines Dokuments oder aus anderen Umständen (wie aus der Rufnummer oder E-Mail-Adresse) erkennbar sein, sofern sich daraus für den Empfänger der Nachricht auf eine bestimmte Person schließen lässt.[155]

b) Tathandlung

Gemäß § 225a StGB werden die Fälschungen durch Eingabe, Veränderung, Löschung oder Unterdrückung hergestellt. Dabei handelt es sich um eine taxative Aufzählung von Tathandlungen.[156]

Beim Eingeben von Daten werden neue Daten durch Eingabegeräte (zB mittels Tastatur) hinzugefügt.[157] Die Veränderung von Daten betrifft unter anderem die Änderung von

---

[149] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.211, 2.212; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 6.

[150] *Bergauer*, Computerstrafrecht (2016) 400; *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.235.

[151] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.214; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 8, 9.

[152] *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.236.

[153] Siehe als ähnlichen Fall einer rechtserheblichen Erklärung das Ersuchen um Darlehnsgewährung auf Facebook in *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.216.

[154] *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 13.

[155] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.216-2.218; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 13-15.

[156] *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 18.

[157] *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.242.

Erklärungen.[158] Auch die unwiderrufliche Löschung von Daten bewirkt die Änderung der Erklärung.[159] Unterdrückt werden Daten, wenn sie zurückgehalten werden.[160]

5.1.2. Subjektiver Tatbestand

Bei der Datenfälschung handelt es sich um ein Vorsatzdelikt.[161] Das Tatsubjekt muss demnach mit dolus eventualis betreffend die Herstellung von falschen Daten bzw die Verfälschung von echten Daten handeln.[162]
Daneben hat der Täter mit erweitertem Vorsatz auf Gebrauch der betreffenden Daten zum Beweis eines Rechts, eines Rechtsverhältnisses oder einer Tatsache, somit mit Täuschungsvorsatz, zu handeln.[163] Eine solche Täuschung ist jedoch nur gegenüber Menschen und nicht gegenüber Maschinen möglich, da nur Menschen einen Willen bilden können.[164]
Insofern wird die Verwirklichung des Straftatbestands der Datenfälschung entsprechend eingeschränkt.

5.1.3. Strafaufhebung

Für die Tat des § 225a StGB kann der Strafaufhebungsgrund der tätigen Reue zur Anwendung kommen. Dieser persönliche Strafaufhebungsgrund setzt voraus, dass die falschen oder verfälschten Daten noch nicht im Rechtsverkehr gebraucht wurden. Weiters muss der Täter die Gefahr beseitigen, dass die betreffenden Daten gebraucht werden können. Dies kann unter anderem durch Löschung der falschen oder Richtigstellung der verfälschten Daten geschehen. Diese Handlung bedarf jedoch der Freiwilligkeit.[165]

5.1.4. Zwischenergebnis

Der Straftatbestand des § 225a StGB umfasst folglich die Handlung der Fälschung oder Verfälschung von Daten. Im Jahr 2023 wurden über 700 Fälle der Datenfälschung angezeigt, wobei ein Viertel der Fälle aufgeklärt werden konnte.[166]

---

158 *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.243.
159 *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.244.
160 *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.245.
161 *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 19.
162 *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 19.
163 *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB § 225a Rz 20, 21.
164 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.223, 2.224.
165 Siehe zum betreffenden Absatz insgesamt *Kienapfel/Schroll* in *Höpfel/Ratz*, WK² StGB § 226 Rz 5-7 (Stand 1.1.2017, rdb.at).
166 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 25.

Das Delikt der Datenfälschung kommt beim Identitätsmissbrauch-Phänomen Spoofing zur Anwendung. Es bestehen verschiedene Formen von Spoofing, wie Webseite-Spoofing, Rufnummern-Spoofing oder E-Mail-Spoofing. All diese Erscheinungsformen haben gemein, dass der Täter einen Informationsgehalt (Webseiteninhalt, Nachrichteninhalt) mit der Intention herstellt, andere Personen über die Identität des Herstellers der Information zu täuschen.[167] Als weitere Erscheinungsform der Datenfälschung ist das Verfälschen von digitalen Ausweisen – zB durch den Austausch des Namens am Ausweis – denkbar.[168]

Bei der Datenfälschung handelt es sich meist um eine Vortat.[169] Werden die gefälschten oder verfälschten Daten im Nachgang gebraucht, so kann die Handlung unter das Delikt des (qualifizierten) Betrugs subsumiert werden.[170]

5.2. Betrug gemäß § 146 StGB und § 147 Abs 1 Z 1 StGB

§ 146 StGB regelt den Straftatbestand des Vermögensdelikts Betrug.[171]
Gemäß § 146 StGB wird das Delikt des Betrugs verwirklicht, wenn der Täter *„mit dem Vorsatz, durch das Verhalten des Getäuschten sich oder einen Dritten unrechtmäßig zu bereichern, jemanden durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die diesen oder einen anderen am Vermögen schädigt*".

5.2.1. Objektiver Tatbestand

a) Tathandlung

Die erste Voraussetzung des objektiven Tatbestands ist, dass die Täterschaft das Opfer über Tatsachen zu täuschen hat. Unter den Begriff Tatsache können alle „*objektiv feststellbaren Umstände der Vergangenheit und der Gegenwart*" verstanden werden.[172] Die Täuschung kann durch aktives Tun oder durch bloßes Unterlassen bzw auch ausdrücklich oder konkludent erfolgen.[173] Die Tathandlung kann daher beispielsweise im Ab-

[167] Siehe zum Webseite-Spoofing ua *Thiele* in *Hinterhofer*, Salzburger Kommentar zum StGB § 225a Rz 30 (44. Lfg, Stand 3.2023, lexisnexis.at).
[168] *Bergauer*, Computerstrafrecht (2016) 400; *Bergauer*, Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht[2] (2022) Rz 11.235.
[169] *Thiele* in *Hinterhofer*, Salzburger Kommentar zum StGB § 225a Rz 30, 54 (44. Lfg, Stand 3.2023, lexisnexis.at).
[170] *Reindl-Krauskopf* in *Höpfel/Ratz*, WK[2] StGB § 225a Rz 28; *Salimi* in *Höpfel/Ratz*, WK[2] DSG § 63 Rz 2 (Stand 30.8.2019, rdb.at).
[171] *Hinterhofer,* Spezialfragen des Betrugs in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht: Profiwissen für die Praxis[2] (2022) Rz 3.2.
[172] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK[2] StGB § 146 Rz 31 (Stand 30.11.2023, rdb.at).
[173] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK[2] StGB § 146 Rz 19.

schluss eines Mobilfunkvertrags mittels fremder Daten bestehen, da der Täter dadurch falsche Angaben über die Wirklichkeit macht. [174]

b) Irrtum

Die Folge der Tathandlung hat der Irrtum des Getäuschten zu sein. In diesem Zusammenhang ist anzumerken, dass ausschließlich Menschen getäuscht werden können. [175]

c) Vermögensverfügung

Als weitere Voraussetzung für die Verwirklichung des Betrugs muss der Getäuschte aufgrund des Irrtumes eine Vermögensverfügung durchführen.[176] Klassisches Beispiel ist das Ausfolgen von Geld.[177]

d) Vermögensschaden

Schlussendlich muss ein Vermögensschaden eintreten, wobei es irrelevant ist, ob der Getäuschte oder eine davon abweichende Person in ihrem Vermögen geschädigt wird.[178] Maßgeblich ist lediglich, dass das Vermögen einer Person im Vergleich zum Stand vor der Verfügung vermindert ist.[179]

5.2.2. Subjektiver Tatbestand

Betrug ist ein Vorsatzdelikt. Das bedeutet, dass das Tatsubjekt die Verwirklichung des objektiven Tatbestands ernstlich für möglich halten und sich damit abfinden muss. Zusätzlich hat die Täterschaft den erweiterten Vorsatz auf die unrechtmäßige Bereicherung zu erfüllen.[180]

5.2.3. Qualifikation nach § 147 Abs 1 Z 1 StGB

Im Zusammenhang mit Identitätsmissbrauch ist auch die Qualifikation nach § 147 Abs 1 Z 1 StGB maßgeblich. Nach dieser Bestimmung wird ein schwerer Betrug unter anderem dann verwirklicht, sofern zur Täuschung über Tatsachen falsche oder verfälschte Daten benützt werden.[181] Hinsichtlich der Voraussetzungen für das Vorliegen von falschen bzw

---

[174] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK² StGB § 146 Rz 21; *Reindl-Krauskopf/ Salimi/ Stricker*, IT-Strafrecht (2018) Rz 2.253.
[175] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK² StGB § 146 Rz 43, 47.
[176] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK² StGB § 146 Rz 52.
[177] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK² StGB § 146 Rz 53.
[178] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.257.
[179] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK² StGB § 146 Rz 66.
[180] Siehe zum betreffenden Absatz insgesamt *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.258, 2.259.
[181] Datenbetrug nach § 147 Abs 1 Z 1 vierter Fall StGB.

verfälschten Daten kann auf die Ausführungen zur Datenfälschung gemäß § 225a StGB verwiesen werden.
Die betreffenden Daten müssen herangezogen werden, um einen Dritten zu täuschen.[182] Die Qualifikation des Datenbetrugs wird beispielsweise dann erfüllt, wenn eine verfälschte E-Mail-Adresse zur Verübung von CEO-Fraud herangezogen wird, wobei in dem Zusammenhang eine Vermögensverfügung und Vermögensschädigung zu erfolgen hat.[183]

5.2.4. Konkurrenz zu § 225a StGB

Die Datenfälschung wird durch die Verwirklichung des schweren Betrugs grundsätzlich verdrängt, sofern die Datenfälschung zur Verübung des Betrugs begangen wird.[184]

Dient die Datenfälschung aber nicht nur dem Betrug, kann echte Konkurrenz zwischen § 225a StGB und § 147 Abs 1 Z 1 StGB bestehen. Dies ist dann der Fall, sofern mit der Datenfälschung „*auch darüber hinausgehende Zwecke verfolgt werden und die Taten sich auch nicht nur in der Vorbereitung anderer Delikte erschöpfen, sondern einen eigenständigen Unrechtsgehalt aufweisen*“.[185]

5.2.5. Zwischenergebnis

Wie in der Cybercrime Statistik des Bundesministeriums für Inneres/Bundeskriminalamts ersichtlich ist, ist ein stetiger Anstieg von Internetbetrug zu verzeichnen.[186] Allein im Jahr 2023 wurden über 32.000 Fälle betreffend § 146 StGB und § 147 StGB angezeigt, wobei 29% der Straftaten schlussendlich geklärt werden konnten – von der Zahl sind jedoch verschiedenste Betrugsmaschen und daher nicht nur Taten im Zusammenhang mit Identitätsmissbrauch umfasst.[187] Angesichts dessen sind die betreffenden Normen § 146 StGB sowie § 147 StGB in der Praxis von nicht außer Acht zulassender Relevanz.

Hinsichtlich der unter Punkt 4.2 genannten Identitätsmissbrauch-Phänomene wird §§ 146 iVm § 147 Abs 1 Z 1 StGB beim Polizisten-Trick, CEO-Fraud sowie Tochter-Sohn-Trick zur Anwendung kommen. Bei diesen Erscheinungsformen legt die Täterschaft einen unwahren Sachver-

---

[182] *Bergauer*, Computerstrafrecht, in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht[2] (2022) Rz 11.152, 11.153.
[183] Siehe ein ähnliches Beispiel in *Bergauer*, Computerstrafrecht, in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht[2] (2022) Rz 11.152.
[184] *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK[2] StGB § 147 Rz 28/32 (Stand 30.11.2023, rdb.at).
[185] RIS-Justiz RS0133582.
[186] *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 30.
[187] *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 30.

halt dar (zB, dass sich ein Verwandter in einer Notsituation befindet oder der Vorgesetzte eine dringende Geldüberweisung in Auftrag gibt), wobei sie dazu falsche Daten (gefälschte Rufnummern oder E-Mail-Adressen) benützt und dadurch über den Aussteller der Nachricht täuscht. Durch diesen Umstand wird das Opfer dazu verleitet, eine Geldüberweisung zu tätigen, wodurch eine Vermögensschädigung eintritt.
Hingegen wird die Phishing-/Smishing-Phase oder das Phänomen SIM-Swapping allein grundsätzlich nicht unter das Delikt des Betrugs zu subsumieren sein.[188] Beim Herauslocken von Daten, welches für das Phishing und SIM-Swapping typisch ist, scheitert es nämlich häufig an der Vermögensverfügung durch das Opfer selbst und der damit verbundenen Vermögensschädigung.[189]

5.3. Üble Nachrede gemäß § 111 StGB

Als weiterer Straftatbestand im Zusammenhang mit Identitätsmissbrauch kommt die üble Nachrede in Frage – nämlich, wenn der Täter mittels einer fremden Identität ehrrührige Inhalte über Dritte verbreitet.
Gemäß § 111 Abs 1 StGB erfüllt jemand das Delikt der üblen Nachrede, der „*einen anderen in einer für einen Dritten wahrnehmbaren Weise einer verächtlichen Eigenschaft oder Gesinnung zeiht oder eines unehrenhaften Verhaltens oder eines gegen die guten Sitten verstoßenden Verhaltens beschuldigt, das geeignet ist, ihn in der öffentlichen Meinung verächtlich zu machen oder herabzusetzen*“.

Im Folgenden werden die Tatbestandselemente näher dargestellt.

5.3.1. Objektiver Tatbestand

a) Zeihen einer verächtlichen Eigenschaft oder Gesinnung
   Unter einer verächtlichen Eigenschaft oder Gesinnung sind verachtenswerte Einstellungen bzw beträchtliche Charaktermängel des Opfers zu verstehen.[190] Diese haben zu einer allgemeineren Ablehnung bzw Verachtung zu führen.[191]

[188] Zur strafrechtlichen Beurteilung der Phishing Phase siehe *Bergauer,* Computerstrafrecht (2016) 409.
[189] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.272; *Bergauer,* Computerstrafrecht (2016) 409.
[190] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.500.
[191] *Rami* in *Höpfel/Ratz*, WK² StGB § 111 Rz 10 (Stand 1.9.2024, rdb.at).

b) Beschuldigen eines unehrenhaften oder sittenwidrigen Verhaltens

Das StGB enthält keine Begriffsbestimmung der Ehre.[192] Unter dem Begriff der Ehre wird nach herrschender Ansicht das „*Ansehen und die Achtung, die ein Mensch in den Augen seiner Umwelt genießt*" verstanden.[193] Dementsprechend sind jene Behauptungen, die aus gesamtgesellschaftlicher Sichtweise gegen allgemeine Wertvorstellungen laufen, wodurch eine konkrete Person in ihrem Ansehen bzw ihrer Achtung verletzt wird, als unehrenhaftes bzw sittenwidriges Verhalten zu qualifizieren.[194] Beispielweise wäre der Vorwurf einer gerichtlich strafbaren Handlung als ein solches unehrenhaftes bzw sittenwidriges Verhalten einzustufen.[195] Auch die Äußerung eines Verdachts, dass Strafverfolgungsbehörden gegen jemanden ermitteln würden oder die Untersuchungshaft gegen eine Person verhängt werden würde, könnte unter den Tatbestand subsumiert werden.[196]

c) Publizitätserfordernis

Für eine dritte Person muss erkennbar sein, wer das Opfer der betreffenden Äußerung (somit des Zeihens einer verächtlichen Eigenschaft oder Gesinnung bzw der Beschuldigung eines unehrenhaften oder sittenwidrigen Verhaltens) ist.[197]

Weitere Bedingung für die Erfüllung des objektiven Tatbestands ist das Vorliegen eines dreipersonalen Verhältnisses.[198] Konkret bedeutet dies, dass die Aussage in einer Weise zu erfolgen hat, dass sie für einen Dritten – dh eine Person, die weder der Äußerer noch das Opfer ist – wahrnehmbar ist.[199]

5.3.2. Subjektiver Tatbestand

Für die Strafbarkeit der üblen Nachrede ist der Vorsatz in Bezug auf die zuvor genannten objektiven Tatbestandselemente des Täters erforderlich.[200]

---

192 *Rami* in *Höpfel/Ratz*, WK² StGB Vor §§ 111 - 117 Rz 6 (Stand 1.9.2024, rdb.at).
193 *Rami* in *Höpfel/Ratz*, WK² StGB Vor §§ 111 - 117 Rz 6.
194 *Reindl-Krauskopf/ Salimi/ Stricker*, IT-Strafrecht (2018) Rz 2.503.
195 *Rami* in *Höpfel/Ratz*, WK² StGB § 111 Rz 11.
196 *Rami* in *Höpfel/Ratz*, WK² StGB § 111 Rz 12/1.
197 *Rami* in *Höpfel/Ratz*, WK² StGB Vor §§ 111 - 117 Rz 10, 10/1.
198 *Rami* in *Höpfel/Ratz*, WK² StGB § 111 Rz 7.
199 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.511, 2.513; *Rami* in *Höpfel/Ratz*, WK² StGB § 111 Rz 7.
200 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.511, 2.514.

5.3.3. Qualifikation nach § 111 Abs 2 StGB

„Wer die Tat in einem Druckwerk, im Rundfunk oder sonst auf eine Weise begeht, wodurch die üble Nachrede einer breiten Öffentlichkeit zugänglich wird, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.“ [201]

Die Tat muss dabei in einem Druckwerk (somit in einem körperlichen Medium, wie Zeitungen), im Rundfunk (dh Fernsehen bzw Radio), oder auf sonstige Weise (unter anderem im Internet) verübt werden.[202] Die letzte Alternative des § 111 Abs 2 StGB wird erfüllt, wenn die üble Nachrede einer breiten Öffentlichkeit, worunter um die 150 Personen fallen, zugänglich wird.[203]

5.3.4. Zwischenergebnis

Hinsichtlich der Erfüllung des gegenständlichen Straftatbestands im Zusammenhang mit Identitätsmissbrauch sind zwei Fälle zu unterscheiden.

So ist unter anderem die Fallkonstellation denkbar, dass sich die Täterschaft fälschlicherweise als Opfer ausgibt und dabei das Opfer eines unehrenhaften Verhaltens beschuldigt. Da für einen Dritten nicht ersichtlich ist, dass eine vom Opfer verschiedene Person die betreffende Äußerung tätigt, wird das Vorliegen des Publizitätserfordernisses als problematisch erachtet werden. Somit würde in diesem Fall der betreffende Straftatbestand der üblen Nachrede nicht verwirklicht werden.[204]

Ferner kann beim Identitätsmissbrauch der Umstand eintreten, dass der Täter die Identität einer anderen Person als das Opfer benutzt und im Rahmen dessen jemanden einer gerichtlich strafbaren Handlung bezichtigt, womit eine üble Nachrede getätigt wird. Zu denken ist dabei an den Polizisten-Trick, im Rahmen dessen ein vermeintlicher Polizist bei einem Dritten anruft und wahrheitswidrig mitteilt, dessen Kind hätte einen tödlichen Unfall verursacht, weshalb der Dritte eine Kaution hinterlegen müsse.[205] In diesem Fall wäre das Erfordernis des dreipersonalen Verhältnisses erfüllt. Dennoch wird in dem betreffenden Beispiel eher das Delikt des Betrugs in Frage kommen, da sich der Täter vorsätzlich dadurch unrechtmäßig bereichern möchte, dass er

---

[201] § 111 Abs 2 StGB.
[202] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.516 - 2.518.
[203] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.518.
[204] Siehe zum Absatz insgesamt *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.511, 2.513.
[205] Siehe zum Kautionsbetrug etwa *Bundesministerium für* Inneres, Anrufkriminalität https://bmi.gv.at/magazin/2022_03_04/Anrufkriminalitaet.aspx (abgefragt am 3.4.2025).

einen Dritten durch die Täuschung über die vorgespielte Festnahme zur Herausgabe von Geld verleitet und diesen so an seinem Vermögen schädigt.[206]

5.4. Besonderer Erschwerungsgrund gemäß § 33 Abs 1 Z 8 StGB

5.4.1. Allgemeines

Bei der Bemessung der Strafe und somit bei der Schuld des Täters hat das Gericht unter anderem Erschwerungs- und Milderungsgründe abzuwägen.[207]

Der im allgemeinen Teil des StGB verankerte § 33 StGB sieht besondere Erschwerungsgründe vor. Nach § 33 Abs 1 Z 8 StGB ist die Begehung einer Tat straferschwerend, wenn „*der Täter die Tat unter Missbrauch der personenbezogenen Daten einer anderen Person begangen hat, um das Vertrauen eines Dritten zu gewinnen, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wird*".
Das StGB enthält keine Legaldefinition des Begriffs „personenbezogene Daten".[208] Vielmehr ist in diesem Zusammenhang auf das Datenschutzrecht zurückzugreifen.[209] Gemäß Art 4 Z 1 DSGVO fallen unter den Begriff „*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen*".
Damit der Erschwerungsgrund zur Anwendung kommen kann, müssen die personenbezogenen Daten bzw Identitätsdaten einer anderen Person missbräuchlich, dh ohne Zustimmung der zum Gebrauch der Daten tatsächlich berechtigten Person, verwendet werden.[210] Das Handeln unter einer erfundenen Identität reicht dagegen nicht aus, um den Erschwerungsgrund zu erfüllen.[211]

Weiters bedarf es einen Dritten, der die Identität der handelnden Person für wahr hält, sowie einer Schädigung des rechtmäßigen Identitätseigentümers.[212]

---

206 Siehe dazu näher die Ausführungen unter Punkt 5.2 gegenständlicher Master Thesis.
207 § 32 Abs 1 und Abs 2 StGB.
208 *Birklbauer/Stiebellehner* in *Hinterhofer*, StGB: Salzburger Kommentar zum StGB § 33 StGB Rz 104 (45. Lfg, Stand Juli 2023, lexisnexis.at).
209 *Birklbauer/Stiebellehner* in *Hinterhofer*, StGB: Salzburger Kommentar zum StGB § 33 StGB Rz 104 (45. Lfg).
210 *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 31.
211 *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 31.
212 *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 33.

5.4.2. Zwischenergebnis

§ 33 Abs 1 Z 8 StGB gilt für alle strafbaren Handlungen[213], wobei das Doppelverwertungsverbot zu beachten ist, wonach Erschwerungs- und Milderungsgründe, die schon die Strafdrohung bestimmen, bei der Strafbemessung nicht einbezogen werden dürfen.[214] Beispielsweise werden bei betrügerischen Nachrichten im Zusammenhang mit Spoofing von tatsächlich vergebenen Rufnummern oder E-Mail-Adressen, bei dem über die Identität des Ausstellers einer Nachricht getäuscht wird, sowohl falsche Daten gemäß § 147 Abs 1 Z 1 StGB erzeugt, als auch personenbezogene Daten gemäß § 33 Abs 1 Z 8 StGB missbraucht.[215] Bei den oben unter Punkt 4.2 beschriebenen Polizisten-Trick und Tochter-Sohn-Trick wird aber § 33 Abs 1 Z 8 StGB nicht einschlägig sein, weil der Täter bei diesen Phänomenen dem Polizisten bzw der Tochter/dem Sohn als Identitätseigentümer nicht „*einen über den Missbrauch der Daten bestehenden Nachteil hinausreichenden Schaden verursacht*“.[216] Vielmehr wird bei diesen Phänomenen das Delikt des §§ 146 iVm § 147 Abs 1 Z 1 StGB erfüllt.[217] In Betracht für § 33 Abs 1 Z 8 StGB kommt aber der CEO-Fraud, da bei diesem Phänomen, wenn die Nachricht zB vom vermeintlichen Einzelunternehmer als Führungskraft stammt, dem Einzelunternehmer als Identitätseigentümer ein finanzieller Schaden zugefügt wird.[218] Unter Beachtung des Doppelverwertungsverbots wird aber dennoch auch beim CEO-Fraud ausschließlich §§ 146 iVm § 147 Abs 1 Z 1 StGB einschlägig sein.

5.5. Datenverarbeitung in Gewinn- oder Schädigungsabsicht gemäß § 63 DSG

Eine weitere für den Identitätsmissbrauch in Frage kommende, allerdings nicht im Strafgesetzbuch festgelegte Norm, findet sich im Datenschutzgesetz.

So ist gemäß § 63 DSG derjenige, der „*mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse ha*t“ zu bestrafen (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bis

---

[213] ErläutRV 689 BlgNR 25. GP 8; *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 27.
[214] § 32 Abs 2 erster Satz StGB; *Riffel* in *Höpfel/Ratz*, WK StGB § 32 Rz 59 (Stand 15.8.2023, rdb.at).
[215] Siehe zum Doppelverwertungsverbot beim Datenbetrug *Bergauer,* Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht² (2022) Rz 11.160.
[216] *Birklbauer/Stiebellehner* in *Hinterhofer*, StGB: Salzburger Kommentar zum StGB § 33 StGB Rz 106 (45. Lfg).
[217] Siehe dazu Punkt 5.2.5 der gegenständlichen Master Thesis.
[218] Als vergleichbares Beispiel kann der Kreditkartenbetrug angeführt werden - siehe *Birklbauer/Stiebellehner* in *Hinterhofer*, StGB: Salzburger Kommentar zum StGB § 33 StGB Rz 106 (45. Lfg).

zu 720 Tagessätze). Der Straftatbestand kommt nur dann zur Anwendung, sofern die Tat nicht nach einer anderen Regelung mit strengerer Strafe bedroht ist.[219]

5.5.1. Objektiver Tatbestand

a) Tatobjekt

Tatobjekt von § 63 DSG sind jene Daten, an denen der Betroffene ein schutzwürdiges Geheimhaltungsinteresse hat.[220] Dabei muss es sich um personenbezogene Daten, sohin nach Art 4 Z 1 DSGVO um Informationen handeln, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei es irrelevant ist, ob die betreffenden Daten automationsunterstützt oder auf sonstige Weise verarbeitet werden.[221] Dementsprechend fallen unter den Begriff „Daten" eine Vielzahl an Informationen, die eine bestimmte Person betreffen, wie die Telefonnummer und Ausweis- oder Bilddaten, die Kommunikationsdiensteanbieter im Rahmen der Identifizierung bzw Registrierung ihrer Kunden verarbeiten.[222]

Neben dem Vorliegen von personenbezogenen Daten muss an Letztgenannten ein schutzwürdiges Geheimhaltungsinteresse seitens des Identitätseigentümers vorliegen.[223] Ein solches Geheimhaltungsinteresse liegt bei allgemein verfügbaren Daten – worunter beispielsweise im Telefonbuch veröffentlichte Daten fallen – sowie Daten, die auf keine Person rückführbar sind und somit anonymisierte Daten darstellen, nicht vor.[224]

b) Tatsubjekt

Als Tatsubjekt kommen nur solche Personen in Betracht, (i) denen Daten ausschließlich im Zuge ihrer berufsmäßigen Beschäftigung anvertraut bzw zugänglich werden oder (ii) die sich Daten durch aktives Handeln[225] widerrechtlich verschaffen.

Einerseits ist vom Delikt somit jener Personenkreis erfasst, der zur Bestreitung des Lebensunterhalts Tätigkeiten ausübt, unabhängig vom Beruf und unabhängig davon, ob einer Tätigkeit im privaten oder öffentlichen Bereich nachgegangen wird.[226]

---

219 § 63 DSG.
220 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 19.
221 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 19, 20.
222 Siehe eine beispielhafte Liste an personenbezogenen Daten unter anderem in *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.511, 2.579.
223 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 30.
224 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 31, 33, 35.
225 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 50.
226 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 44; *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.585.

Andererseits, und demnach über den zuvor beschriebenen Täterkreis hinaus, sind vom Straftatbestand des § 63 DSG auch alle Personen umfasst, die sich Daten widerrechtlich verschafft haben. Dementsprechend handelt es sich bei § 63 DSG auch um ein Allgemeindelikt.[227] Diese Tätergruppe wird mE hinsichtlich der Begehung von Identitätsmissbrauch mehr von Bedeutung sein. Voraussetzung ist ein aktives Tun des Täters, passives Erlangen genügt zur Erfüllung des Tatbestands nicht.[228] Unter den Begriff des „widerrechtlichen Verschaffens" können alle Handlungen fallen, die in einem Verstoß der Rechtsordnung (zB einer strafrechtlichen Norm) resultieren.[229] Beispielsweise wird das Herauslocken von Identitätsdaten durch Phishing oder SIM-Swapping ein solches widerrechtliches Verschaffen von Daten darstellen.[230]

c) Tathandlung

Als Tathandlung kommt ausschließlich das Selbst-Benützen, das Zugänglichmachen oder die Veröffentlichung von Daten in Frage.[231] Diese Handlungen haben es gemein, dass durch sie das schutzwürdige Geheimhaltungsinteresse der betroffenen Person an ihren Daten verletzt wird.[232]

Unter den Terminus Selbst-Benützen von Daten fällt jeder Einsatz von Daten bzw jede Handlung im Zusammenhang mit personenbezogenen Daten.[233] Obwohl das Gesetz eine Außenwirkung der Handlung nicht voraussetzt, ist eine solche nach Teilen des Schrifttums erforderlich, da ansonsten keine Geheimhaltungsinteressen der betroffenen Person verletzt werden.[234] Vom Benützen sind grundsätzlich alle Formen des Identitätsmissbrauchs erfasst.[235] Beispielsweise wird das Heranziehen von im Rahmen einer Phishing-Attacke widerrechtlich erlangten fremden Identitätsdaten zur unberechtigten Erlangung von Geld erfasst sein.[236]

Das Zugänglichmachen von Daten betrifft Handlungen, durch die bestimmte, zahlenmäßig beschränkte dritte Personen Kenntnis von für sie bislang nicht bekannten Daten erhalten

---

227 *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG)² § 63 Rz 6 (Stand 1.2.2022, rdb.at).
228 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.588.
229 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.589.
230 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.590.
231 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.593.
232 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.593.
233 Siehe dazu *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 61.
234 Siehe dazu *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 62.
235 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 65.
236 weitere Beispiele zum Selbst-Benützen siehe *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 65.

können.[237] Dadurch werden die schutzwürdigen Geheimhaltungsinteressen der betroffenen Person an ihren Daten verletzt.[238]

Dagegen stellt die Veröffentlichung von Daten das Zugänglichmachen von Daten an einen unbestimmten Adressatenkreis, zB im Internet, dar.[239]

5.5.2. Subjektiver Tatbestand

Hinsichtlich der inneren Tatseite verlangt die betreffende Norm zwei verschiedene Formen von Vorsatz. So muss zum einen der Eventualvorsatz der Täterschaft auf die objektiven Tatbestandselemente vorliegen. Demnach muss es der Täter ernstlich für möglich halten und sich damit abfinden, die Tathandlungen in Bezug auf das Tatobjekt zu verwirklichen. Zum anderen hat die Täterschaft mit erweitertem Vorsatz auf die unrechtmäßige Bereicherung zu handeln oder mit erweitertem Vorsatz zu handeln, absichtlich den Betroffenen in seinem Anspruch auf Geheimhaltung seiner personenbezogenen Daten zu schädigen.[240]

5.5.3. Rechtfertigungsgründe

Das Delikt des § 63 DSG wird dann nicht verwirklicht, wenn die Datenverarbeitung rechtmäßig – somit unter anderem gemäß den Regelungen des Art 6 DSGVO oder Art 9 DSGVO – erfolgt.[241] Dies ist etwa der Fall, wenn die Einwilligung in die betreffende Datenverarbeitung erfolgt ist oder die Datenverarbeitung zur Erfüllung des Vertrags, einer rechtlichen Verpflichtung oder zum Schutz lebenswichtiger Interessen erforderlich ist. Die aufgelisteten Bestimmungen stellen jeweils Rechtfertigungsgründe dar.[242]

5.5.4. Zwischenergebnis/Konkurrenz

Grundsätzlich kommen dem SIM-Swapping nachgelagerte Handlungen, wie zB das Heranziehen der im Rahmen des SIM-Swappings erlangten Rufnummer zur Durchführung von missbräuchlichen Banküberweisungen, für die Verwirklichung des § 63 DSG aus den folgenden

---

[237] *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 67, 68; *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG)² § 63 Rz 19, 20.
[238] *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 67, 68; *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG)² § 63 Rz 19, 20.
[239] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG)² § 63 Rz 22.
[240] Siehe zum betreffenden Absatz insgesamt *Tipold* in *Leukauf/Steininger*, Strafrechtliche Nebengesetze³ § 63 DSG Rz 17-20 (Stand 1.9.2022, rdb.at).
[241] *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 80, 81.
[242] *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 81.

Gründen in Frage: Zunächst hat sich die Täterschaft durch das SIM-Swapping Zugang zu der SIM-Karte und somit der Telefonnummer eines Dritten widerrechtlich verschafft. Daraufhin zieht die Täterschaft die widerrechtlich erlangte Rufnummer mit dem Vorsatz heran, sich unrechtmäßig zu bereichern.
Das Delikt der Datenverarbeitung in Gewinn- oder Schädigungsabsicht kommt nur dann zur Anwendung, wenn die Tat nicht nach einer anderen Norm mit einer strengeren Strafe bedroht ist.[243] Diese Subsidiaritätsklausel betrifft die konkrete Datenverwendung.[244] Werden beispielsweise verfälschte Identitätsdaten im Rahmen eines Betrugs verwendet, wodurch ein schwerer Betrug begangen wird, tritt die Strafbarkeit nach § 63 DSG zurück.[245] In diesem Zusammenhang ist anzumerken, dass das Delikt des schweren Betrugs nur dann verwirklicht werden kann, wenn im Rahmen der Tathandlung ein Menschen getäuscht wird.[246]

5.6. Ergebnis

Die Strafverfolgung hängt besonders vom Anzeigeverhalten der Bevölkerung ab. Im Jahr 2023 wurden insgesamt rund 33.000 Fälle von Datenfälschung, Betrug und schwerem Betrug (wobei es sich dabei um Internetbetrug handelt) angezeigt.[247] Rund 29 % davon konnten schlussendlich aufgeklärt werden.[248] Bei den betreffenden Zahlen handelte es sich um verschiedenste Tatbegehungen. Eine gesonderte Statistik für im Zusammenhang mit Identitätsmissbrauch verübte Taten liegt nicht vor. Es ist auch zu bedenken, dass nicht alle vom Identitätsmissbrauch Betroffenen eine Anzeige vornehmen – die Dunkelziffer der betreffenden Delikte ist demnach wohl nicht unbeachtlich.[249]

Bei der Bestrafung der Taten ist der Grundsatz „nulla poena sind lege“ zu beachten. Danach darf betreffend eine verübte Tat nur jene Strafe verhängt werden, die das Gesetz vorsieht.[250] Die Tat muss somit zum Zeitpunkt ihrer Begehung unter einen Straftatbestand subsumiert werden können.[251] In diesem Zusammenhang ist auf das Verbot des Gewohnheitsrechts und auf das Analogieverbot hinzuweisen.[252] Somit dürfen weder durch das Gewohnheitsrecht noch

---

243 § 63 DSG.
244 *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 103.
245 Siehe dazu *Salimi* in *Höpfel/Ratz*, WK² DSG § 63 Rz 103.
246 *Kirchbacher/Sadoghi* in *Höpfel/Ratz*, WK² StGB § 146 Rz 43, 47.
247 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023; 25, 30.
248 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023; 25, 30.
249 *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023; 31; *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 1.10.
250 *Stricker* in *Leukauf/Steininger,* StGB: Strafgesetzbuch inklusive Update 2020 § 1 Rz 2 (2020, lindedigital.at).
251 *Stricker* in *Leukauf/Steininger*, StGB: Strafgesetzbuch inklusive Update 2020 Rz 3.
252 *Stricker* in *Leukauf/Steininger*, StGB: Strafgesetzbuch inklusive Update 2020 Rz 5, 7.

durch Analogie neue Straftatbestände eingeführt werden oder bereits bestehende Straftatbestände verschärft werden.[253]
Die Auslegung eines Straftatbestands ist stets durch den äußerst möglichen Wortsinn beschränkt.[254] Ausschließlich bei Vorliegen einer unbeabsichtigten planwidrigen Lücke ist eine Analogie zugunsten der Täterschaft (zB von Rechtfertigungsgründen) zulässig.[255]

Zusammenfassend können bei Identitätsmissbrauch, jeweils abhängig von der konkreten Straftat, die Delikte (i) Datenfälschung gemäß § 225a StGB, (ii) Betrug gemäß § 146 StGB bzw schwerer Betrug gemäß § 147 Abs 1 Z 1 StGB, (iii) üble Nachrede gemäß § 111 StGB sowie (iv) Datenverarbeitung in Gewinn- oder Schädigungsabsicht gemäß § 63 DSG erfüllt werden. Im Zusammenhang mit der Verwirklichung der Straftatbestände ist der besondere Erschwerungsgrund gemäß § 33 Abs 1 Z 8 StGB zu beachten.

Die Erscheinungsformen von Identitätsmissbrauch entwickeln sich trotz der grundsätzlichen generalpräventiven Wirkung von bereits existierenden Straftatbeständen[256] stets weiter.
Aufgrund des Analogieverbots ist der Gesetzgeber angehalten, möglichst alle in Betracht kommenden künftigen Phänomene von Straftatbeständen abzudecken bzw bei neu aufkommenden Kriminalitätsformen durch Einführung neuer Straftatbestände rasch zu reagieren, sodass die Täterschaft zur Verantwortung gezogen werden kann.[257] Um auch für künftige Fälle effektiven strafrechtlichen Schutz zu bieten, könnte der Gesetzgeber mE laufend evaluieren, ob doch die Einführung eines eigenen Straftatbestands für Identitätsmissbrauch in Erwägung zu ziehen ist.

6. Meldestellen und Auskunftspflichten von Anbietern von Kommunikationsdiensten

In diesem Abschnitt wird erörtert, über welche Möglichkeiten von Cybercrime betroffene Personen verfügen, Straftaten zu melden. Darüber hinaus werden die an das Bekanntwerden des Verdachts einer Straftat anschließenden Ermittlungsbefugnisse von Behörden im Zusammenhang mit Cybercrime Delikten dargestellt.

253 *Stricker* in *Leukauf/Steininger*, StGB: Strafgesetzbuch inklusive Update 2020 Rz 5, 7.
254 *Stricker* in *Leukauf/Steininger*, StGB: Strafgesetzbuch inklusive Update 2020 Rz 10.
255 *Stricker* in *Leukauf/Steininger*, StGB: Strafgesetzbuch inklusive Update 2020 Rz 8.
256 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 1.12.
257 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 1.6.

6.1. Meldestellen

Einleitend ist anzumerken, dass zahlreiche Optionen zur Meldung von Hinweisen zu (vermeintlichen) Straftaten offenstehen. Diese reichen von der Erstattung einer Anzeige an die Kriminalpolizei oder Staatsanwaltschaft gemäß § 80 Abs 1 StPO bis zu schlichten Meldungen an für Cybercrime zuständige Stellen. Hinsichtlich der Möglichkeit, Anzeige zu erstatten ist anzumerken, dass es sich hierbei um ein Recht von Opfern einer Straftat handelt.[258] Dessen Gebrauch liegt im Ermessen des jeweiligen Opfers, es besteht keine Anzeigepflicht.[259]

Neben dem Anzeigerecht können sich betroffene Personen beispielsweise an die Cybercrime-Meldestelle des österreichischen Bundeskriminalamts wenden.[260] Weiters steht ihnen die Webseite „Watchlist Internet" des Österreichischen Instituts für angewandte Telekommunikation zur Verfügung, im Rahmen derer sie Hinweise zu Cybercrime Delikten melden können.[261]
Abschließend ist auf die speziell gegen Rufnummernmissbrauch (worunter die unlautere Nutzung von Rufnummern verstanden wird) eingerichtete Meldestelle der RTR-GmbH hinzuweisen.[262] Bei der Meldestelle können bspw Betrugs- bzw Datendiebstahlversuche oder sonstige Belästigungen gemeldet werden.[263] Die Bekanntgabe von Sachverhalten dieser Art kann sowohl von betroffenen Personen als auch von Anbietern von Kommunikationsdiensten, die über Hinweise von Nummernmissbrauch verfügen, erfolgen.[264]
In der Summe stehen den betroffenen Personen somit einige Optionen zur Verfügung, im Rahmen der Telekommunikation verübte Delikte anzuzeigen bzw zu melden.

6.2. Auskunftspflichten von Anbietern von Kommunikationsdiensten

Neben den Handlungsmöglichkeiten der Opfer sind die Ermittlungsbefugnisse der Behörden zum Ausfindigmachen der Täterschaft von besonderer Relevanz.
Komplexe Sachverhalte – insbesondere angesichts des Umstands, dass die Delikte mit hohem technischem Know-how verbunden sein können sowie möglicherweise ein Auslandsbezug der

---

258 *Schwaighofer* in *Fuchs/Ratz*, WK StPO § 80 Rz 2 (Stand 1.12.2020, rdb.at).
259 *Schwaighofer* in *Fuchs/Ratz*, WK StPO § 80 Rz 2.
260 Die Meldestelle des österreichischen Bundeskriminalamts ist unter https://bundeskriminalamt.at/mdst/cc.aspx abrufbar.
261 https://www.watchlist-internet.at/; über die Watchlist Internet kann sich die Öffentlichkeit einen Überblick über einige aktuelle Phänomene verschaffen.
262 ErläutRV 1043 BlgNR 27. GP 40; www.rufnummernmissbrauch.at
263 ErläutRV 1043 BlgNR 27. GP 40.
264 Das Meldeformular ist unter https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/meldeformular.de.html abrufbar; im folgenden Kapitel „Telekommunikationsrechtliche Aspekte" der gegenständlichen Master Thesis wird näher auf die Meldestelle gegen Nummernmissbrauch der RTR-GmbH eingegangen.

Tat besteht – können die Strafverfolgungsbehörden bei ihren Ermittlungen vor Herausforderungen stellen.

Im Folgenden wird dargestellt, über welche Ermittlungsbefugnisse die Behörden verfügen, Täter, die Straftaten im Rahmen der Telekommunikation begangen haben, ausfindig zu machen und welchen Verpflichtungen Anbieter von Kommunikationsdiensten dementsprechend unterliegen.
Die Anbieter haben das jeweilige behördliche Auskunftsersuchen einer rechtlichen Überprüfung zu unterziehen, da die unberechtigte bzw überschießende Weitergabe von Daten einen Verstoß gegen das Recht auf Geheimhaltung gemäß § 1 Abs 1 DSG des betreffenden Kunden darstellt und somit datenschutzrechtliche Folgen nach sich ziehen kann.

Da zu den – die Telekommunikation betreffenden – Befugnissen der Behörden einige gesetzliche Grundlagen bestehen, werden einzelne ausgewählte Normen näher beleuchtet.

6.2.1. Auskunft über Stammdaten gemäß § 181 Abs 9 TKG 2021 iVm § 135 Abs 1a erster Fall StPO

Gemäß § 181 Abs 9 TKG 2021 iVm § 135 Abs 1a erster Fall StPO sind Anbieter von Kommunikationsdiensten auf Ersuchen der Kriminalpolizei, Staatsanwaltschaften und Gerichte zur Auskunft über Stammdaten von Nutzern verpflichtet, sofern dies zur Aufklärung und Verfolgung eines konkreten Verdachts einer Straftat erforderlich erscheint. Unter den Begriff Stammdaten fallen die folgenden Daten: Name, akademischer Grad, Anschrift, Nutzernummer und sonstige Kontaktinformation für die Nachricht, Information über Art und Inhalt des Vertragsverhältnisses, Bonität und Geburtsdatum (entsprechend § 160 Abs 3 Z 5 TKG 2021).
Ein Ersuchen der Behörde um Auskunft über die genannten Daten an den Betreiber kann einen ersten geeigneten Schritt darstellen, um Hinweise zu dem vermeintlichen Täter zu erlangen.
Da bei einigen kriminellen Verhaltensweisen aber auch Spoofing eingesetzt wird[265], besteht die Möglichkeit, dass die Stammdatenabfrage – sofern eine existierende Rufnummer verwendet wurde – nicht zum tatsächlichen Täter, sondern vielmehr zu einer nicht mit der Straftat in Verbindung stehenden Person, führt. Somit ist die Stammdatenabfrage nicht in sämtlichen Fällen ein geeignetes Mittel zur Ausforschung der Täterschaft.

[265] Siehe dazu Punkt 4.1 der vorliegenden Master Thesis.

6.2.2. Sicherstellung bzw Beschlagnahme von Datenträgern und Daten

Das Ergebnis einer Stammdatenabfrage muss nicht zwangsläufig zu einer im Hoheitsgebiet Österreich ansässigen bzw in den Registern der österreichischen Behörden eingetragenen Person führen. Ebenso besteht die Möglichkeit der Namensgleichheit sowie desselben Geburtstages von Personen. Sofern die Identität einer Person durch die vom Betreiber vorgelegten Stammdaten nicht mit Sicherheit festgestellt werden kann, wird die zuständige Ermittlungsbehörde um Übermittlung weiterer beim Anbieter hinterlegter Daten, wie zB der vom Nutzer einer Rufnummer beim Vertragsabschluss vorgelegten Dokumente, ersuchen. Beispielsweise können beim Anbieter gespeicherte Ausweiskopien Rückschlüsse auf die hinter der Rufnummer stehenden Person liefern. Da nicht alle auf einer Ausweiskopie enthaltenen Daten unter den Begriff „Stammdaten" iSd § 160 Abs 3 Z 5 TKG 2021 (der eine taxative Liste an Daten anführt[266]) zu subsumieren sind, berechtigt § 181 Abs 9 TKG 2021 iVm § 135 Abs 1a erster Fall StPO Anbieter nicht zur Herausgabe der Ausweiskopie. Es besteht auch keine sonstige spezielle Rechtsgrundlage, die Anbieter zur Übermittlung verpflichtet. Daher ist dafür – gemäß der Rechtsprechung zur Bekanntgabe des PUK-Codes („*Personal Unlocking Key*", eine „*vom Anbieter vergebene Nummer, die dem Teilnehmer die Überwindung der Sperre des PIN- Codes ermöglicht*"[267] und die somit dem Entsperren einer SIM-Karte bzw eines Mobiltelefons dient) – als allgemeine Ermittlungsbefugnis wohl die Sicherstellung, also die Begründung der Verfügungsmacht über Gegenstände, gemäß §§ 109 ff StPO heranzuziehen.[268]

Bei den Regelungen der Sicherstellung ist zu beachten, dass der Anbieter nur zur Herausgabe von Daten verpflichtet wird.[269] Eine zusätzliche Leistung kann vom Anbieter dagegen nicht abverlangt werden.[270] So entschied beispielsweise das OLG Wien, dass die Herstellung eines Duplikats einer SIM-Karte nicht unter § 110 StPO zu subsumieren ist – vor allem, da es sich hierbei um eine zusätzliche Leistung des Anbieters handeln würde und somit überschießend wäre.[271] Folglich sind von der Sicherstellung als allgemeine Ermittlungsbefugnis nicht alle Handlungen abgedeckt, die keiner sonstigen speziellen Rechtsgrundlage unterliegen.

Die Normen der Sicherstellung wurden Anfang 2025 einer Reform unterzogen. Anlass dafür war eine Entscheidung des VfGH vom Dezember 2023 (VfGH 14.12.2023, G 352/2021). Gegen-

---

266 *Lendl* in *Fuchs/Ratz,* WK StPO § 76a Rz 2 (Stand 15.3.2023, rdb.at).
267 Die Begriffsdefinition ist in § 2 Z 7 Überwachungskostenverordnung BGBl II 2004/322 zu finden.
268 Zur Bekanntgabe des PUK-Codes auf Grundlage von § 110 StPO siehe *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 5.75; *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz,* WK StPO § 134 Rz 38 (Stand 1.3.2021, rdb.at); *Ghazanfari*, Bekanntgabe des PUK-Codes und Duplizierung einer SIM-Karte - Sicherstellung? JBl 2021, 740; OLG Wien, 11.7.2019, 23 Bs 172/19s.
269 *Ghazanfari*, JBl 2021, 740; OLG Wien, 11.7.2019, 23 Bs 172/19s.
270 *Ghazanfari*, JBl 2021, 740; OLG Wien, 11.7.2019, 23 Bs 172/19s.
271 *Ghazanfari*, JBl 2021, 740; OLG Wien, 11.7.2019, 23 Bs 172/19s.

stand dieses Erkenntnisses war die Sicherstellung von Mobiltelefonen, die lediglich einer Anordnung der Staatsanwaltschaft bedurfte und somit ohne eine richterliche Bewilligung zulässig war. Der VfGH entschied, dass diese Vorgehensweise gegen das Recht auf Datenschutz und das Recht auf Privatleben verstößt und somit verfassungswidrig ist. Dies ist unter anderem deshalb der Fall, da die Sicherstellung von Datenträgern und die Auswertung von Daten bereits bei einem Anfangsverdacht und auch schon beim Verdacht einer nur leichten Straftat erfolgen konnte. Darüber hinaus hatten die Strafverfolgungsbehörden die Möglichkeit, auf alle sich auf dem Gerät befindlichen Daten zuzugreifen und sich somit ein weitreichendes Bild über die von der Sicherstellung betroffenen Personen (die auch nicht verdächtigte Dritte sein können) zu verschaffen. So war beispielsweise sogar die Wiederherstellung von bereits gelöschten Daten möglich. Die betroffenen Personen hatten aber keine Kenntnis davon, welche Daten tatsächlich ausgewertet werden. Es war auch kein wirksamer Rechtsschutz gegeben, da dieser unter anderem eine richterliche Kontrolle erfordert. Aufgrund dessen wurden die Bestimmungen des § 110 Abs 1 Z 1 und Abs 4 StPO sowie § 111 Abs 2 StPO, die die Sicherstellung der auf Datenträgern gespeicherten Informationen aus Beweisgründen regeln, mit Ablauf des 31.12.2024 aufgehoben.[272]

Anfang Dezember 2024 hat sich der Nationalrat auf eine neue Regelung geeinigt. Demgemäß darf ab 2025 die Beschlagnahme von Datenträgern und Daten durch die Staatsanwaltschaft grundsätzlich erst nach erteilter gerichtlicher Bewilligung angeordnet werden.[273] In der Anordnung und Bewilligung sind unter anderem die Daten, die zu beschlagnahmen sind, zu umschreiben sowie ein konkreter Zeitraum zu definieren.[274] Die Durchführung der Beschlagnahme obliegt der Kriminalpolizei, wobei diese berechtigt ist, Datenträger und Daten bei Gefahr in Verzug auch von sich aus sicherzustellen.[275] Punktuelle Daten oder Daten, die die mittels Bild- und Tonaufzeichnungsgeräten an öffentlichen oder öffentlich zugänglichen Orten aufgenommen wurden, unterliegen weiterhin den allgemeinen Regelungen der Sicherstellung und sind daher ohne richterliche Bewilligung zulässig.[276] Beispielsweise stellen Kundenkarteien punktuelle Daten dar, wenn daraus „*bloß ein punktuelles Bild über eine Person gewonnen wird*“.[277] Bei einzelnen Ausweisdaten handelt es sich um punktuelle Daten aus einer Kundendatei, da daraus Informationen ersichtlich sind, die einen eng umrissenen Einblick in einen bestimmtes vertragli-

[272] Siehe zum betreffenden Absatz insgesamt VfGH 14.12.2023, G352/2021 (G352/2021-46).
[273] § 115f Abs 2 StPO.
[274] § 115f Abs 3 StPO.
[275] § 115f Abs 4 StPO.
[276] § 110 Abs 1 Z 1 StPO iVm § 110 Abs 2 StPO bzw § 110 Abs 1 Z 1 StPO iVm § 110 Abs 3a StPO.
[277] IA Strafprozessrechtsänderungsgesetz 2024 15/A 28. GP 30 https://www.parlament.gv.at/dokument/XXVIII/A/15/imfname_1660740.pdf.

ches Rechtverhältnis bieten.[278] Diese Daten können gemäß § 110 Abs 1 Z 1 und Abs 3a StPO von der Kriminalpolizei eigenmächtig sichergestellt werden.

6.2.3. Auskunft über Zugangsdaten gemäß § 135 Abs 1a zweiter Fall StPO

Weiters kann die Auskunft über Zugangsdaten gemäß § 135 Abs 1a zweiter Fall StPO die Identifizierung des Täters ermöglichen. Konkret handelt es sich um die Erteilung der Auskunft über Namen, Anschrift und Nutzerkennung zu öffentlichen IP-Adressen und über einzelne Informationen zu E-Mail-Daten.[279] Bei Letzteren handelt es sich um die Beauskunftung von Namen und Anschrift zu einer E-Mail-Adresse, der bei der Verwendung von E-Mail-Diensten einem Nutzer zugewiesenen Nutzerkennung sowie der E-Mail-Adresse und öffentlichen IP-Adresse des Absenders einer E-Mail (§ 134 Z 1b lit b bis d StPO).

So kann beispielsweise um Erteilung der Auskunft über Name, Anschrift und Nutzerkennung zu einer im Rahmen von Phishing-Mails genutzten IP-Adresse ersucht werden.[280] Aus den folgenden Gründen wird eine solche Auskunft möglicherweise jedoch kein geeignetes Mittel für weitere Ermittlungen darstellen: Einerseits fälschen Täter oftmals die bei der Straftat eingesetzten IP-Adressen (IP-Spoofing), weshalb die Täter anhand der IP-Adresse überhaupt nicht identifiziert werden können.[281] Andererseits schränkt die gesetzliche Bestimmung des § 135 Abs 1a zweiter Fall iVm § 134 Z 1b lit a StPO die Auskunftserteilung über öffentliche IP-Adressen ein. Die Auskunftserteilung ist nämlich nicht zulässig, wenn die öffentliche IP-Adresse vielen Nutzern, worunter eine Anzahl etwa ab 30 Personen zu verstehen ist, zugeordnet werden würde.[282] Aus technischer Sicht kann eine IP-Adresse bis zu mehreren tausend Personen zugewiesen werden.[283] Vor dem Hintergrund, dass IP-Adressen nur in limitierter Anzahl zur Verfügung stehen, machen Anbieter von der mehrfachen Zuweisung von IP-Adressen in mobilen Netzen – somit im Smartphone-Bereich als auch im Breitband-Bereich – oftmals Gebrauch.[284] Dementsprechend wird die betreffende Ermittlungsbefugnis in einigen Fällen nicht herangezogen werden können.

---

[278] Siehe dazu IA Strafprozessrechtsänderungsgesetz 2024 15/A 28. GP 30 https://www.parlament.gv.at/dokument/XXVIII/A/15/imfname_1660740.pdf, wonach punktuelle Daten jene Daten sind, *„die ein bestimmtes, zeitlich eng begrenztes vertragliches oder öffentlich-rechtliches Rechtsgeschäft oder Rechtsverhältnis betreffen*".

[279] § 134 Z 1b StPO.

[280] § 135 Abs 1a zweiter Fall StPO iVm § 134 Z 1b lit a StPO.

[281] *Büchel/Hirsch,* Internetkriminalität[2] 32.

[282] § 135 Abs 1a zweiter Fall StPO iVm § 134 Z 1b lit a; ErläutRV 2309 BlgNR 27. GP 32.

[283] ErläutRV 2309 BlgNR 27. GP 32.

[284] *Rundfunk und Telekom Regulierungs*-GmbH, RTR NETZ NEUTRALITÄTSBERICHT 2023 (2023) 31; ErläutRV 2309 BlgNR 27. GP 32.

6.2.4. Auskunft über Daten einer Nachrichtenübermittlung und Überwachung von Nachrichten gemäß § 135 StPO

Von grundlegender Bedeutung zur Identifizierung der Täter von Cybercrime Delikten und somit für den Ermittlungserfolg sind weiters die Auskunft über Daten einer Nachrichtenübermittlung gemäß § 135 Abs 2 StPO sowie die Überwachung von Nachrichten gemäß § 135 Abs 3 StPO. Die beiden Ermittlungsmaßnahmen bedürfen der Anordnung durch die Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung und die betreffenden Auskünfte sind von den Anbietern von Kommunikationsdiensten unverzüglich zu erteilen.[285]

Bei der Auskunft über Daten einer Nachrichtenübermittlung handelt es sich um die Erteilung einer Auskunft über Verkehrsdaten (im Wesentlichen über die Rufnummern, zu denen Anrufe getätigt wurden und von denen Anrufe erhalten wurden), Zugangsdaten (die nicht einer Anordnung gemäß § 135 Abs 1a zweiter Fall StPO unterliegen) und Standortdaten.[286] Eine solche Auskunft kann somit vor allem auch Rückschlüsse auf den Aufenthalt des Täters liefern.
Es könnten auch allfällige weitere Täter eruiert werden, da die Daten einer Nachrichtenübermittlung etwa Informationen über aktive Verbindungen (somit vom Täter getätigte Verbindungen) und passive Verbindungen (somit Verbindungen, die der Täter entgegennimmt bzw erhält) bereitstellen.[287]
Allerdings sind an die Erteilung der betreffenden Auskünfte strengere Voraussetzungen als für die in den vorherigen Punkten genannten Ermittlungsmaßnahmen gebunden. So ist die Auskunft unter anderem zulässig, wenn zu erwarten ist, dass dadurch die Aufklärung einer mit einer Freiheitsstrafe von mehr als einem Jahr vorsätzlich begangenen Straftat gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten eines Beschuldigten ermittelt werden können (§ 135 Abs 2 Z 3 StPO).

Dagegen regelt § 135 Abs 3 StPO das Überwachen von Nachrichten und Informationen, die von einer natürlichen Person über ein Kommunikationsnetz gemäß § 4 Z 1 TKG 2021 oder einen Dienst der Informationsgesellschaft gemäß § 1 Abs 1 Z 2 Notifikationsgesetz[288] gesendet, übermittelt und empfangen werden.[289] Die Überwachung von Nachrichten gemäß § 135 Abs 3 StPO betrifft somit vor allem das Eruieren von Kommunikationsinhalten.[290]

---

285 § 137 Abs 1 StPO; § 138 Abs 2 StPO.
286 § 134 Z 2 StPO; *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 5.65.
287 *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz,* WK StPO § 134 Rz 32.
288 Darunter wird „*jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung*“ verstanden. Beispiele dafür sind der Online-Vertrieb von Waren oder Access- und Hostproviding Dienste (*Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz,* WK StPO § 134 Rz 44).
289 § 134 Z 3 StPO.
290 *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 5.71.

Es können Inhalte von Telefonaten, SMS und E-Mails oder grundsätzlich auch Inhalte von Nachrichten, die über nummernunabhängige Dienste gesendet, übermittelt und empfangen werden, eruiert werden.[291]

Zur Überwachung von Nachrichten, die über nummernunabhängige Dienste ausgetauscht werden (beispielsweise über WhatsApp) ist aber anzumerken, dass diese meist verschlüsselt übertragen werden.[292] Aus diesem Grund wäre zur Eruierung des konkreten Nachrichteninhalts im Klartext eine Entschlüsselung erforderlich, was aber nur durch Eindringen in das zu überwachende Endgerät ohne Kenntnis dessen Inhabers und den anschließenden Einsatz einer Spionagesoftware am Kommunikationsgerät möglich wäre.[293] Eine diesen Voraussetzungen entsprechende Rechtsgrundlage hat der VfGH jedoch als verfassungswidrig aufgehoben, da die Regelung gegen das Recht auf Achtung des Privatlebens gemäß Art 8 EMRK verstoßen hat.[294]

Ebenso sind von § 135 Abs 3 StPO die Überwachung von Aufrufen von Websites oder das Surfen im Internet umfasst.[295]

Die Überwachung der genannten Inhalte und Informationen ist etwa zulässig, wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel von der Nachricht ist, der Verdächtige ist oder anzunehmen ist, dass der Verdächtige die technische Einrichtung benützen wird oder mit dieser eine Verbindung herstellen wird (§ 135 Abs 3 Z 3 StPO).

Eine solche Nachrichtenüberwachung ist daher beispielweise bei Verdacht eines schweren Betrugs unter Verwendung falscher oder verfälschter Daten gemäß § 147 Abs 1 Z 1 StGB, jedoch unter anderem nicht zur Aufklärung einer Datenfälschung nach § 225a StGB zulässig.

6.2.5. Auskunftspflichten bei Sachverhalten mit Auslandsbezug

Auch bei Vorliegen der materiellen und prozessualen Voraussetzungen können die zuvor genannten Ermittlungsmaßnahmen unter gewissen Umständen zur Verfolgung der Täter nicht geeignet sein. Dies vor allem dann, wenn die Täter vom Ausland aus agieren[296] (bzw Straftaten unter Nutzung von Rufnummern, die einem ausländischen Anbieter von Kommunikationsdiensten zugeteilt sind, verübt werden). In diesem Fall können Daten nur im Rahmen der Rechtshilfe bzw mittels der Europäischen Ermittlungsanordnung erlangt werden, wobei dies einige Zeit in

---

[291] *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz,* WK StPO § 134 Rz 45; ErläutRV 17 BlgNR 26. GP 8.
[292] *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz,* WK StPO § 134 Rz 45.
[293] *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz,* WK StPO § 134 Rz 45.
[294] VfGH 11.12.2019, G72/2019 ua (G72-74/2019-48, G181-182/2019-18).
[295] ErläutRV 17 BlgNR 26. GP 8.
[296] *Nemeth/Müller/*Feiler, Missbrauchspotenzial in neuer EU-Verordnung zu digitalen Beweismitteln https://www.derstandard.de/story/3000000172389/missbrauchspotenzial-in-neuer-eu-verordnung-zu-digitalen-beweismitteln (Stand 5.6.2023).

Anspruch nehmen kann.[297] Telekommunikationsdaten unterliegen aber strikten – zum Teil sehr kurzen – Aufbewahrungsfristen.[298] Ferner ist bei internationalen Anbietern der Ort der Datenspeicherung nicht immer eindeutig, weshalb das Rechtshilfeersuchen nicht immer mit Sicherheit an den richtigen Staat adressiert wird.[299] Diese Hindernisse sollen durch die Verordnung (EU) 2023/1543 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren („E-Evidence VO“) künftig behoben werden. Demnach sind Strafverfolgungsbehörden eines EU-Mitgliedstaats ab 18. August 2026 befugt, Anordnungen zur Herausgabe von Teilnehmer-, Verkehrs- und Inhaltsdaten direkt an Anbieter von elektronischen Kommunikationsdiensten anderer EU-Mitgliedstaaten zu übermitteln.[300] Künftig kann zB ein österreichisches Gericht direkt bei einem spanischen Anbieter die Herausgabe von Daten verlangen.

Je nachdem, welche Daten von der Herausgabeanordnung umfasst sind, bestehen unterschiedliche Voraussetzungen: So ist die Herausgabeanordnung hinsichtlich Verkehrs- und Inhaltsdaten etwa zulässig, wenn eine Straftat vorliegt, die im Anordnungsstaat mit einer Freiheitsstrafe von mindestens drei Jahren bedroht ist und sie vom Gericht im Anordnungsstaat validiert wurde.[301] Die Herausgabeordnung von Teilnehmerdaten zum Zweck der Ermittlung der Identität eines Verdächtigen (die weniger sensibel als Verkehrs- und Inhaltsdaten sind) kann nach gerichtlicher oder staatsanwaltschaftlicher Bewilligung für sämtliche Straftaten erlassen werden.[302] Erfordert die Herausgabeanordnung die Beauskunftung von Verkehrs- und/oder Inhaltsdaten (mit Ausnahme von ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten), ist diese auch an die zuständige nationale Behörde zu übermitteln.[303] Die nationale Behörde kann sodann grundsätzlich binnen 10 Tagen nach Erhalt der Unterrichtung Einwände gegen die Herausgabe der Daten geltend machen.[304]

Die E-Evidence VO sieht strikte Fristen vor, innerhalb derer die Betreiber die angeforderten Daten zu übermitteln haben. Diese sind seitens des Anbieters von Kommunikationsdiensten binnen 10 Tagen, in Notfällen sogar binnen 8 Stunden zu übermitteln, wobei die schriftliche Kom-

---

297 *Nemeth/Müller/*Feiler, Missbrauchspotenzial in neuer EU-Verordnung zu digitalen Beweismitteln https://www.derstandard.de/story/3000000172389/missbrauchspotenzial-in-neuer-eu-verordnung-zu-digitalen-beweismitteln (Stand 5.6.2023); siehe dazu etwa auch *Herrnfeld*, Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel, ZWF 2022, 2, wonach die Beweiserhebung im Ausland im Durchschnitt zwischen drei und sechs Monaten bzw gegebenenfalls auch bis zu einem Jahr betragen kann.

298 Siehe dazu genauer Punkt 8.1 der gegenständlichen Master Thesis; *Herrnfeld*, Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel, ZWF 2022, 2.

299 *Herrnfeld*, Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel, ZWF 2022, 2.

300 *Publications Office of the European Union*, Elektronische Beweismittel in Strafverfahren – Herausgabeanordnung und Sicherungsanordnung https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM:4649186 (Stand 30.5.2023); Art 4 und Art 5 E-Evidence VO.

301 Art 4 Abs 2 E-Evidence VO, Art 5 Abs 4 E-Evidence VO.

302 ErwG 36 E-Evidence VO, Art 4 Abs 1 E-Evidence VO, Art 5 Abs 3 E-Evidence VO.

303 Art 8 Abs 1 E-Evidence VO.

304 Art 12 E-Evidence VO.

munikation zwischen den Behörden und Anbietern von Kommunikationsdiensten über ein dezentrales IT-System erfolgen wird.[305]

6.3. Ergebnis

Wie oben dargestellt, stehen den zuständigen Behörden vielfache, zum Teil sehr eingriffsintensive Ermittlungsbefugnisse zur Verfügung. In einigen Fällen werden diese Ermittlungsansätze zur Ausforschung der Täter zielführend sein. Bei gewissen Formen von Identitätsmissbrauch, wie zB Spoofing, werden sie allerdings zu unbeteiligten Personen führen, die zunächst unberechtigt verdächtigt werden, eine Straftat begangen zu haben. Den Maßnahmen der Behörden sind somit in der Praxis Grenzen gesetzt.
Hinsichtlich der aufgrund der fortschreitenden Digitalisierung stetig neu auftretenden und veränderten Formen von Identitätsmissbrauch ist zum einen (sowohl seitens der nationalen als auch europäischen Gesetzgebung) darauf zu achten, auch die Ermittlungsbefugnisse weiterzuentwickeln, sodass eine effektive und erfolgreiche Strafverfolgung sichergestellt wird. So hat der europäische Gesetzgeber zuletzt etwa durch die Einführung der E-Evidence VO auf den Umstand, dass Straftaten (wie ua Identitätsmissbrauch-Phänomene) in der digitalen Welt auch vom Ausland aus begangen werden[306], reagiert. Dadurch soll es in den kommenden Jahren zu einer effektiveren Strafverfolgung bei Sachverhalten mit Auslandsbezug kommen.[307] Zum anderen ist es maßgeblich, dass hinreichend Personal mit den für den Bereich Cybercrime fachspezifischen Kenntnissen zur Verfügung steht. So wurden Mitte 2024 der Kriminalassistenzdienst (der den Kriminaldienst bei der Tatortarbeit, IT-Forensik und Präventionsarbeit unterstützen soll) sowie Cybercrime-Trainingscenter (die die Ausbildung von Cybercrime-Spezialisten zum Ziel haben) implementiert.[308]

7. Telekommunikationsrechtliche Aspekte

In diesem Abschnitt werden die telekommunikationsrechtlichen Aspekte im Zusammenhang mit Identitätsmissbrauch näher dargelegt. Hierbei ist zu erwähnen, dass unter die Regulierung des TKG 2021 gemäß dem Marktortprinzip grundsätzlich alle in Österreich angebotenen Kommuni-

---

[305] Art 10 E-Evidence VO, Art 19 bis 23 E-Evidence VO.
[306] Siehe etwa *Herrnfeld*, Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel, ZWF 2022, 2, die anführt, dass eine Vielzahl an Straftaten „*in der digitalen Welt ohne jegliche territoriale Grenze begangen werden können*."
[307] *Kilic*, Die EU-Verordnung 2023/1543 (Beweismittelsicherungs-VO) vereinfacht den Zugriff auf elektronische Beweismittel im Fokus der Strafverfolgung, RZ 2024, 307.
[308] *Bundesministerium für Inneres*, Bundeskriminalamt: Modernisierung des Kriminaldienstes: Start für Kriminalassistenzdienststellen https://www.bmi.gv.at/news.aspx?id=635763326733366B5261303D (Stand 2.6.2024).

kationsdienste, unabhängig vom Sitz des Anbieters, fallen.[309] Das bedeutet jedoch nicht, dass die gesamten Bestimmungen des TKG 2021 für alle Kommunikationsdienste gelten. So beschränken manche Regelungen ihre Anwendbarkeit auf einzelne Arten von Kommunikationsdiensten.

Im Folgenden wird zunächst thematisiert, welche Auswirkungen die Registrierungspflicht gemäß § 166 Abs 2 TKG 2021 auf die Strafverfolgung hat. Sodann wird erörtert, ob ausgewählte telekommunikationsrechtliche Normen als präventive Sicherheitsmaßnahmen gegen einzelne kriminelle Erscheinungsformen beitragen. Hierbei wird der Schwerpunkt auf § 121 TKG 2021, der Maßnahmen gegen Nummernmissbrauch vorsieht, sowie auf die Bestimmungen der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009)[310], die die Anzeige von Rufnummern regeln, gelegt.

7.1. Registrierungspflicht gemäß § 166 Abs 2 TKG 2021 versus Identitätsmissbrauch

Laut einem Bericht der GSM Association („GSMA“, die weltweite Vereinigung von Mobilfunkanbietern) war die Prepaid SIM Registrierung im Jahr 2021 bereits in 157 Ländern verpflichtend vorgeschrieben[311]. Die Registrierungspflicht ist unterschiedlich ausgestaltet. In einigen Ländern waren mit Stand Ende 2020 Identitätsdaten zu erfassen sowie zu speichern und nur auf Anfrage einzelnen Behörden zur Verfügung zu stellen.[312] In wenigen Ländern waren die von den Betreibern erfassten Identitätsdaten dagegen mit Behörden proaktiv zu teilen.[313] Weiters waren mit Stand Februar 2021 in einzelnen Ländern die vom Kunden im Rahmen der SIM-Karten-Registrierung angeführten Daten mit einer zentralen staatlichen Datenbank abzugleichen.[314]

In Österreich ist die Registrierung von SIM-Karten seit 01.01.2019 verpflichtend vorgeschrieben. Betreiber von öffentlichen Kommunikationsdiensten sind gemäß § 166 Abs 2 TKG 2021 verpflichtet, die Identität ihrer Kunden zu erheben und die zur Identifizierung erforderlichen Stammdaten (Titel, Name und Geburtsdatum) anhand geeigneter Identifizierungsverfahren (bspw durch Vorlage eines amtlichen Lichtbildausweises, Bankident-Verfahren oder Photoident-Verfahren[315]) zu registrieren.

---

309 § 4 Z 4 TKG 2021; *Abazagic*, WhatsApp, Facebook Messenger & Co im TKG 2021: Zur Regulierung nummernunabhängiger interpersoneller Kommunikationsdienste, MR 2022, 343 (344).
310 BGBl II 2009/212.
311 *GSMA*, Access to Mobile Services and Proof of Identity 2021 (2021) 15.
312 *GSMA*, Access to Mobile Services and Proof of Identity 2021 (2021) 16.
313 *GSMA*, Access to Mobile Services and Proof of Identity 2021 (2021) 16.
314 *GSMA*, Access to Mobile Services and Proof of Identity 2021 (2021) 16.
315 §§ 3 bis 5 IVO.

Wie bereits unter Punkt 3.1 der gegenständlichen Master Thesis ausgeführt, war das Ziel dieser Einführung, dass Kunden von Kommunikationsdiensteanbietern im Anlassfall identifizierbar sind, damit die effektive Strafverfolgung sowie Gefahrenabwehr möglich sind.[316] Die von den Anbietern erfassten Daten sind lediglich auf Anfrage von dazu berechtigen Behörden zu beauskunften.[317]

Ob zum Zwecke der effektiveren Gefahrenabwehr und Strafverfolgung tatsächlich die Einführung einer Identifizierungs- und Registrierungsverpflichtung erforderlich sei, wurde im Vorfeld der Einführung massiv diskutiert. Seitens der Internet Service Providers Austria („ISPA", Dachverband der österreichischen Internet Service-Anbieter) wurde angeführt, dass die Einführung der verpflichtenden Identifizierung/Registrierung in einigen Ländern zu keinem Nutzen für die Strafverfolgungsbehörden geführt habe.[318] In diesem Zusammenhang verwies diese auch auf das Risiko, dass sich Kriminelle mittels gefälschter Dokumente ausweisen können oder ein Schwarzmarkt für Prepaid-SIM-Karten entstehen könne.[319] Es ist weiters auf die Möglichkeit des Erwerbes von anonymen SIM-Karten aus anderen Ländern hinzuweisen.[320]

Laut einer Studie der GSMA vom Jahr 2016 konnte durch die obligatorische SIM-Karten Registrierung bis dahin grundsätzlich kein direkter Rückgang der Kriminalität nachgewiesen werden.[321] Dem kann entgegnet werden, dass nach der Einführung der Registrierungspflicht zumindest eine Chance zur Strafverfolgung besteht. Zuvor war es Anbietern von Kommunikationsdiensten aufgrund von anonymen SIM-Karten zum Teil nicht möglich, Behörden auf deren Anfrage Auskunft über Stammdaten ihrer Kunden zu erteilen. Auch wenn – aufgrund der sich stets weiterentwickelnden Phänomene – die Täterschaft nicht immer festgestellt werden kann, wurde durch die Registrierungsverpflichtung für berechtigte Behörden zumindest ein Ermittlungsansatz geschaffen.[322]

---

316 ErläutRV 15 BlgNR 26. GP 5; Vorblatt und WFA 15 BlgNR 26. GP 3.

317 Siehe dazu beispielsweise Punkt 6.2.1. „Auskunft über Stammdaten gemäß § 181 Abs 9 TKG 2021 iVm § 135 Abs 1a erster Fall StPO" der gegenständlichen Master Thesis.

318 *Internet Service Providers Austria*, ISPA-STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES MIT DEM DAS SICHERHEITSPOLIZEIGESETZ, DAS BUNDESSTRAßEN-MAUTGESETZ 2002, DIE STRAßENVERKEHRSORDNUNG 1960 UND DAS TELEKOMMUNIKATIONSGESETZ 2003 GEÄNDERT WERDEN https://www.parlament.gv.at/dokument/XXV/SNME/29465/imfname_666671.pdf (Stand 18.8.2017) 4.

319 *Internet Service Providers Austria*, ISPA-STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES MIT DEM DAS SICHERHEITSPOLIZEIGESETZ, DAS BUNDESSTRAßEN-MAUTGESETZ 2002, DIE STRAßENVERKEHRSORDNUNG 1960 UND DAS TELEKOMMUNIKATIONSGESETZ 2003 GEÄNDERT WERDEN https://www.parlament.gv.at/dokument/XXV/SNME/29465/imfname_666671.pdf (Stand 18.8.2017) 4.

320 *Forgó* in *Steinmaurer,* TKG 2021 § 166 Rz 10 (Stand 1.9.2024, rdb.at).

321 *GSMA*, Mandatory registration of prepaid SIM cards: Addressing challenges through best practice (2016) 2.

322 Siehe dazu unter anderem die Entscheidung des EGMR 30.01.2020, Bsw 50001/12, *Breyer gg Deutschland*, Rn 90, in der der Gerichtshof wie folgt ausführt: „*Wie der GH anerkennt, erleichtert und beschleunigt die Vorregistrierung von Mobiltelefon-Teilnehmern die Ermittlungen durch die Strafverfolgungsbehörden erheblich und kann dadurch zu einer effektiven Strafverfolgung und einer Verhütung von Straftaten beitragen*."

Als weiteres Argument gegen die Identifizierungs-/Registrierungsverpflichtung wurde genannt, dass durch deren Einführung die Nutzer von SIM-Karten unter Generalverdacht gestellt werden würden.[323]

Die Kritik, dass die Registrierungsverpflichtung weder erforderlich noch verhältnismäßig sei, brachten Jonas und Patrick Breyer im Rahmen ihrer Individualrechtsbeschwerde vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) vor.[324] Sie sahen sich durch die in Deutschland bestehende Registrierungspflicht von Prepaid SIM-Karten (nach welcher – ähnlich wie in Österreich – Name, Anschrift, Geburtsdatum sowie Datum des Vertragsbeginns über Anschlussinhaber zu erheben und speichern sind; in der damaligen deutschen Fassung bestand aber noch keine Verpflichtung, die Daten der Personen durch geeignete Identifizierungsverfahren zu verifizieren) in ihren Rechten auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK sowie auf Freiheit der Meinungsäußerung nach Art 10 EMRK verletzt.[325] Die Frage, ob die Registrierungspflicht für Prepaid-SIM-Karten mit den genannten Rechten vereinbar ist, wurde im Jahr 2020 vom EGMR entschieden.[326] Prüfungsmaßstab des gegenständlichen Falls war ausschließlich Art 8 EMRK, da der Schwerpunkt nicht auf dem Eingriff in die Korrespondenz (und somit auf der Meinungsäußerungsfreiheit), sondern auf der Speicherung der Daten lag.[327]
Unstrittig war, dass die Speicherung der Daten einen Eingriff in das Recht auf Achtung des Privatlebens darstellt, da der Begriff „Privatleben“ weit auszulegen ist.[328]
Die Speicherung der angeführten Daten war gesetzlich vorsehen.[329] Auch die Zugriffsrechte der Behörden, die in gegenständlichem Fall zu berücksichtigen waren, wurden durch das Gesetz entsprechend geregelt.[330] Weiters war ein legitimer Zweck für den Eingriff in Art 8 EMRK gegeben.[331] Die Registrierungspflicht verfolgte nämlich die Ziele der „*öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung, der Verhütung von Straftaten und des Schutzes der Rechte und Freiheiten anderer*“.[332]
Zur Frage, ob die Maßnahme in einer demokratischen Gesellschaft tatsächlich notwendig ist, führt der Gerichtshof aus, dass die Verbrechensbekämpfung, die öffentliche Sicherheit und der Schutz der Rechte Dritter durchaus notwendig seien – die einzelnen Staaten hätten dabei einen

[323] So bspw die Datenschutzorganisation *epicenter.works*, Überwachungspaket https://epicenter.works/thema/ueberwachungspaket (abgefragt am 3.4.2025).
[324] EGMR, 30.01.2020, Bsw 50001/12, *Breyer gg Deutschland*.
[325] *Spittka*, Registrierungspflicht für Prepaid-SIM-Karten verstößt nicht gegen EMRK: Zugleich Besprechung von EGMR, Entscheidung vom 30.1.2020 – Nr. 50001/12 – Breyer gegen Deutschland, KuR 2020, 263 (264, 266).
[326] *Spittka*, KuR 2020, 263.
[327] *Spittka*, KuR 2020, 263 (264).
[328] EGMR 30.01.2020, Bsw 50001/12, *Breyer gg Deutschland*, Rn 74, 81.
[329] *Spittka*, KuR 2020, 263 (265).
[330] *Spittka*, KuR 2020, 263 (265).
[331] *Spittka*, KuR 2020, 263 (265).
[332] EGMR 30.01.2020, Bsw 50001/12, *Breyer gg Deutschland*, Rn 86.

gewissen Ermessensspielraum.[333] Im Rahmen der Verhältnismäßigkeitsprüfung (Abwägung der öffentlichen Interessen und privaten Interessen) wurde insbesondere dargelegt, dass bloß eine begrenzte Speicherung von einzelnen Bestandsdaten erfolgt, dabei aber weder Verkehrs- noch Standortdaten erhoben werden.[334]
Aus den genannten Gründen wurde entschieden, dass die Registrierungspflicht von Prepaid-SIM-Karten mit Art 8 EMRK vereinbar und somit zulässig ist.[335]

7.2. Maßnahmen gegen Nummernmissbrauch gemäß § 121 TKG 2021

Um auf die fortschreitende Digitalisierung und den damit einhergehenden vielschichtigen Möglichkeiten der rechtsmissbräuchlichen Nutzung von Telekommunikationsdiensten zu reagieren, wurden auch im Europäischen Kodex für elektronische Kommunikation (EECC) durch die Einführung von Art 97 Abs 2 entsprechende Schritte gesetzt. Nach dieser Rechtsgrundlage kann es Anbietern unter anderem auferlegt werden, den Zugang zu bestimmten Rufnummern oder Diensten zur Unterbindung von Betrug bzw Missbrauch zu sperren.[336]

Die betreffende Bestimmung wurde in Österreich durch § 121 TKG 2021 umgesetzt und dehnte die bisherigen Eingriffsmöglichkeiten der Regulierungsbehörde aus.[337] § 121 TKG 2021 sieht für die Regulierungsbehörde bestimmte Möglichkeiten vor, um auf Nummernmissbrauch, wovon der rechtswidrige Gebrauch von Rufnummern im Rahmen von Betrugs- bzw Datendiebstahlversuchen und sonstigen Belästigungen umfasst ist[338], zu reagieren.
So kann Anbietern bei erheblichem Rufnummernmissbrauch per Bescheid die Sperre von Nummern oder Nummernbereichen oder die Vorschaltung kostenfreier automatisierter Sprachinformationen aufgetragen werden.[339] Unter erheblichem Rufnummernmissbrauch „*sind alle Verhaltensweisen zu verstehen, die in größerem Umfang wiederholt gesetzt werden und die kumuliert einen ungerechtfertigten und nicht geringfügigen Eingriff in die Privatsphäre oder Vermögenslage von Endnutzern beabsichtigen, darstellen oder zumindest in Kauf nehmen*“ (§ 121 Abs 2 TKG 2021). Bei den Maßnahmen sollte das effektivste Mittel gewählt werden und parallel dazu die Interessen der Endnutzer sowie technischen Möglichkeiten beachtet werden.[340]

---

333 *Spittka*, KuR 2020, 263 (265); EGMR 30.01.2020, Bsw 50001/12, *Breyer gg Deutschland*, Rn 108.
334 *Spittka*, KuR 2020, 263 (265).
335 EGMR 30.01.2020, Bsw 50001/12, *Breyer gg Deutschland*, Rn 110.
336 Art 97 Abs 2 Richtlinie (EU) 2018/1972 des europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl L 2018/321, 36.
337 *Steinmaurer*, Telekommunikationsrecht – der Europäische Kodex für die elektronische Kommunikation, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021) Rz 15.22 – 15.24.
338 ErläutRV 1043 BlgNR 27. GP 40.
339 § 121 Abs 2 iVm 4 TKG 2021.
340 § 121 Abs 4 TKG 2021.

In diesem Zusammenhang ist die im TKG 2021 verankerte Rechtsgrundlage der „Interoperabilität" zu beachten.[341] Im Rahmen der Interoperabilität gemäß § 50 TKG 2021 haben Anbieter von Sprachkommunikationsdiensten und nummerngebundenen Textnachrichten nämlich sicherzustellen, dass ihre Kunden grundsätzlich alle Rufnummern der nationalen Nummerierungspläne der Mitgliedstaaten der Europäischen Union erreichen können.[342] Entsprechende Einschränkungen haben angemessen und notwendig zu sein.[343] Da die Sperre von Rufnummern die Interoperabilität berührt, ist eine solche wohl vorzugsweise erst dann aufzutragen, wenn kein anderes effektives Mittel zur Verhinderung des Missbrauchsszenarios zur Verfügung steht.[344] Zu beachten ist dabei auch, dass eine Sperre von konkreten einzelnen Rufnummern nicht immer zweckmäßig ist – so beispielsweise, wenn Call-ID Spoofing betrieben wird, da die Anrufe nicht von der manipulierten Rufnummer, sondern von einem anderen Anschluss ausgehen.[345] Eine derartige Sperre sowie die Sperre von Nummernbereichen können daher zur Folge haben, dass tatsächlich unbeteiligte Personen nicht mehr erreichbar sind bzw keine Kommunikationsdienste mehr in Anspruch nehmen können.[346]

Das Setzen derartiger Maßnahmen kann, sofern sie nicht objektiv gerechtfertigt sind, in den Grundsatz der Nichtdiskriminierung gemäß § 128 TKG 2021 eingreifen, da grundsätzlich jedermann (unabhängig von Staatsangehörigkeit, Wohnsitz oder Ort der Niederlassung) berechtigt ist, Kommunikationsdienste zu nutzen.[347] Sofern Personen, zB aufgrund ihres Geschlechts oder ihrer ethnischen Zugehörigkeit bei der Inanspruchnahme einer Dienstleistung eine weniger günstige Behandlung erfahren, liegt eine Diskriminierung vor, die gemäß § 31 Gleichbehandlungsgesetz (GlBG) untersagt ist.
Somit ist stets darauf zu achten, dass die aufgetragenen und ergriffenen Maßnahmen angemessen sind und entsprechend befristet werden.[348]

Neben den beschriebenen Möglichkeiten, auf bereits bekannten Nummernmissbrauch zu reagieren, ist die Präventionsarbeit zur Bekämpfung von Nummernmissbrauch maßgeblich.[349]

---

[341] *Rundfunk und Telekom Regulierungs-GmbH*, 117. Mobilregulierungsdialog https://www.rtr.at/TKP/aktuelles/veranstaltungen/veranstaltungen/Mobilregulierungsdialog/117Mobilregulierungsdialog.de.html (117. Regulierungsdialog Maßnahmen Ping-Anrufe durch Betreiber.pdf, Stand 16.4.2021).
[342] ErläutRV 1043 BlgNR 27. GP 21.
[343] ErläutRV 1043 BlgNR 27. GP 41.
[344] *Rundfunk und Telekom Regulierungs-GmbH*, 117. Mobilregulierungsdialog https://www.rtr.at/TKP/aktuelles/veranstaltungen/veranstaltungen/Mobilregulierungsdialog/117Mobilregulierungsdialog.de.html (117. Regulierungsdialog Maßnahmen Ping-Anrufe durch Betreiber.pdf, Stand 16.4.2021).
[345] *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).
[346] *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).
[347] § 128 TKG 2021.
[348] § 121 Abs 2 TKG 2021.
[349] ErläutRV 1043 BlgNR 27. GP 41.

Den Anbietern von Kommunikationsdiensten kommt hierbei eine bedeutende Rolle zu. Beispielsweise können sie durch Informationen über gängige Phänomene von Nummernmissbrauch auf ihren Webseiten zur Sensibilisierung und Aufklärung beitragen.[350] Da der Großteil der in Österreich lebenden Personen Smartphones nutzt[351], kann durch eine solche Maßnahme de facto die gesamte Bevölkerung erreicht werden. Durch das Ergreifen präventiver Maßnahmen kann die Anzahl der vom Missbrauch betroffenen Opfer gebührend vermindernd werden.

7.3. Regelungen betreffend die Rufnummer des Anrufers gemäß KEM-V 2009

In den beiden vorherigen Punkten wurde vor allem darauf eingegangen, welche Maßnahmen Behörden und Anbieter von Kommunikationsdiensten nach Bekanntwerden krimineller Verhaltensweisen setzen können. Nun soll erörtert werden, ob nicht schon durch das Ergreifen von ex-ante Maßnahmen das Auftreten von neuen Phänomenen im Zusammenhang mit Identitätsmissbrauch unterbunden werden kann.

Bis vor Kurzem regelte im Wesentlichen § 5 KEM-V 2009 in welcher Form Rufnummern bei einer angerufenen Person aufzuscheinen haben.[352] Danach ist grundsätzlich seitens der Kommunikationsnetz- und Kommunikationsdiensteanbieter sicherzustellen, dass eine rückrufbare Rufnummer übertragen wird.[353] Eine Ausnahme davon ist zB gegeben, wenn die Rufnummernunterdrückung aktiviert wurde.[354] Auch bei von ausländischen Kommunikationsnetzen stammenden Anrufen ist in der Regel die Rufnummer anzuzeigen, die über das jeweilige ausländische Netz übergeben wurde.[355] Einzelne Rufnummernbereiche sind davon ausgenommen - so ist es bspw untersagt, Rufnummern für frei kalkulierbare Mehrwertdienste (denen die Rufnummernbereiche 900, 901, 930 und 931 zugeordnet sind)[356] als anrufende Nummer zu nutzen.[357] Ebenso ist es lediglich Telefonauskunftsdiensten gestattet, die für deren Dienste vorgesehene öffentliche Kurzrufnummer 118 einzusetzen.[358]
Aus den dargestellten Regelungen kommt die Bedeutung der Richtigkeit der Rufnummernanzeige hervor, dennoch lieferten sie keine hinreichende Abhilfe gegen eine vorherrschende Form des Identitätsmissbrauchs, nämlich Call-ID Spoofing.

---

[350] Zur Relevanz der Bewusstseinsbildung und Aufklärung der Bevölkerung siehe *Bundesministerium für Inneres/Bundeskriminalamt*, Cybercrime Report 2023, 31.
[351] *Statista GmbH*, Anteil der Smartphone-Besitzer sowie Nutzung von Mobile Commerce in Österreich von 2013 bis 2023 https://de.statista.com/statistik/daten/studie/568185/umfrage/smartphone-besitz-und-smartphone-nutzung-in-oesterreich/ (abgefragt am 3.4.2025).
[352] Erläut zur KEM-V 2009, BGBl II 2009/212, § 5.
[353] § 5 Abs 3 KEM-V 2009.
[354] § 5 Abs 3 KEM-V 2009; Erläut zur KEM-V 2009, BGBl II 2009/212, § 5.
[355] § 5 Abs 4 KEM-V 2009.
[356] § 86 KEM-V 2009.
[357] § 5 Abs 5 KEM-V 2009.
[358] § 5 Abs 5 KEM-V 2009, § 43 KEM-V 2009.

Dagegen wurden in Deutschland bereits im Dezember 2022 entsprechende Maßnahmen gegen Spoofing eingeführt.[359] Als technischer Schutzmechanismus dient unter anderem das Verbot der Übermittlung und Anzeige bestimmter Rufnummern (für Auskunftsdienste, Massenverkehrsdienste, Premium-Dienste, Kurzwahldienste sowie die Notrufnummern 110 und 112) als Rufnummer des Anrufers.[360] Derartige Anrufe müssen seitens der Anbieter von Telekommunikationsdiensten abgebrochen werden.[361] Darüber hinaus dürfen lediglich dann deutsche Rufnummern als anrufende Nummern angezeigt werden, wenn die Verbindung aus dem deutschen Telefonnetz stammt.[362] Sofern ein Anruf mit einer deutschen Absendernummer aus dem ausländischen Telefonnetz übergeben wird, ist die Rufnummernanzeige zu unterdrücken, ausgenommen ein deutscher Nutzer tätigt den Anruf vom Ausland nach Deutschland.[363] Letztere Maßnahme wurde vor dem Hintergrund, dass zahlreiche Anrufe, bei denen die Manipulation von Rufnummern angewendet wird, vom Ausland aus getätigt werden, eingeführt.[364] Dadurch, dass in diesem Fall die Rufnummer (ausgenommen bei internationalem Roaming) unterdrückt wird, wird bei den angerufenen Personen kein falsches Vertrauen in die Authentizität der angezeigten Rufnummer erweckt.[365] Gleichwohl kann Call-ID Spoofing nicht zur Gänze verhindert werden.[366]

Die beschriebenen Maßnahmen stellen einen ersten Schritt zur Bekämpfung von Spoofing dar. Gleichzeitig bewirkt die Einführung dieser Regelungen in einzelnen Ländern die Verlagerung des Missbrauchs ins Ausland. So wird davon ausgegangen, dass aufgrund der ergriffenen Maßnahmen in Deutschland vermehrt österreichische Telefonnummern zum Missbrauch herangezogen wurden.[367] Aufgrund des Umstands, dass Spoofing auch in Österreich häufig im Rahmen betrügerischer Handlungen eingesetzt wird, erwog auch die RTR-GmbH Maßnahmen gegen die unzulässige Verfälschung von Rufnummern in die Wege zu leiten.[368]

---

359 *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

360 *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

361 § 120 Abs 3 dTKG; *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

362 § 120 Abs 4 dTKG.

363 § 120 Abs 4 dTKG; *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

364 *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

365 *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

366 *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

367 *Rundfunk und Telekom Regulierungs-GmbH*, JAHRESBERICHT der Schlichtungsstellen 2023 (2024) 30.

368 *Rundfunk und Telekom Regulierungs-GmbH*, Öffentliche Konsultation der RTR zum Entwurf einer Novelle der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009) https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/konsultationen/konsult9nov_kem-v_2009.de.html (Stand 2.10.2023).

Mit der Einführung von § 5a KEM-V soll das Spoofing bei Sprachanrufen mit österreichischen Rufnummern aus dem Ausland nach Österreich unterbunden werden. Gemäß der Bestimmung haben österreichische Anbieter von Kommunikationsdiensten grundsätzlich zu überprüfen, ob tatsächlich jene Person anruft, deren Rufnummer angezeigt wird und, sofern eine solche Verifizierung nicht sichergestellt werden kann, die Anzeige der anrufenden Rufnummer zu unterdrücken. Sollten im Rahmen der Verifizierung zweifelsweise Hinweise vorliegen, dass der Anruf nicht von jener Person ausgeht, der die Rufnummer zugeteilt wurde, haben die Anbieter die Zustellung des Anrufs sogar zu unterbinden. Ausgenommen von der Unterdrückung der Rufnummer sind jene Anrufe, von denen keine betrügerischen Intentionen und somit keine Gefahr für die angerufene Person ausgeht (zB technische Anwendungen wie ein Notfalltelefon in Liftanlagen). Angesichts des Implementierungsaufwandes wurde den Betreibern eine Umsetzungsfrist gewährt, sodass die Bestimmung für mobile Rufnummern spätestens seit dem 1.9.2024 anzuwenden ist.[369]

7.4. Ausblick

Durch die zuvor angeführten Maßnahmen wird ein erster Schritt gegen Spoofing gesetzt. Die entsprechenden Gegenmaßnahmen sind allerdings noch erweiterungsfähig, da durch § 5a KEM-V 2009 zwar das Spoofing mit österreichischen Rufnummern in Österreich, nicht aber das Spoofing bei SMS, das Spoofing mit österreichischen Rufnummern im Ausland oder das Spoofing mit ausländischen Rufnummern in Österreich adressiert wird.[370] Die RTR-GmbH hat in ihrer Öffentlichen Konsultation zum Budget 2025 bereits festgehalten, dass die Weiterentwicklung der betreffenden Rechtsgrundlagen erforderlich ist und als ein wesentliches Ziel „*die Sicherstellung des Vertrauens in den österreichischen Rufnummernraum sowohl bei Telefonaten als auch bei SMS*“ definiert.[371]

Neben der Gefahr, dass Personen dem Absender einer Nachricht ihr Vertrauen entgegenbringen, kann auch vom Inhalt einer Nachricht eine Gefahr ausgehen. Als prominentes Beispiel dafür kann das Phänomen Flubot genannt werden, wodurch – sofern der Inhalt der Nachricht befolgt wurde – auf einigen Endgeräten eine Malware installiert wurde (siehe dazu genauer Punkt 4.4 der gegenständlichen Master Thesis). Angesichts dessen wird über die verpflichtende Einführung einer sogenannten „SMS-Firewall“, die betrügerische Nachrichten bzw Phishing-

[369] Siehe zum betreffenden Absatz insgesamt § 5a KEM-V 2009; Erläut zur 9. Novelle der KEM-V 2009 nach § 112 TKG 2021.

[370] *Rundfunk und Telekom Regulierungs-GmbH*, Newsletter RTR.Telekom.Post, RTR plant neue rechtliche Rahmenbedingungen gegen Spoofing https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/Newsletter/telekom_und_post_newsletter_03-2023.de.html (Stand 25.10.2023).

[371] *Rundfunk und Telekom Regulierungs-GmbH*, Öffentliche Konsultation der RTR zum Budget 2025 https://www.rtr.at/rtr/wer_wir_sind/Organisation/Finanzierung/Budgetkonsultation/Konsultation-der-RTR-zum-Budget-2025.de.html (Budget_2025_Konsultationsdokument.pdf S 34, Stand 12.11.2024).

Nachrichten ausfiltern soll, diskutiert.[372] Ohne entsprechende gesetzliche Regelung würde eine Inhaltsüberprüfung von gesendeten bzw empfangenen Nachrichten jedoch gegen das im TKG 2021 verankerte Kommunikationsgeheimnis, wonach das „*Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten*“ unzulässig ist, verstoßen.[373] Eine solche Nachrichtenfilterung mittels unterschiedlicher technischer Ausgestaltung ist in anderen europäischen Ländern bereits in Betrieb bzw angedacht.[374]
Abzuwarten bleibt, ob bzw in welcher Form eine solche Nachrichtenanalyse in Österreich umgesetzt werden wird.

7.5. Ergebnis

Es ist faktisch unmöglich, alle potenziell künftig auftretenden Phänomene von Identitätsmissbrauch zu verhindern bzw aufzuklären. Durch das Inkrafttreten der Identifizierungs- und Registrierungsverpflichtung sowie die im TKG 2021 und der KEM-V 2009 vorgesehenen Maßnahmen gegen Nummernmissbrauch wurden bereits entsprechende regulatorische Schritte gesetzt. Ebenso sind die von Kommunikationsdiensteanbietern ergriffenen freiwilligen Maßnahmen zum Schutz ihrer Kunden von erheblicher Bedeutung.

Zudem ist ein besonderes Augenmerk auf die laufende Evaluierung und Weiterentwicklung von technischen Maßnahmen sowie auf deren verpflichtende Umsetzung durch die Einführung von neuen rechtlichen Vorschriften zu legen. Denn mithilfe effektiver technischer Maßnahmen können bereits bekannte Erscheinungsformen bekämpft werden und dadurch die Bevölkerung vor Identitätsmissbrauch und dessen erheblichen negativen Folgen erfolgreich geschützt werden.

8. Datensicherheitsrechtliche Aspekte

Der letzte Abschnitt der gegenständlichen Master Thesis widmet sich den datensicherheitsrechtlichen Aspekten im Zusammenhang mit Identitätsmissbrauch. Die Anbieter von Kommuni-

---

[372] *„Die Presse" Verlags-Gesellschaft m.b.H. & Co KG*, SMS-Firewall: Mobilfunker scannen Handynachrichten https://www.diepresse.com/19466282/sms-firewall-mobilfunker-scannen-handynachrichten (Stand 13.3.2025); *Wiese*, Noch 2025 soll in Österreich die SMS-Firewall kommen https://futurezone.at/netzpolitik/sms-firewall-oesterreich-deutschland-spanien-phishing-malware/403021170 (Stand 13.3.2025).

[373] § 161 Abs 3 TKG 2021; *„Die Presse" Verlags-Gesellschaft m.b.H. & Co KG*, SMS-Firewall: Mobilfunker scannen Handynachrichten https://www.diepresse.com/19466282/sms-firewall-mobilfunker-scannen-handynachrichten (Stand 13.3.2025); *Wiese*, Noch 2025 soll in Österreich die SMS-Firewall kommen https://futurezone.at/netzpolitik/sms-firewall-oesterreich-deutschland-spanien-phishing-malware/403021170 (Stand 13.3.2025).

[374] Siehe *Wiese*, Noch 2025 soll in Österreich die SMS-Firewall kommen https://futurezone.at/netzpolitik/sms-firewall-oesterreich-deutschland-spanien-phishing-malware/403021170 (Stand 13.3.2025): So plant ein deutscher Netzbetreiber, verdächtige Links auszufiltern, wobei aber nicht der Inhalt der Nachricht an sich überwacht werden soll. Weiters sind seitens der spanischen Netzbetreiber jegliche Anrufe/SMS zu blockieren, die von Absendern ausgehen, die nicht durch Eintragung in eine behördliche Datenbank entsprechend legitimiert sind.

kationsdiensten verarbeiten eine Reihe von Kundendaten, die den Kunden sowie Behörden auf verschiedensten Wegen zugänglich gemacht werden können. Die unberechtigte Zugänglichmachung von Kundendaten über diverse Kanäle, wie zB über das Kundenservice, einen Online-Zugang oder den Shop eines Anbieters, gilt es zu schützen.[375] Im Folgenden werden die auf Kommunikationsanbieter anwendbaren datenschutzrechtlichen Vorschriften dargelegt. Darüber hinaus wird anhand ausgewählter nationaler sowie internationaler Rechtsprechung auf die Relevanz der Implementierung von geeigneten und effektiven technischen und organisatorischen Maßnahmen, um das Risiko von Identitätsmissbrauch zu minimieren, eingegangen.

8.1. Rechtsgrundlagen

Anbieter von Kommunikationsdiensten sind Adressaten verschiedenster datenschutzrechtlicher Bestimmungen. So unterliegen sie einerseits der DSGVO und somit deren Art 32.

Nach der Regelung des Art 32 DSGVO haben Anbieter von Kommunikationsdiensten „*unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen [...] geeignete technische und organisatorische Maßnahmen [zu treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten*“.

Der Anbieter hat die zu ergreifenden angemessenen und effektiven Datensicherheitsmaßnahmen zum Schutz der personenbezogenen Daten seiner Kunden je nach Datenverarbeitung und somit stets im Einzelfall festzulegen.[376]

Die Verordnung führt eine nicht abschließende Liste von betreffenden Maßnahmen an, wie zB die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Dienste und Systeme, die Sicherstellung der Verfügbarkeit von Daten und die Überprüfung der Wirksamkeit von technischen und organisatorischen Maßnahmen (Art 32 Abs 1 lit a bis d DSGVO).

Vor der Wahl entsprechender Maßnahmen haben Anbieter eine Risikoanalyse der Datenverarbeitung durchzuführen.[377] Es ist insbesondere zu analysieren, ob eine allfällige Vernichtung,

---

[375] *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Authentifizierung im Bereich Telekommunikation - Risikofelder https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Authentifizierung.html (abgefragt am 3.4.2025).

[376] *Blümel*, Abdingbarkeit technischer und organisatorischer Maßnahmen nach Art 32 DSGVO, Jahrbuch Datenschutzrecht 2022, 105 (106).

Veränderung, Offenlegung, ein Verlust oder unbefugter Zugang von bzw zu Daten zu einem Schaden (sei es ein physischer, materieller oder immaterieller Schaden – wie zB Identitätsmissbrauch) führen könnte.[378]

Auf Basis der Risikohaftigkeit sind Maßnahmen zu implementieren, um ein angemessenes Schutzniveau der verarbeiteten Daten zu erreichen.[379]
Im Ergebnis soll durch das Ergreifen der Maßnahmen das Risiko eines potentiellen Schadens minimiert werden.[380]
Der Anbieter hat den Nachweis der Implementierung und Einhaltung von Datensicherheitsmaßnahmen gemäß Art 32 DSGVO anhand entsprechender Dokumentation zu erbringen.[381] Das Entsprechen der Rechenschaftspflicht ist im Falle eines konkreten Identitätsmissbrauchs und der damit verbundenen möglichen Verhängung von Geldbußen, Haftung oder Leistung von Schadenersatz von Relevanz.[382]

Neben der DSGVO sind hinsichtlich der Verarbeitung personenbezogener Daten oder nicht öffentlich zugänglicher Daten einer juristischen Person die sektorspezifischen Normen nach dem 14. Abschnitt des TKG 2021 (deren Grundlage die ePrivacy-RL[383] bildet) von Anbietern von Kommunikationsdiensten zu beachten. Die §§ 160 bis 174 TKG 2021 gelten als lex specialis zur DSGVO.[384] Seit dem Inkrafttreten des TKG 2021 sind die sonderdatenschutzrechtlichen Bestimmungen nicht nur auf konventionelle Kommunikationsdienste, wie Telefonie- oder SMS-Dienste, sondern auch auf die vielfach genutzten nummernunabhängigen Kommunikationsdienste (somit zB Messenger-Dienste, wie zB WhatsApp und Facebook Messenger) anzuwenden.[385] Der Umstand, dass die Anbieter dieser Kommunikationsdienste nun auch in den Adressatenkreis des 14. Abschnittes des TKG 2021 fallen, ist angesichts der Tatsache, dass laut einer Befragung der RTR-GmbH im Juli 2022 60% aller privaten Gesprächsminuten auf Internet-, Videotelefonie- und Videokonferenzdienste sowie 90% der Nachrichten auf Instant-Messenger

---

377 Siehe dazu ErwG 83 DSGVO, *Tlapak/Klammer*, C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen, in *Anderl* (Hrsg), #Cybercrime Handbuch für die Praxis (2023) 42.
378 Siehe dazu ErwG 83 DSGVO, *Tlapak/Klammer*, C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen, in *Anderl* (Hrsg), #Cybercrime 42.
379 *Tlapak/Klammer*, C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen, in *Anderl* (Hrsg), #Cybercrime 43.
380 *Tlapak/Klammer*, C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen, in *Anderl* (Hrsg), #Cybercrime 43.
381 *Tlapak/Klammer*, C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen, in *Anderl* (Hrsg), #Cybercrime 50.
382 *Tlapak/Klammer*, C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen, in *Anderl* (Hrsg), #Cybercrime 50.
383 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 2002/201, 37.
384 Siehe dazu DSB 30.11.2018, D122.931/0003-DSB/2018; Art 95 DSGVO.
385 *Abazagic*, MR 2022, 343 (344).

oder E-Mail-Dienste entfielen, von Relevanz.[386] Denn die Bestimmungen des TKG verstärken den Schutz der im Rahmen der Telekommunikation verarbeiteten und entstehenden Daten.[387] Mit der Verarbeitung der im 14. Abschnitt des TKG 2021 aufgelisteten Datenarten (Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten) sind spezifische Verpflichtungen, sowohl zu deren Schutz als auch im Falle der Verletzung deren Schutzes, verbunden.[388]

Zu den Stammdaten zählen jene Daten, die für die Begründung, Abwicklung, Änderung oder Beendigung des Vertrages oder Erstellung und Herausgabe von Nutzerverzeichnissen erforderlich sind.[389] Die taxative Liste von Stammdaten beinhaltet den Namen, den akademischen Grad, die Anschrift, die Nutzernummer und sonstige Kontaktinformation für die Nachricht, die Information über Art und Inhalt des Vertragsverhältnisses, die Bonität und das Geburtsdatum.[390]
Unter Verkehrsdaten sind jene *Daten, „die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“*, zu subsumieren.[391] Unter diese Datenkategorie fallen beispielsweise die Rufnummer des anrufenden Nutzers (sogenannte aktive Rufnummer), die Rufnummer des angerufenen Nutzers (passive Rufnummer), der Zeitpunkt und die Dauer eines Gesprächs und die Mobilfunkgeräteerkennung (IMEI).[392] Zur Datenkategorie Standortdaten zählen die geografischen Standorte von Endeinrichtungen von Nutzern und unter Inhaltsdaten sind Inhalte übertragener Nachrichten zu verstehen.[393]

§ 165 TKG 2021 legt die Zweckbindung von Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten fest, dh, dass die genannten Daten „*nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden*“ dürfen. Spezifische und detaillierte Regelungen zu den Verarbeitungszwecken und Löschfristen der einzelnen Datenkategorien sind in § 166 bis § 169 TKG 2021 zu finden.

So ist eine Datenverwendung von Stammdaten nur für den Abschluss, die Durchführung, Änderung oder Beendigung des Vertrags mit dem Kunden, zur Verrechnung von Entgelten, zur Erstellung von Nutzerverzeichnissen und zur Erteilung von Auskünften an Betreiber von Notdiensten gestattet. Die betreffenden Daten sind grundsätzlich nach Vertragsende zu löschen. Ausgenommen davon ist eine darüberhinausgehende Aufbewahrung zu Zwecken der Verrechnung,

386 *Rundfunk und Telekom Regulierungs-GmbH*, Nutzung von Kommunikationsdiensten im Internet (2022) 6.
387 *Vouk*, Exkurs: C.9. Telekommunikationsrechtliche Vorgaben, in *Anderl* (Hrsg), #Cybercrime Handbuch für die Praxis (2023) 105.
388 *Vouk*, C.9. Exkurs: Telekommunikationsrechtliche Vorgaben, in *Anderl* (Hrsg), #Cybercrime 105.
389 § 160 Abs 3 Z 5 TKG 2021.
390 § 160 Abs 3 Z 5 TKG 2021, *Forgó* in *Steinmaurer,* TKG 2021 § 160 Rz 19 (Stand 1.9.2024, rdb.at).
391 § 160 Abs 3 Z 6 TKG 2021.
392 *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 99 TKG 2003 Rz 5.
393 § 160 Abs 3 Z 8 und Z 9 TKG 2021.

der Bearbeitung von Beschwerden oder zur Erfüllung anderweitiger gesetzlicher Verpflichtungen, wie zB zur Erfüllung der unternehmensrechtlichen bzw steuerrechtlichen Aufbewahrungspflicht nach § 212 Unternehmensgesetzbuch (UGB) und § 132 Bundesabgabenordnung (BAO), zulässig.[394]

Verkehrsdaten dürfen nur zu den im Gesetz geregelten Zwecken (wie zB zur Verrechnung und zur Beauskunftung an zuständige Behörden) verarbeitet werden.[395] Sie sind grundsätzlich nach Beendigung der Verbindung bzw, sofern sie für Verrechnungszwecke erforderlich sind, nach Abschluss des Bezahlungsvorgangs zu löschen bzw zu anonymisieren.[396]

Darüber hinaus regelt § 169 TKG 2021 die Datenverarbeitungszwecke und Löschfristen für Standortdaten, die nicht zugleich Verkehrsdaten sind. Zu den Verkehrsdaten zählen jene Standortdaten, die zur Übertragung einer Nachricht im Kommunikationsnetz oder zur Fakturierung erforderlich sind.[397] Auf sie sind die Regelungen des § 167 TKG 2021 anzuwenden.[398] Dagegen zählen zu den Standortdaten, die nicht zugleich Verkehrsdaten sind, präzisere Daten über den Aufenthaltsort eines Kunden.[399] Diese dürfen nur dann verarbeitet werden, wenn sie anonymisiert wurden oder der Kunde seine Einwilligung dazu im Zusammenhang mit der Inanspruchnahme von Diensten mit Zusatznutzen erteilt hat.[400] Unter Dienste mit Zusatznutzen fallen unter anderem ortsbezogene Informationen (zB zur nächsten Sehenswürdigkeit) oder Wetterdienste.[401]

Betreffend Inhaltsdaten normiert § 168 TKG 2021, dass diese nur soweit dies gesetzlich im TKG 2021 vorgesehen ist und die Speicherung einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt, aufbewahrt werden dürfen. Da beispielsweise Mobilboxnachrichten oder SMS-Nachrichten einen wesentlichen Bestandteil eines Kommunikationsdienstes ausmachen, ist eine solche Speicherung gestattet.[402]

Die Verarbeitung von Inhaltsdaten, Verkehrsdaten und Standortdaten tangiert die Privatsphäre des jeweiligen Nutzers, weswegen Anbieter hinsichtlich der genannten Daten zur Wahrung des Kommunikationsgeheimnisses verpflichtet sind (§ 161 TKG 2021). Die Daten sind von den An-

---

394 Siehe zum betreffenden Absatz insgesamt § 166 TKG 2021; *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 97 TKG 2003 Rz 18.
395 § 167 TKG 2021.
396 § 167 TKG 2021.
397 *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG § 99 TKG 2003 Rz 6.
398 *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG § 99 TKG 2003 Rz 6.
399 *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG § 99 TKG 2003 Rz 6.
400 *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 102 TKG 2003 Rz 8.
401 *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG § 102 TKG 2003 Rz 8.
402 *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 101 TKG 2003 Rz 7.

bietern demnach stets geheim zu halten. Ein Verstoß gegen den Schutz der Vertraulichkeit wird strafrechtlich sanktioniert.[403]

Als Ergänzung zu Art 32 DSGVO normiert § 163 TKG 2021 die Verpflichtung zur Ergreifung von Sicherheitsmaßnahmen bei der Erbringung von Kommunikationsdiensten. Durch die Implementierung entsprechender Maßnahmen soll der Schutz der verarbeiteten Daten „*vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe*“ sichergestellt werden.[404] Ferner soll dafür gesorgt werden, dass nur berechtigte Personen für zulässige Zwecke Zugang zu den personenbezogenen Daten erhalten.[405] Für die Verarbeitung der personenbezogenen Daten hat der Anbieter ein Sicherheitskonzept umzusetzen.[406]
Die genannten Regelungen entsprechen weitgehendst dem Zweck der gemäß der DSGVO zu ergreifenden Datensicherheitsmaßnahmen.

Im Zusammenhang mit dem Ergreifen von Sicherheitsmaßnahmen nach dem TKG 2021 ist auf die Besonderheit des § 163 Abs 2 TKG 2021 hinzuweisen, der für die Prävention von Identitätsmissbrauch maßgeblich ist. Denn nach dieser Bestimmung sind Kunden über Fälle, in denen ein besonderes Risiko der Verletzung der Vertraulichkeit besteht und gegebenenfalls über mögliche Abhilfen zu informieren.

Sofern tatsächlich eine Verletzung des Schutzes personenbezogener Daten, etwa durch Offenlegung von Daten zur Identifizierung einer Person (wie Ausweisdaten) stattgefunden hat, sind Anbieter verpflichtet, eine entsprechende Meldung an die Datenschutzbehörde vorzunehmen.[407] Darüber hinaus sind die von der Sicherheitsverletzung betroffenen Personen zu benachrichtigen, wenn anzunehmen ist, dass sie in ihrer Privatsphäre beeinträchtigt werden und nicht durch das Ergreifen von technischen Schutzmaßnahmen (zB durch Verschlüsselung) sichergestellt werden kann, dass die offengelegten Daten für unbefugte Personen unzugänglich sind.[408]

---

403 § 187 Abs 1 TKG 2021.
404 § 163 Abs 3 Z 2 TKG 2021.
405 § 163 Abs 3 Z 1 TKG 2021.
406 § 163 Abs 3 Z 3 TKG 2021.
407 Art 33 DSGVO, § 164 Abs 1 TKG 2021.
408 Art 34 DSGVO, § 164 Abs 1 und Abs 2 TKG 2021; *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 96 Rz 25.

8.2. Rechtsprechung

8.2.1. Einvernehmliches Abgehen von Datensicherheitsmaßnahmen zwischen Datenverantwortlichen und Betroffenen

Wie zuvor erörtert, listet die DSGVO Beispiele an Maßnahmen zur Datensicherheit auf. Der Kommunikationsdiensteanbieter hat nach seinem Ermessen die für den jeweiligen Einzelfall geeigneten technischen und organisatorischen Maßnahmen auszuwählen und umzusetzen.[409]
In diesem Zusammenhang stellt sich die Frage, ob durch Vereinbarung mit der von der Datenverarbeitung betroffenen Person von den getroffenen Maßnahmen zu Lasten der Datensicherheit abgewichen werden kann.

Hinsichtlich dessen hat die DSB (DSB 16.11.2018, D213.692/0001-DSB/2018) entschieden, dass es Unternehmen nicht gestattet ist, mit ihren Kunden zu vereinbaren, dass die ergriffenen technischen und organisatorischen Maßnahmen nach Art 32 DSGVO zu deren Nachteil abgeändert werden dürfen. Das Ergreifen von Datensicherheitsmaßnahmen liegt nämlich in der Verantwortung des jeweiligen Anbieters. Eine Einwilligung von betroffenen Personen kann nur eine Rechtsgrundlage für eine Datenverarbeitung schaffen. Da im gegenständlichen Fall aber keine Rechtsgrundlage für eine Datenverarbeitung geschaffen werden soll, sondern das Abweichen von Datensicherheitsmaßnahmen legitimiert werden soll, ist das Einholen einer Einwilligung für letzteren Fall unzulässig.[410]

Weiters erging zu der Frage der Möglichkeit des Abgehens von Datensicherheitsmaßnahmen eine Entscheidung des OGH (OGH 23.10.2018, 4 Ob 179/18 d). Gegenstand des Verfahrens war unter anderem eine AGB-Klausel einer Online-Plattform zur Partnervermittlung, wonach diese „*für die unbefugte Kenntniserlangung Dritter von persönlichen Daten von Kunden*“ zB im Rahmen eines Hackerangriffs, auch im Falle von grob fahrlässigem oder vorsätzlichem Handeln, ihrerseits nicht haften würde.[411] In seiner Entscheidung hielt der OGH fest, dass der Datenverantwortliche sowie der Auftragsverarbeiter verpflichtet sind, angemessene Datensicherheitsmaßnahmen umzusetzen, damit unbefugten Dritten kein Zugang zu personenbezogenen Daten gewährt wird.[412] Das Ergreifen dieser Maßnahmen stellt auch eine vertragliche Nebenpflicht dar.[413] Der Haftungsausschluss stellt, da er sich auch auf grob fahrlässiges und vorsätzli-

---

[409] *Blümel*, Jahrbuch Datenschutzrecht 2022, 105 (106).
[410] Siehe zum betreffenden Absatz insgesamt DSB 16.11.2018, D213.692/0001-DSB/2018; *Blümel*, Jahrbuch Datenschutzrecht 2022, 105 (116).
[411] OGH 23.10.2018, 4 Ob 179/18 d.
[412] OGH 23.10.2018, 4 Ob 179/18 d.
[413] OGH 23.10.2018, 4 Ob 179/18 d.

ches Handeln der Online-Plattform bezieht, laut Entscheidung des OGH einen Verstoß gegen § 6 Abs 1 Z 9 KSchG dar.[414]

Diese Rechtsprechungslinie entspricht auch dem Zweck des Grundrechts auf Datenschutz und dem durch die Einführung der DSGVO beabsichtigten umfassenden Schutz der Verarbeitung von Daten.[415]

8.2.2. (Un)zureichende Datensicherheitsmaßnahmen zur Verhinderung von Datenmissbrauch

Da Art 32 DSGVO bzw § 163 TKG 2021 keine taxative Liste an konkreten Sicherheitsmaßnahmen zur Verhinderung von Datenmissbrauch anführt, obliegt es dem jeweiligen Anbieter entsprechende Maßnahmen auszuwählen und zu implementieren.

Im Folgenden werden einzelne Fälle erörtert, in denen unzureichende Maßnahmen gesetzt wurden, deren Folge die Verletzung des Schutzes personenbezogener Daten war.
So erging unter anderem eine Entscheidung der DSB (DSB 9.10.2019, D 130.073/0008-DSB/2019) zum Nichtergreifen eines „Double-Opt-In-Verfahrens". Gegenstand des Verfahrens war, dass die E-Mail-Adresse eines Minderjährigen unberechtigterweise von einem Dritten zur Erstellung von Onlinedating-Profilen herangezogen wurde.[416] In der Folge erhielt der Minderjährige unerwünschte E-Mails.[417] Dieses Szenario war möglich, da die im Rahmen der Registrierung des Onlinedating-Profils angeführte E-Mail-Adresse nicht bestätigt werden musste.[418] Somit war kein Double-Opt-In-Verfahren implementiert, weswegen keine hinreichenden Datensicherheitsmaßnahmen im Einsatz waren.[419] Die DSB stellte in der genannten Vorgehensweise einen Verstoß gegen das Recht auf Geheimhaltung personenbezogener Daten nach § 1 Abs 1 DSG fest.[420]
Aus der genannten Entscheidung folgt, dass das Implementieren eines Double-Opt-In-Verfahrens eine geeignete Datensicherheitsmaßnahme zur Einholung einer Einwilligung darstellen kann. Im Rahmen dessen ist jedoch der schmale Grat zwischen der Implementierung des Double-Opt-In-Verfahrens als geeignete Datensicherheitsmaßnahme und dem Versenden des Bestätigungslinks als E-Mail im Rahmen des Double-Opt-In-Verfahrens, das im Falle einer

414 *Blümel*, Jahrbuch Datenschutzrecht 2022, 105 (116).
415 Siehe dazu die Meinung von *Knotzer* in *Blümel*, Jahrbuch Datenschutzrecht 2022, 105 (113).
416 DSB 9.10.2019, D 130.073/0008-DSB/2019.
417 DSB 9.10.2019, D 130.073/0008-DSB/2019.
418 DSB 9.10.2019, D 130.073/0008-DSB/2019.
419 DSB 9.10.2019, D 130.073/0008-DSB/2019.
420 DSB 9.10.2019, D 130.073/0008-DSB/2019.

nicht neutralen Ausgestaltung als unzulässige Direktwerbung gewertet werden kann, zu beachten.[421]

Ferner spielt das Double-Opt-In-Verfahren sowohl bei der Registrierung als auch bei der Nutzung von Messengerdiensten, wie WhatsApp, eine entscheidende Rolle. Bei WhatsApp wird dem Rufnummerninhaber beispielsweise im Rahmen der Registrierung ein Code per SMS bzw per Anruf auf seine Rufnummer zugesendet, mit dessen Eingabe beim Messengerdienst die Verifizierung erfolgt.[422] Weiters besteht optional die Möglichkeit, eine Verifizierung auch während der Nutzung des Dienstes zu aktivieren.[423] In diesem Fall wird ein vom Rufnummerninhaber selbst gewählter Code regelmäßig abgefragt, damit auf den Messengerservice weiterhin zugegriffen werden kann.[424]
Eine solche, lediglich optionale Methode, stellt mE keine ausreichende Datensicherheitsmaßnahme iSd Art 32 DSGVO bzw § 163 TKG 2021 dar. Es ist diesfalls die Entscheidung des Nutzers des Dienstes, ob weitreichendere Maßnahmen zum Schutz seiner Daten gesetzt werden oder nicht. Doch wie zuvor beschrieben, obliegt es dem Anbieter des Messengerdienstes für alle ihre Nutzer taugliche Maßnahmen zur Verhinderung von Datenmissbrauch zu setzen. Durch eine obligatorische regelmäßige Verifizierung der Rufnummer könnte größtenteils gewährleistet werden, dass ausschließlich die Person, der die Rufnummer zugeteilt ist, die betreffende Rufnummer für die Inanspruchnahme von Messengerdiensten nutzen kann. Dadurch könnte Identitätsmissbrauch im Rahmen des Versendens betrügerischer Nachrichten hintangehalten werden.

Zum Ergreifen von Sicherheitsmaßnahmen im Telekommunikationsbereich erging im Jahr 2020 in Deutschland eine Entscheidung des Landesgerichts Bonn (LG Bonn 11.11.2020, OWi 1/20). In diesem Fall wurde die Authentifizierung von Anrufern im Kunden-Call-Center eines deutschen Telekommunikationsanbieters analysiert. Die Mitarbeiter des Call-Centers wurden dazu angewiesen, jeweils den Namen sowie das Geburtsdatum des Anrufers zu erfragen. Im Falle einer positiven Authentifizierung anhand dieser Merkmale, erteilten die Call-Center-Mitarbeiter dem Anrufer Auskünfte oder wurden Änderungen bezüglich der Daten oder Kundenbeziehung vorgenommen. Dadurch war es all Jenen, denen die Merkmale einer Person bekannt waren, möglich, Auskünfte über die im Zusammenhang mit dem Mobilfunkvertrag verarbeiteten Daten

---

[421] Siehe zum betreffenden Absatz insgesamt *Anderl/Ciarnau*, Mehr Datenschutz gegen anzügliche E-Mails Pflicht, Die Presse 2020/09/04, DSB 9.10.2019, DSB-D130.073/0008-DSB/2019 (24.2.2020); VwGH 26.6.2013, 2012/03/0089.

[422] Siehe dazu *WhatsApp Ireland Limited*, Informationen zur Registrierung und Verifizierung in zwei Schritten https://faq.whatsapp.com/506595211487528/?helpref=hc_fnav (abgefragt am 3.4.2025).

[423] Siehe dazu *WhatsApp Ireland Limited*, Informationen zur Verifizierung in zwei Schritten https://faq.whatsapp.com/1278661612895630?helpref=faq_content (abgefragt am 3.4.2025).

[424] Siehe dazu *WhatsApp Ireland Limited*, Informationen zur Verifizierung in zwei Schritten https://faq.whatsapp.com/1278661612895630?helpref=faq_content (abgefragt am 3.4.2025).

einzuholen. So erhielt im gegenständlichen Fall die ehemalige Lebensgefährtin eines Kunden Auskunft über die neue Telefonnummer ihres Ex-Partners, woraufhin sie belästigende Anrufe tätigte. In seiner Entscheidung führte das Landesgericht Bonn aus, dass die Authentifizierungsmaßnahmen keinen hinreichenden Schutz der Daten vor Herausgabe an unberechtigte Dritte geboten haben, weswegen ein Verstoß gegen Art 32 DSGVO vorlag. Dieser Verstoß wurde mit einer Geldbuße von EUR 900.000, -- geahndet. In diesem Fall hätten nämlich weitere, nur dem tatsächlichen Kunden bekannte Informationen seitens des Call-Centers vor Herausgabe der Daten abgefragt werden müssen.[425]

Welche folgenreichen Auswirkungen unzureichende Sicherheitsstandards bzw Authentifizierungsmaßnahmen haben, zeigt unter anderem auch eine Entscheidung der spanischen Datenschutzbehörde.[426] In gegenständlichem Fall gab sich ein Anrufer gegenüber einem spanischen Telekommunikationsanbieter als vermeintlicher Inhaber einer Rufnummer aus und stellte einen Antrag auf Duplikation einer SIM-Karte, woraufhin das Duplikat ausgestellt wurde. Dadurch wurde die Identität des eigentlichen SIM-Inhabers für schädliche Banktransaktionen missbraucht. In ihrer Entscheidung führte die spanische Datenschutzbehörde aus, dass der Telekommunikationsanbieter keine ausreichenden Sicherheitsmaßnahmen gesetzt habe. Es wurden zwar vor SIM-Duplizierung einzelne personenbezogene Daten abgefragt, jedoch wurde das originale Ausweisdokument der betreffenden Person nicht abgefragt. Da ein Dritter somit ohne Rechtsgrundlage Zugang zu personenbezogenen Daten erhielt, wurde gegenüber dem spanischen Telekommunikationsanbieter eine Geldstrafe in der Höhe von EUR 70.000, -- verhängt.[427]

Die angeführten Entscheidungen zeigen, dass es zur Verhinderung von Identitätsmissbrauch stets erforderlich ist, angemessene technische und organisatorische Datensicherheitsmaßnahmen zu setzen.

8.3. Geldbußen, Haftung und Schadenersatz

Folgend soll erörtert werden, welche Sanktionen das Nichtbefolgen der zuvor beschriebenen datenschutzrechtlichen Bestimmungen nach sich zieht.

---

[425] Siehe zum betreffenden Absatz insgesamt *Axel von Walter*, LG Bonn reduziert Bußgeld gegen 1&1 deutlich und ebnet Weg für EU-Verbandssanktion im Datenschutz, DSB 2021, 56; LG Bonn 11.11.2020, OWi 1/20.

[426] *NOYB – European Center for Digital Rights*, AEPD (Spain) - EXP202105333 https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS-00505-2022 (Stand 13.12.2023).

[427] Siehe zum betreffenden Absatz insgesamt *NOYB – European Center for Digital Rights*, AEPD (Spain) - EXP202105333 https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS-00505-2022 (Stand 13.12.2023).

Im Falle einer Verletzung des Schutzes von Identitätsdaten kann es zur Auferlegung von Maßnahmen seitens der DSB, zur Zahlung von Geldbußen und/oder zur Leistung von Schadenersatz gegenüber Betroffenen kommen.[428]

Zu den Abhilfebefugnissen der DSB zählen beispielsweise die Verwarnung bei Verstößen mittels Bescheids, die Anweisung, wie bestimmte Verarbeitungsvorgänge auszuführen sind, sowie die Verhängung einer vorübergehenden oder endgültigen Beschränkung einer Verarbeitung, einschließlich eines Verbots.[429]

Zusätzlich zu oder anstatt der angeführten Maßnahmen kann die DSB auch eine Geldbuße verhängen.[430] So kann die DSB eine Geldbuße gegen Anbieter von Kommunikationsdiensten verhängen, wenn diese gegen das Recht auf Geheimhaltung und gegen Bestimmungen der DSGVO verstoßen haben.[431] Bei einem Verstoß gegen Art 32 DSGVO kann eine Geldbuße von bis zu 10 Millionen Euro oder von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs des betreffenden Unternehmens verhängt werden, je nachdem, welcher der Beträge höher ist.[432] Sofern die Grundsätze für die Verarbeitung gemäß Art 6 DSGVO nicht eingehalten wurden, ist sogar eine Verhängung einer Geldbuße in Höhe von bis zu 20 Millionen Euro oder von bis zu 4 % des gesamten von einem Unternehmen weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs möglich.[433] Die Verhängung der Geldbuße sowie deren Höhe erfolgt nach den Umständen des Einzelfalls.[434] Dabei sind unter anderem die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung des Ausmaßes des von der betroffenen Person erlittenen Schadens, die vom Verstoß betroffenen Datenkategorien sowie die Schwere des Verschuldens zu berücksichtigen.[435]

Im Falle eines Identitätsmissbrauchs hat die davon betroffene Person ferner einen Anspruch auf Schadenersatz gegen den Anbieter – insbesondere, sofern dieser gegen das Recht auf Geheimhaltung oder gegen die Bestimmungen der DSGVO verstoßen hat und der betroffenen Person daraus ein materieller oder immaterieller Schaden entstanden ist.[436] Hintergrund des immateriellen Schadenersatzes ist eine Ausgleichsfunktion für den durch den DSGVO-Verstoß

---

428 Art 58 DSGVO, Art 82 DSGVO, Art 83 DSGVO.
429 Art 58 Abs 2 DSGVO, siehe dazu genauer *Zavadil* in *Knyrim*, DatKomm Art 58 DSGVO (Stand 1.7.2024, rdb.at).
430 Art 83 Abs 2 DSGVO.
431 § 30 Abs 1 DSG iVm § 1 Abs 1 DSG.
432 Art 83 Abs 4 lit a DSGVO.
433 Art 83 Abs 5 lit a DSGVO.
434 Art 83 Abs 2 DSGVO.
435 Die gesamte Liste an Kriterien ist in Art 83 Abs 2 DSGVO angeführt.
436 § 29 Abs 1 DSG, Art 82 DSGVO.

erlittenen Schaden – er hat keine Straffunktion.[437] Zum Anspruch auf Ersatz eines immateriellen Schadens bei Identitätsmissbrauch ist ferner festzuhalten, dass ein solcher nur dann in Frage kommt, wenn jemand nach einem Datendiebstahl die Identität der Person annimmt, die vom Datendiebstahl betroffen war.[438] Der Identitätsmissbrauch muss jedoch nicht nachgewiesen werden.[439] Vielmehr ist der Schadenersatzanspruch gemäß § 29 Abs 1 DSG nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu beurteilen.[440] Somit hat ein Schaden vorzuliegen und die Handlung oder Unterlassung des Kommunikationsdiensteanbieters hat kausal für den Schaden sein.[441] Darüber hinaus müssen Rechtswidrigkeit (zB ein Verstoß gegen die DSGVO bzw gegen eine vertragliche Hauptleistungs- oder Nebenleistungspflicht[442]) sowie Verschulden des Anbieters vorliegen.[443]

8.4. Ergebnis

Angesichts der in den vorherigen Kapiteln aufgezeigten Folgen von Identitätsmissbrauch scheint es evident, wie essenziell es ist, dass Anbieter den zuvor skizzierten datensicherheitsrechtlichen Normen entsprechen. Denn vor allem durch das Ergreifen von für den Einzelfall hinreichenden Datensicherheitsmaßnahmen als auch durch das Einhalten des Zweckbindungsgrundsatzes und der Löschungsverpflichtungen kann ein wesentlicher Beitrag zur Prävention von Identitätsmissbrauch geleistet werden.

---

[437] *Thiele*, EuGH: Immaterieller Schadenersatz bei Datendiebstahl? jusIT 2024/111; EuGH C-182/22, C-189/22, *Scalable Capital*, ECLI:EU:C:2024:531 Rn 24.
[438] *Thiele*, jusIT 2024/111 (156, 157); EuGH C-182/22, C-189/22, *Scalable Capital*, ECLI:EU:C:2024:531 Rn 58.
[439] *Thiele*, jusIT 2024/111 (156, 157); EuGH C-182/22, C-189/22, *Scalable Capital*, ECLI:EU:C:2024:531 Rn 58.
[440] *Anderl/Tlapak*, H.3. Ansprüche Betroffener, in *Anderl* (Hrsg), #Cybercrime Handbuch für die Praxis (2023) 285.
[441] *Anderl/Tlapak*, H.3. Ansprüche Betroffener, in *Anderl* (Hrsg), #Cybercrime 285.
[442] Siehe dazu *Blümel*, Jahrbuch Datenschutzrecht 2022, 105 (111), wonach die Einhaltung von IT-Sicherheitspflichten als Hauptleistungs- und Nebenleistungspflicht geschuldet sein kann.
[443] *Anderl/Tlapak*, H.3. Ansprüche Betroffener, in *Anderl* (Hrsg), #Cybercrime 285.

9. Zusammenfassung

Unter Identitätsmissbrauch ist das unbefugte Sichverschaffen fremder Identitätsdaten und der Gebrauch dieser Identitätsdaten zu verstehen.[444] Um die Bevölkerung vor Identitätsmissbrauch sowie davor zu schützen, Opfer von Straftaten durch das fälschliche Vertrauen in ihr Gegenüber, das unbefugt eine fremde Identität angenommen hat, zu werden, bedarf es einer Kombination aus präventiven Maßnahmen und geeigneten Maßnahmen zur Strafverfolgung. Dementsprechend handelt es sich beim Identitätsmissbrauch um eine Querschnittsmaterie, da für dessen Bekämpfung insbesondere einige strafrechtliche, telekommunikationsrechtliche und datensicherheitsrechtliche Bestimmungen von Relevanz sind.

Als Ergebnis der gegenständlichen Arbeit ist festzuhalten, dass die in den einzelnen Kapiteln genannten Rechtsgebiete durchaus bereits einen erheblichen Beitrag zur Verhinderung bzw Bekämpfung von Identitätsmissbrauch im Rahmen der Nutzung von Kommunikationsdiensten leisten.

Zunächst leisten die verschiedenen einschlägigen Straftatbestände (§ 225a StGB, § 146 StGB und § 147 Abs 1 Z 1 StGB, § 111 StGB, § 33 Abs 1 Z 8 StGB und § 63 DSG) sowie die bereits bestehenden Ermittlungsbefugnisse der Behörden einerseits einen Beitrag zur Prävention von Identitätsmissbrauch als auch andererseits einen erheblichen Beitrag zur Aufklärung und wirksamen Strafverfolgung von Identitätsmissbrauch.
Hinsichtlich der für den Identitätsmissbrauch einschlägigen Straftatbestände ist insbesondere auf § 225a StGB und §§ 146 StGB iVm § 147 Abs 1 Z 1 StGB hinzuweisen. So wird bspw beim Phänomen Spoofing der Straftatbestand der Datenfälschung gemäß § 225a StGB erfüllt. Bei den versendeten betrügerischen Nachrichten im Zusammenhang mit dem Polizisten-Trick, CEO-Fraud und Tochter-Sohn-Trick kommt dagegen der schwere Betrug gemäß § 146 iVm § 147 Abs 1 Z 1 StGB zur Anwendung.
Zudem sieht die StPO – zB mit der Nachrichtenüberwachung, der Sicherstellung von Daten oder dem Ersuchen um Auskunft zu Stammdaten – bereits essenzielle Ermittlungsmaßnahmen zur Ausforschung der Täterschaft vor. Weiters darf durch das Inkrafttreten der E-Evidence VO eine effektivere Strafverfolgung von Kriminalitätsformen mit Auslandsbezug erwartet werden.

[444] Siehe zur Definition von Identitätsmissbrauch zB *Reindl-Krauskopf*, ÖJZ 2015/19, 112 (114); *Riffel* in *Höpfel/Ratz*, WK² StGB § 33 Rz 26.

Neben den wirksamen strafrechtlichen bzw strafprozessualen Aspekten leisten die bereits seit einigen Jahren für Anbieter von Kommunikationsdiensten bestehenden sektorspezifischen datenschutzrechtlichen Regelungen sowie das strenge Regime der DSGVO hinsichtlich des Ergreifens von Datensicherheitsmaßnahmen einen erheblichen Beitrag zur Verhinderung bzw Bekämpfung von Identitätsmissbrauch.
Nicht zu übersehen sind darüber hinaus die telekommunikationsrechtlichen Beiträge. So wurden beispielsweise durch die Einführung von Anti-Spoofing Maßnahmen im Telekommunikationsrecht in jüngster Vergangenheit erste Schritte zur Bekämpfung des vorherrschenden Phänomens Spoofing gesetzt.[445]

Im Lichte dessen darf allerdings nicht übersehen werden, dass sich die Formen von Identitätsmissbrauch stetig weiterentwickeln und verändern. Dem dynamischen Umfeld hat auch die Rechtsordnung Stand zu halten. Insofern ist der Gesetzgeber angehalten, die Veränderungen stets im Blick zu behalten, um schnellstmöglich entsprechende Anpassungen der rechtlichen Bestimmungen vornehmen zu können.

[445] Siehe dazu § 5a KEM-V 2009.

10. Abstract

In den vergangenen Jahren sind die Fälle von Identitätsmissbrauch im Rahmen der Telekommunikation gestiegen. Unter „Identitätsmissbrauch“ ist das unbefugte Sichverschaffen fremder, einer einzelnen Person zuordenbarer, Daten (sogenannter Identitätsdaten) und die Verwendung dieser Daten zu verstehen. Die Formen von Identitätsmissbrauch im Zusammenhang mit der Nutzung von Kommunikationsdiensten sind vielfältig und entwickeln sich stets weiter. Als Phänomene können das Fälschen von Rufnummern (Spoofing) (mit dem diverse Formen von betrügerischen Anrufen/Nachrichten einhergehen), das Phishing oder SIM-Swapping genannt werden. Die gegenständliche Arbeit befasst sich unter anderem mit den strafrechtlichen Aspekten von Identitätsmissbrauch, folglich mit der Datenfälschung gemäß § 225a StGB, dem Betrug gemäß § 146 StGB und dem schweren Betrug gemäß § 147 Abs 1 Z 1 StGB, der üblen Nachrede gemäß § 111 StGB, dem besonderen Erschwerungsgrund gemäß § 33 Abs 1 Z 8 StGB sowie der Datenverarbeitung in Gewinn- oder Schädigungsabsicht gemäß § 63 DSG. Daneben werden die Ermittlungsbefugnisse der Behörden, um die Täterschaft ausfindig machen zu können (wie Auskunftsersuchen betreffend Stammdaten zu einer Rufnummer oder die Sicherstellung bzw Beschlagnahme von Datenträgern und Daten), im nationalen und europäischen Kontext dargelegt. Weiters wurden im Telekommunikationsrecht bereits einige Normen eingeführt, um Identitätsmissbrauch hintanzuhalten (zB die Identifizierungs- und Registrierungsverpflichtung gemäß § 166 Abs 2 TKG 2021 sowie Maßnahmen gegen Nummernmissbrauch gemäß § 121 TKG 2021 und § 5a KEM-V 2009). Auch das Datenschutzrecht sieht spezielle Regelungen für Anbieter von Kommunikationsdiensten vor, die Letztere verpflichten, entsprechende Datensicherheitsmaßnahmen zu setzen, um Personen vor Identitätsmissbrauch zu schützen. Jene Rechtsnormen, die die Datensicherheit betreffen, werden anhand einschlägiger Rechtsprechung beleuchtet.

Im Rahmen vorliegender Arbeit wird analysiert, ob durch die genannten Rechtsgebiete tatsächlich bereits ein wirksamer Schutz gegen Identitätsmissbrauch besteht.

11. Quellenverzeichnis

11.1. Literatur

Abazagic, Handbuch Telekomrecht: Regelungen des TKG 2021 für das Massengeschäft und EU-Vorgaben für Netzneutralität und Roaming (2025).

Abazagic, WhatsApp, Facebook Messenger & Co im TKG 2021: Zur Regulierung nummernunabhängiger interpersoneller Kommunikationsdienste, MR 2022, 343.

Akinlade, Grundlagen der Informatik und IT-Security – Security als Managementfunktion, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021).

Anderl/Ciarnau, Mehr Datenschutz gegen anzügliche E-Mails Pflicht, Die Presse 2020/09/04, DSB 9.10.2019, DSB-D130.073/0008-DSB/2019 (24.2.2020).

Anderl/Tlapak, H.3. Ansprüche Betroffener, in *Anderl* (Hrsg), #Cybercrime Handbuch für die Praxis (2023).

Axel von Walter, LG Bonn reduziert Bußgeld gegen 1&1 deutlich und ebnet Weg für EU-Verbandssanktion im Datenschutz, DSB 2021, 56 zu LG Bonn 11.11.2020, OWi 1/20.

Bartz, Identitätsdiebstahl: Zur Frage der Strafbarkeit des Identitätsdiebstahls und der Notwendigkeit eines eigenen Straftatbestands im deutschen Recht (2017).

Bergauer, Computerstrafrecht in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht: Profiwissen für die Praxis^2 (2022).

Bergauer, Das materielle Computerstrafrecht (2016).

Bergauer in *Jahnel* (Hrsg), Kommentar zur Datenschutz-Grundverordnung (2021).

Birklbauer/Stiebellehner in *Hinterhofer*, StGB: Salzburger Kommentar zum StGB § 33 StGB (45. Lfg, Stand Juli 2023, lexisnexis.at).

Blümel, Abdingbarkeit technischer und organisatorischer Maßnahmen nach Art 32 DSGVO, Jahrbuch Datenschutzrecht 2022, 105 (106).

Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche Aspekte und technische Aspekte (2011).

Büchel/Hirsch, Internetkriminalität: Phänomene – Ermittlungshilfen – Prävention[2] (2020).

Bundesministerium für Inneres/Bundeskriminalamt, Cybercrime Report 2021: Lagebericht über die Entwicklung von Cybercrime (2022).

Bundesministerium für Inneres/Bundeskriminalamt, Cybercrime Report 2023: Lagebericht über die Entwicklung von Cybercrime (2024).

Feiel, Das Telekommunikationsgesetz 2021 – ein Überblick, MR 2021, 310.

Forgó in *Steinmaurer,* TKG 2021 § 160 (Stand 1.9.2024, rdb.at).

Forgó in *Steinmaurer,* TKG 2021 § 166 (Stand 1.9.2024, rdb.at).

Ghazanfari, Bekanntgabe des PUK-Codes und Duplizierung einer SIM-Karte – Sicherstellung? JBl 2021, 740.

GSMA, Access to Mobile Services and Proof of Identity 2021 (2021).

GSMA, Mandatory registration of prepaid SIM cards: Addressing challenges through best practice (2016).

Herrnfeld, Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel, ZWF 2022, 2.

Hinterhofer, Spezialfragen des Betrugs in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht: Profiwissen für die Praxis[2] (2022).

Illibauer in *Knyrim,* DatKomm Art 12 DSGVO (Stand 1.7.2024, rdb.at).

Jerabek/Ropper/Reindl-Krauskopf/Schroll/Oberressl in *Höpfel/Ratz*, WK² StGB § 74 (Stand 1.5.2024, rdb.at).

Kienapfel/Schroll in *Höpfel/Ratz*, WK² StGB § 226 (Stand 1.1.2017, rdb.at).

Kilic, Die EU-Verordnung 2023/1543 (Beweismittelsicherungs-VO) vereinfacht den Zugriff auf elektronische Beweismittel im Fokus der Strafverfolgung, RZ 2024, 307.

Kirchbacher/Sadoghi in *Höpfel/Ratz*, WK² StGB § 146 (Stand 30.11.2023, rdb.at).

Kirchbacher/Sadoghi in *Höpfel/Ratz*, WK² StGB § 147 (Stand 30.11.2023, rdb.at).

Kollmann/Moser in *Birklbauer/Haumer/Nimmervoll/Wess*, StPO - Linzer Kommentar zur Strafprozessordnung § 118 (Stand 11.2020, lexisnexis.at).

Lendl in *Fuchs/Ratz,* WK StPO § 76a (Stand 15.3.2023, rdb.at).

Meyer, Identität und virtuelle Identität natürlicher Personen im Internet (2011).

Moser, Evaluierung des Rückgangs der Anfallszahlen bei Gericht, Österreichisches Anwaltsblatt 2019/194, 461.

Österreichisches Institut für angewandte Telekommunikation (ÖIAT), Identitätsdiebstahl: Die Folgen für Betroffene und wie ihnen geholfen werden kann (April 2022).

Rami in *Höpfel/Ratz*, WK² StGB Vor §§ 111–117 (Stand 1.9.2024, rdb.at).

Rami in *Höpfel/Ratz*, WK² StGB § 111 (Stand 1.9.2024, rdb.at).

Reindl-Krauskopf, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112.

Reindl-Krauskopf in *Höpfel/Ratz*, WK² StGB § 225a (Stand 1.1.2017, rdb.at).

Reindl-Krauskopf/Salimi/Stricker, IT-Strafrecht: Cyberdelikte und Ermittlungsbefugnisse (2018).

Reindl-Krauskopf/Tipold/Zerbes in *Fuchs/Ratz,* WK StPO § 134 (Stand 01.03.2021, rdb.at).

Riesz in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 96 TKG 2003.

Riesz in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 97 TKG 2003.

Riesz in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 99 TKG 2003.

Riesz in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 101 TKG 2003.

Riesz in *Riesz/Schilchegger* (Hrsg), TKG: Telekommunikationsgesetz (2016) § 102 TKG 2003.

Riffel in *Höpfel/Ratz*, WK^2 StGB § 32 (Stand 15.8.2023, rdb.at).

Riffel in *Höpfel/Ratz*, WK^2 StGB § 33 (Stand 15.8.2023, rdb.at).

Rundfunk und Telekom Regulierungs-GmbH, JAHRESBERICHT der Schlichtungsstellen 2021 (2022).

Rundfunk und Telekom Regulierungs-GmbH, JAHRESBERICHT der Schlichtungsstellen 2022 (2023).

Rundfunk und Telekom Regulierungs-GmbH, JAHRESBERICHT der Schlichtungsstellen 2023 (2024).

Rundfunk und Telekom Regulierungs-GmbH, RTR NETZ NEUTRALITÄTSBERICHT 2023 (2023).

Rundfunk und Telekom Regulierungs-GmbH, Nutzung von Kommunikationsdiensten im Internet (2022).

Salimi in *Höpfel/Ratz*, WK^2 StGB Vor §§ 62 - 67 (Stand 1.3.2022, rdb.at).

Salimi in *Höpfel/Ratz*, WK^2 DSG § 63 (Stand 30.8.2019, rdb.at).

Salimi in *Höpfel/Ratz*, WK^2 StGB § 67 (Stand 1.3.2022, rdb.at).

Salimi in *Triffterer/Rosbaud/Hinterhofer,* StGB: Salzburger Kommentar zum StGB § 127 (27. Lfg, Stand 11.2012, lexisnexis.at).

Schwaighofer in *Fuchs/Ratz*, WK StPO § 80 (Stand 1.12.2020, rdb.at).

Spittka, Registrierungspflicht für Prepaid-SIM-Karten verstößt nicht gegen EMRK: Zugleich Besprechung von EGMR, Entscheidung vom 30.1.2020 – Nr. 50001/12 – Breyer gegen Deutschland, KuR 2020, 263.

Spornberger, IT-Strafrecht – IT-Strafrecht im Überblick, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021).

Steinmaurer, Telekommunikationsrecht – der Europäische Kodex für die elektronische Kommunikation, in *Zankl* (Hrsg), Rechtshandbuch der Digitalisierung (2021).
Stricker in *Leukauf/Steininger,* StGB: Strafgesetzbuch inklusive Update 2020 § 1
(2020, lindedigital.at).

Teichmann/Falker, CEO-Fraud: Empfehlungen für das Legal Risk Management, GRCaktuell 2021, 48.

Thiele, EuGH: Immaterieller Schadenersatz bei Datendiebstahl? jusIT 2024/111.

Thiele in *Hinterhofer*, Salzburger Kommentar zum StGB § 225a (44. Lfg Stand 3.2023, lexisnexis.at).

Thiele/Wagner, Praxiskommentar zum Datenschutzgesetz (DSG)[2] § 63 (Stand 1.2.2022, rdb.at).

Tipold in *Leukauf/Steininger*, StGB[4] § 225a (Stand 1.10.2016, rdb.at).

Tipold in *Leukauf/Steininger*, Strafrechtliche Nebengesetze[3] § 63 DSG (Stand 1.9.2022, rdb.at).

Tlapak/Klammer, C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen, in *Anderl* (Hrsg), #Cybercrime Handbuch für die Praxis (2023).

Vouk, Exkurs: C.9. Telekommunikationsrechtliche Vorgaben, in *Anderl* (Hrsg), #Cybercrime Handbuch für die Praxis (2023).

Zavadil in *Knyrim*, DatKomm Art 58 DSGVO (Stand 1.7.2024, rdb.at).

11.2. Internetquellen

Anfragebeantwortung durch die Bundesministerin für Justiz Dr. Alma Zadić, LL.M. vom 30.5.2023 zu der schriftlichen Anfrage (14796/J) der Abgeordneten Mag. Christian Drobits, Kolleginnen und Kollegen an die Bundesministerin für Justiz betreffend Identitätsdiebstahl https://www.parlament.gv.at/gegenstand/XXVII/AB/14309.

A-SIT Zentrum für sichere Informationstechnologie – Austria, KI-basierte Cyberangriffe: Aktuelle Trends und Gefahren https://www.onlinesicherheit.gv.at/Services/News/KI-Cyberattacken-Risiken-Trends.html (Stand 14.11.2023).

A-SIT Zentrum für sichere Informationstechnologie – Austria, Audio-Deepfakes und Voice-Cloning: So schützen Sie sich vor Betrug https://www.onlinesicherheit.gv.at/Services/News/Audio-Deepfake-Voice-Cloning.html (Stand 12.10.2023).

Bundesamt für Sicherheit in der Informationstechnik, Botnetze-Auswirkungen und Schutzmaßnahmen https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/botnetze_node.html (abgefragt am 3.4.2025).

Bundesamt für Sicherheit in der Informationstechnik, Social Engineering – der Mensch als Schwachstelle https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html (abgefragt am 3.4.2025).

Bundeskriminalamt, Prävention: Tochter-Sohn-Trick https://www.bundeskriminalamt.at/news.aspx?id=582B3033474E43655243633D (Stand 11.11.2022).

Bundesministerium für Inneres, Anrufkriminalität https://bmi.gv.at/magazin/2022_03_04/Anrufkriminalitaet.aspx (abgefragt am 3.4.2025).

Bundesministerium für Inneres, Bundeskriminalamt: Ermittlungserfolg gegen „falsche Polizisten“ am Telefon https://www.bundeskriminalamt.at/news.aspx?id=63346C2B366B75663968773D (Stand 17.11.2022).

Bundesministerium für Inneres, Bundeskriminalamt: Modernisierung des Kriminaldienstes: Start für Kriminalassistenzdienststellen https://www.bmi.gv.at/news.aspx?id=635763326733366B5261303D (Stand 2.6.2024).

Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, Rufnummernmissbrauch über eSIM-Karten https://www.konsumentenfragen.at/konsumentenfragen/Aktuelles/Konsumentenfragen/Rufnummernmissbrauch-ueber-eSIM-Karten.html (Stand 6.2.2024).

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Manipulation von Rufnummern https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (abgefragt am 3.4.2025).

Datenschutzbehörde, Formulare https://dsb.gv.at/eingabe-an-die-dsb/formulare (Antrag gemäß Art. 15 DSGVO auf Auskunft / Request for Access (Article 15 GDPR), Stand 4.2020).

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Authentifizierung im Bereich Telekommunikation – Risikofelder https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Authentifizierung.html (abgefragt am 3.4.2025).

„Die Presse" Verlags-Gesellschaft m.b.H. & Co KG, SMS-Firewall: Mobilfunker scannen Handynachrichten https://www.diepresse.com/19466282/sms-firewall-mobilfunker-scannen-handynachrichten (Stand 13.3.2025).

epicenter.works, Überwachungspaket https://epicenter.works/thema/ueberwachungspaket (abgefragt am 3.4.2025).

Internet Service Providers Austria, ISPA-STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES MIT DEM DAS SICHERHEITSPOLIZEIGESETZ, DAS BUNDESSTRAßENMAUTGESETZ 2002, DIE STRAßENVERKEHRSORDNUNG 1960 UND DAS TELEKOMMUNIKATIONSGESETZ 2003 GEÄNDERT WERDEN https://www.parlament.gv.at/dokument/XXV/SNME/29465/imfname_666671.pdf (Stand 18.8.2017).

*Nemeth/Müller/*Feiler, Missbrauchspotenzial in neuer EU-Verordnung zu digitalen Beweismitteln https://www.derstandard.de/story/3000000172389/missbrauchspotenzial-in-neuer-eu-verordnung-zu-digitalen-beweismitteln (Stand 5.6.2023).

NOYB – European Center for Digital Rights, AEPD (Spain) - EXP202105333 https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS-00505-2022 (Stand 13.12.2023).

Österreichisches Institut für angewandte Telekommunikation (ÖIAT), Gefälschtes A1-Mail im Umlauf https://www.watchlist-internet.at/news/gefaelschtes-a1-mail-im-umlauf/ (Stand 31.10.2022).

Österreichisches Institut für angewandte Telekommunikation (ÖIAT), Post E-Mail „Dein Paket wartet!“ ist fake! https://www.watchlist-internet.at/news/post-e-mail-dein-paket-wartet-ist-fake/ (Stand 2.2.2022).

Publications Office of the European Union, Elektronische Beweismittel in Strafverfahren – Herausgabeanordnung und Sicherungsanordnung https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM:4649186 (Stand 30.5.2023).

Rundfunk und Telekom Regulierungs-GmbH, Betrugsanrufe vom "Austrian Police Department" schlagen derzeit hohe Wellen: einfach ignorieren und auflegen! https://www.rtr.at/TKP/presse/pressemitteilungen/pressemitteilungen/pinfo26072022tkp.de.html (Stand 26.7.2022).

Rundfunk und Telekom Regulierungs-GmbH, 5G-SIM-Karten setzen sich immer mehr durch: Österreicher:innen upgraden auf neueste Netztechnik https://www.rtr.at/TKP/presse/pressemitteilungen/presseinformationen_2024/pinfo10102024tkp.de.html (Stand 10.10.2024).

Rundfunk und Telekom Regulierungs-GmbH, 117. Mobilregulierungsdialog https://www.rtr.at/TKP/aktuelles/veranstaltungen/veranstaltungen/Mobilregulierungsdialog/117Mobilregulierungsdialog.de.html (117. Regulierungsdialog Maßnahmen Ping-Anrufe durch Betreiber.pdf, Stand 16.4.2021).

Rundfunk und Telekom Regulierungs-GmbH, Manipulation von Rufnummern https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/spam-unerwuenschte_anrufe_und_nachrichten/manipulation_von_telefonnummern.de.html (abgefragt am 3.4.2025).

Rundfunk und Telekom Regulierungs-GmbH, Newsletter RTR.Telekom.Post, RTR plant neue rechtliche Rahmenbedingungen gegen Spoofing https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/Newsletter/telekom_und_post_newsletter_03-2023.de.html (Stand 25.10.2023).

Rundfunk und Telekom Regulierungs-GmbH, Öffentliche Konsultation der RTR zum Budget 2025 https://www.rtr.at/rtr/wer_wir_sind/Organisation/Finanzierung/Budgetkonsultation/Konsultation-der-RTR-zum-Budget-2025.de.html (Budget_2025_Konsultationsdokument.pdf, Stand 12.11.2024).

Rundfunk und Telekom Regulierungs-GmbH, Öffentliche Konsultation der RTR zum Entwurf einer Novelle der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009) https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/konsultationen/konsult9nov_kem-v_2009.de.html (Stand 2.10.2023).

Rundfunk und Telekom Regulierungs-GmbH, Unerwünschte Nachrichten per SMS, Whatsapp & Co https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/spam-unerwuenschte_anrufe_und_nachrichten/unerwuenschte_sms.de.html (abgefragt am 3.4.2025).

Rundfunk und Telekom Regulierungs-GmbH, Scam-Anrufe/Phishing-Anrufe https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/information/informationen_fuer_konsumenten/TKKS_Spam.de.html (abgefragt am 3.4.2025).

Rundfunk und Telekom Regulierungs-GmbH, Tipps bei Phishing SMS https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/tippsgegenspam/tipps_phishing-sms.de.html (abgefragt am 3.4.2025).

Salzburger Nachrichten Medien GmbH & Co. KG, Fast jeder zweite Betrug wird im Internet verübt https://www.sn.at/panorama/oesterreich/fast-jeder-zweite-betrug-wird-im-internet-veruebt-143270104 (Stand 7.8.2023).

Standard Verlagsgesellschaft m.b.H., Eklatant steigende Fallzahlen von „Tochter-Sohn-Betrug" https://www.derstandard.at/story/2000141679885/eklatant-steigende-fallzahlen-von-tochter-sohn-betrug (Stand 10.12.2022).

Statista GmbH, Anteil der Smartphone-Besitzer sowie Nutzung von Mobile Commerce in Österreich von 2013 bis 2023 https://de.statista.com/statistik/daten/studie/568185/umfrage/smartphone-besitz-und-smartphone-nutzung-in-oesterreich/ (abgefragt am 3.4.2025).

Statista GmbH, Wie besorgt sind Sie, dass Sie im Internet Opfer eines Identitätsdiebstahls werden könnten? https://de.statista.com/statistik/daten/studie/542843/umfrage/grad-der-besorgnis-der-eu-buerger-in-bezug-auf-identitaetsdiebstahl-im-internet/#statisticContainer (abgefragt am 3.4.2025).

WhatsApp Ireland Limited, Informationen zur Registrierung und Verifizierung in zwei Schritten https://faq.whatsapp.com/506595211487528/?helpref=hc_fnav (abgefragt am 3.4.2025).

WhatsApp Ireland Limited, Informationen zur Verifizierung in zwei Schritten https://faq.whatsapp.com/1278661612895630?helpref=faq_content (abgefragt am 3.4.2025).

Wiese, Noch 2025 soll in Österreich die SMS-Firewall kommen https://futurezone.at/netzpolitik/sms-firewall-oesterreich-deutschland-spanien-phishing-malware/403021170 (Stand 13.3.2025).

11.3. Judikatur

DSB 22.12.2021, D155.027 2021-0.586.257.
DSB 9.10.2019, D 130.073/0008-DSB/2019.
DSB 30.11.2018, D122.931/0003-DSB/2018.
DSB 16.11.2018, D213.692/0001-DSB/2018.
EGMR 30.1.2020, Bsw 50001/12, *Breyer gg. Deutschland*.
EuGH C-182/22, C-189/22, *Scalable Capital*, ECLI:EU:C:2024:531.
OGH 23.10.2018, 4 Ob 179/18 d.

OLG Wien, 11.7.2019, 23 Bs 172/19s.
RIS-Justiz RS0133582.
VfGH 14.12.2023, G 352/2021 (G352/2021-46).
VfGH 11.12.2019, G72/2019 ua (G72-74/2019-48, G181-182/2019-18).
VwGH 26.6.2013, 2012/03/0089.

11.4. Rechtsquellen

Bundesgesetz, mit dem ein Telekommunikationsgesetz (Telekommunikationsgesetz 2021 – TKG 2021) erlassen wird, BGBl I 2021/190.

Bundesgesetz über allgemeine Bestimmungen und das Verfahren für die von den Abgabenbehörden des Bundes, der Länder und Gemeinden verwalteten Abgaben (Bundesabgabenordnung – BAO), BGBl 1961/194.

Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen (Unternehmensgetzbuch – UGB), BGBl I 2005/120.

Bundesgesetz über die Gleichbehandlung (Gleichbehandlungsgesetz – GlBG), BGBl I 2004/66.

Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), BGBl I 2004/10.

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 2017/120.

Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG), BGBl I 2016/118.

Erläuternde Bemerkungen zur KEM-V 2009, BGBl II Nr 212/2009.

Erläuternde Bemerkungen zur 9. Novelle der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009) nach § 112 TKG 2021.

Erläuterungen zum DSA-Begleitgesetz: ErläutRV 2309 BlgNR 27. GP.

Erläuterungen zum Strafprozessrechtänderungsgesetz 2018: ErläutRV 17 BlgNR 26. GP.

Erläuterungen zum Strafrechtsänderungsgesetz 2015: ErläutRV 689 BlgNR 25. GP.

Erläuterungen zum Telekommunikationsgesetz 2021: ErläutRV 1043 BlgNR 27. GP.

Erläuterungen zur Änderung des Telekommunikationsgesetzes 2003: ErläutRV 15 BlgNR 26. GP.

Initiativantrag zum Strafprozessrechtsänderungsgesetz 2024: IA 15/A 28. GP. https://www.parlament.gv.at/dokument/XXVIII/A/15/imfname_1660740.pdf

Materialen zum E-Government-Gesetz: ErläutRV 252 BlgNR 22. GP.

Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen: „Eine allgemeine Politik zur Bekämpfung der Internetkriminalität“, KOM (2007) 267 endgültig (22.5.2007).

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 2002/201, 37.

Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl L 2018/321, 36.

Strafprozeßordnung 1975 (StPO), BGBl 1975/631.

Verordnung des Bundesministers für Verkehr, Innovation und Technologie über Verfahren zur Identifikation von Teilnehmern (Identifikationsverordnung – IVO), BGBl II 2019/7.

Verordnung der Rundfunk und Telekom Regulierungs-GmbH, mit der Bestimmungen für Kommunikationsparameter, Entgelte und Mehrwertdienste festgelegt werden (Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 – KEM-V 2009), BGBl II 2009/212.

Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für

elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, ABl L 2023/191, 118.

VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

Vorblatt und Wirkungsorientierte Folgenabschätzung zur Änderung des Telekommunikationsgesetzes 2003: Vorblatt und WFA 15 BlgNR 26. GP.