Schwachstelle Mensch – Prävention gegen alte und neue Formen der Kriminalität

EuropaInstitut

AN DER UNIVERSITÄT ZÜRICH

Assoziiertes Institut der Universität Zürich & Kooperationspartner der ETH Zürich
RECHT BERATUNG WEITERBILDUNG

Herausgeber:
Christian Schwarzenegger, Rolf Nägeli

Schwachstelle Mensch – Prävention gegen alte und neue Formen der Kriminalität

12. Zürcher Präventionsforum
Tagungsband 2021

EIZ Publishing

Verlag: EIZ Publishing (eizpublishing.ch)
Herausgeber: Christian Schwarzenegger, Reinhard Brunner, Europa Institut an der Universität Zürich
Produktion, Satz & Vertrieb: buch & netz (buchundnetz.com)
Cover: buch & netz
ISBN:
978-3-03805-408-5 (Print – Softcover)
978-3-03805-456-6 (PDF)
978-3-03805-457-3 (ePub)
DOI: https://doi.org/10.36862/eiz-408
Version: 1.00-20211215

Dieses Werk ist als gedrucktes Buch sowie als Open-Access-Publikation in verschiedenen Formaten verfügbar: https://buchundnetz.com/werke/schwachstelle-mensch-praevention-gegen-alte-und-neue-formen-der-kriminalitaet/

Vorwort

Die Kriminalität ist im Wandel. Während sich Täter und Opfer früher in der realen Welt begegnet sind, findet vieles heute im digitalen Raum statt. Doch obwohl neue technische Möglichkeiten zur Tatbegehung genutzt werden, löst der technische Fortschritt das „Einfallstor Mensch" nicht einfach ab. Vielmehr liegen die Gründe für das Gelingen von deliktischen Verhaltensweisen häufig immer noch in der Ausnutzung menschlicher Eigenschaften wie Hilfsbereitschaft oder Gutgläubigkeit für die gezielte Manipulation des Opfers – *Social Engineering* nennt sich dieses Vorgehen. Im Rahmen des zwölften Zürcher Präventionsforums wurde aufgezeigt, welche Faktoren zur Vulnerabilität der Menschen beitragen und es wurden Einblicke in ausgewählte Praxisbeispiele gegeben. Die Tagung setzte sich zum Ziel aufzuzeigen, was der Fokus auf die „Schwachstelle Mensch" für die Kriminalprävention bedeutet und welche Massnahmen vielversprechend scheinen. Entsprechend gehen die Beiträge des vorliegenden Bands insbesondere den Fragen nach, wie sich Opfer- und Täterverhalten im Umgang mit den neuen Technologien entwickelt haben, welche neuen Erscheinungsformen der technologiegestützten Kriminalität es gibt und wie diesen Entwicklungen wirksam begegnet werden kann.

Dr. Mirjam Loewe-Baur, Präventionsabteilung der Kantonspolizei Zürich, befasst sich mit verschiedenen Erscheinungsformen von *Social Engineering*. Sie zeigt auf, wie Täter und Täterinnen die neuen Technologien ausnutzen und mit welchen Schwierigkeiten die Prävention, insbesondere im Umgang mit Opfern, konfrontiert wird.

Oliver Hirschi, MSc in Business Information Technology, MAS in Information Security, Leiter „eBanking – aber sicher!", Dozent an der Hochschule Luzern, führt in die grundlegenden Regeln der Passwortsicherheit ein. Er zeigt auf, wie Täter an die Passwörter einzelner User gelangen können, welche Rolle technische Neuerungen dabei spielen und wie sowohl beim Opfer als auch auf einer technologischen Ebene präventiv angesetzt werden kann.

Prof. Dr. Nora Markwalder, Assistenzprofessorin für Strafrecht, Strafprozessrecht und Kriminologie an der Universität St. Gallen, zeigt auf, welchen Einfluss neue Technologien auf die Art und Weise der Tatbegehung haben und wie sich die Kriminalität vermehrt in den digitalen Raum verlagert. Sie erläutert in ihrem Beitrag, welche Informationslücken bestehen und welche Probleme sich für die Prävention daraus ergeben.

Dr. Rutger Leukfeldt, Senior researcher, Netherlands Institute for the Study of Crime and Law Enforcement, Susanne van't Hoff-de Goede, Centre of Expertise Cyber Security, The Hague University of Applied Sciences, Dr. Rick van der Kleij, Centre of Expertise Cyber Security, The Hague University of Applied Sciences, The Netherlands Organisation for Applied Scientific Research (TNO) und Dr. Steve G.A. van der Wejer, Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) klären über die verschiedenen protektiven und Risikofaktoren für eine Online-Viktimisierung auf. Dabei gehen sie insbesondere auf die Diskrepanz zwischen selbstwahrgenommenem Risikobewusstsein im Netz und tatsächlichem Verhalten sowie dem fehlenden Bewusstsein der Gesellschaft über die Risiken von Cyberkriminalität ein.

Stefan Giger, Head Debit Processes & Fraud Management, UBS Switzerland AG, Zürich, vermittelt einen Einblick in die häufigsten Formen des Kartenbetrugs und zeigt auf, mit welchen Methoden die Täter an Karte und PIN des Opfers gelangen und wo die Prävention einsetzen muss.

Prof. Dr. Marc Jean-Richard-dit-Bressel, Rechtsanwalt, LL.M., Staatsanwalt und Abteilungsleiter bei der Staatsanwaltschaft III, Qualifizierte Wirtschaftskriminalität, Zürich, Titularprofessor an der Universität Zürich, setzt sich im letzten Beitrag des Sammelbandes mit der Frage auseinander, welche Bedeutung das Opferverhalten für die Strafbarkeit des Täters haben kann. Dafür geht er u.a. darauf ein, ob die Arglisthürde beim Betrugstatbestand eine geeignete kriminalpolitische Massnahme zur Erziehung des Opfers ist.

Für das gute Gelingen der Tagung und der Veröffentlichung dieses Bandes möchten wir Valeria Piritore für die professionelle Organisation und Durchführung der Veranstaltung sowie Noura Mourad, Sue Osterwalder, Vivian Stein und Petra Bitterli für die Gestaltung dieses Tagungsbandes herzlich danken.

Zürich, im September 2021

Christian Schwarzenegger, Rolf Nägeli

Inhaltsübersicht

Social Engineering – Der Mensch als Einfallstor

Mirjam Loewe-Baur

Inhalt

I. Von der Hilfsbereitschaft zur Gier – und der Macht der Situation

Die Schwachstelle Mensch rückt immer stärker in den Fokus der Täter. Während früher häufig technische Systeme angegriffen wurden, hacken sich Betrüger heute vorwiegend in die Psyche des Menschen, um sich zu bereichern. Die Modi Operandi sind dabei so vielfältig und schnelllebig, dass man leicht die Übersicht verlieren kann. Um einen Einblick in die Vielfalt von sogenannten Social Engineering Phänomenen zu ermöglichen, werden nachfolgend drei Beispiele erläutert, welche aktuell vertieft durch die Kantonspolizei Zürich bearbeitet werden.

Die Präventionsabteilung der Kantonspolizei Zürich hat sich erstmals im Jahr 2016 vertieft mit der Schwachstelle Mensch auseinandergesetzt. Ein Anstieg von sogenannten *Telefonbetrugsdelikten* – angefangen beim klassischen En-

keltrickbetrug[1] bis hin zur auch heute noch vorherrschenden Masche des falschen Polizisten[2] – führte dazu, dass Geschädigte, losgelöst von einem Strafverfahren, durch Präventionsspezialistinnen und -spezialisten interviewt wurden. Ziel war einerseits der Erkenntnisgewinn und andererseits eine Erstbetreuung der Geschädigten. Entgegen den Leserkommentaren von Medienbeiträgen zum Thema Telefonbetrug, in welchen Betroffene häufig als „dement", „naiv" oder gar „dumm" dargestellt werden, zeigte sich uns ein Bild sehr aktiver, kritisch denkender Personen, die gut in ihrem Umfeld eingebunden waren.

> Ja klar kannte ich den Telefonbetrug und dachte immer: So dumm kann man ja gar nicht sein.[3]

Nicht nur in Medienberichten, sondern auch in der Fachliteratur werden oftmals die mit dem erhöhten Alter in Verbindung stehenden abnehmenden kognitiven Fähigkeiten und ein schlechter physischer Gesundheitszustand als eine Erklärung für die Opferwerdung[4] von Telefonbetrugsdelikten herangezogen.[5] Die Interviews führten zur Erkenntnis, dass einerseits ansonsten positiv konnotierte Personeneigenschaften der Geschädigten wie Hilfsbereitschaft oder Gutgläubigkeit ausgenutzt wurden und andererseits seitens Täterschaft mit hohen zeitlichen und emotionalen Drucksituationen fungiert wurde.[6] Wie später dargelegt wird, sind diese beiden Komponenten, die Ausnutzung von Personen- und Situationseigenschaften, zentraler Bestandteil von Social Engineering. Insbesondere die Wirkung von Drucksituationen wird von vielen Personen unterschätzt was zur gefährlichen Annahme führt, selbst niemals betroffen zu sein. Geschädigte beschreiben eindrücklich, sie seien sich der „Macht der Situation" nicht bewusst gewesen.[7]

---

1 Die anrufende Person gibt sich hier als verwandte oder bekannte Person aus. Es erfolgt eine Geldforderung, um eine vorgegebene Notsituation zu beenden.

2 Die anrufende Person gibt sich hier als Polizistin oder Polizist aus. Es erfolgt eine Geldforderung, um eine Gefahrensituation der betroffenen Person abzuwenden.

3 Zitat einer Geschädigten.

4 Im vorliegenden Beitrag wird der kriminologische Opferbegriff verwendet. Der Begriff ist im kriminologischen Sinn weiter gefasst als im juristischen Sinn. Während er in der Rechtswissenschaft für Personen reserviert ist, die in ihrer körperlichen, psychischen oder sexuellen Integrität beeinträchtigt worden sind (Art. 1 Abs. 1 OHG), werden in der Kriminologie auch Personen berücksichtigt, die bezüglich ihres Vermögens geschädigt wurden.

5 Habermeyer/Guldimann, 25 ff.

6 Beispielsweise: „Wenn du das Geld nicht in den nächsten beiden Stunden bereitstellst, kann ich [nach einem Unfall] nicht operiert werden".

7 Für mehr Erkenntnisse und Präventionsansätze aus den Geschädigten-Interviews siehe Loewe-Baur/Eggli, 163 ff.

Als zweites Beispiel soll hier eines der wohl komplexesten Social Engineering Phänomene beschrieben werden, der sogenannte *Romance Scam*, auch Love Scam oder Liebesbetrug im Internet genannt. Die Betroffenen werden über soziale Netzwerke von vermeintlichen Personen angeschrieben, welche grosse Sympathie bekunden. Es entwickelt sich eine Liebesbeziehung, obwohl ein Treffen aufgrund vorgeschobener plausibel klingender Gründe nie zustande kommt. Ist die betroffene Person in einer emotionalen Abhängigkeit, erfolgen rasch Geldforderungen zur Behebung angeblicher Notlagen. Hinter dem vermeintlichen Partner steckt jedoch ein kriminelles Netzwerk.

Das Unverständnis der Gesellschaft darüber, dass man über Monate oder Jahre eine Beziehung mit jemandem führen kann, den man nie getroffen hat und dieser Person gar grosse Geldsummen zur Verfügung stellt, ist noch grösser als im Bereich des Telefonbetrugs. Im Rahmen von sogenannten polizeipräventiven Interventionen werden Betroffene durch die Polizei, losgelöst von einem Strafverfahren, aufgeklärt und beraten. Die Erfahrung zeigt, dass viele Betroffene lange Zeit Mühe haben einzusehen oder sich einzugestehen, dass sie betrogen wurden und die geliebte Person nicht existiert. Ein polizeilich geführtes Monitoring der Fälle aus dem Jahr 2019 zeigt, dass zum Zeitpunkt der Anzeige lediglich 47% der Betroffenen den Kontakt abgebrochen hatten. Weiter zeigt sich ein sehr heterogenes Bild in Bezug auf Alter, Bildungsstatus, beruflicher Position und Wohlstand. Von der Managerin mittleren Alters, welche im Finanzsektor tätig ist, über den Rentner, welcher sich ein erotisches Abenteuer erhofft, bis zur Grossmutter, die nach dem Tod ihres Ehemannes eine neue Liebe sucht, ist alles möglich. Ähnlich wie beim Telefonbetrug sind gewisse Personeneigenschaften wie Gutgläubigkeit, aber auch Impulsivität ausgeprägt.[8] Auffallend ist zudem, dass sich die Betroffenen häufig in einer schwierigen Lebenslage befinden (z.B. Scheidung oder Jobverlust) und unverarbeitete schwierige Lebenserfahrungen vorhanden sind. Die Kontaktaufnahme durch den Scammer erfolgt zunächst meist sehr ungezwungen. Viele Betroffene sind nicht aktiv auf der Suche nach einer neuen Partnerschaft. Der Beziehungsaufbau erfolgt langsam, indem der Social Engineer beispielsweise Komplimente äussert, aber auch gezielt auf die (allenfalls schwierige) Lebenssituation der Betroffenen eingeht und diese spiegelt (ebenfalls gerade eine Scheidung hinter sich oder den Job verloren). Zusammen mit dem intensiven Kontakt, den Liebesbekundungen und dem entgegengebrachten Verständnis entsteht eine tiefe Abhängigkeit.[9] Dass ein persönliches Treffen nie zustande kommt und Geld für eigenartige „Notfälle“ gefordert wird, wird plötzlich nicht mehr hinterfragt. Interessanterweise gibt eine Vielzahl der Be-

[8] So auch Whitty, 105.

[9] So auch Marx/Rüdiger, 212.

troffenen an, phasenweise an der Echtheit ihres „Partners" gezweifelt zu haben oder daran gedacht zu haben, den Kontakt abzubrechen. Dennoch gelang es der Täterschaft immer wieder, so auf die Bedürfnisse der Betroffenen einzugehen, dass der Kontakt und damit die Zahlungen bestehen blieben.[10]

Ein gänzlich unterschiedliches Social Engineering Phänomen ist der derzeit stark vorherrschende *Online Anlagebetrug*. Hier werden Personen dazu animiert, Geld auf betrügerischen Online Plattformen zu investieren. Angesprochen werden Personen, welche ihr Geld möglichst rasch vermehren möchten und damit eine gewisse Ausprägung an Gier aufweisen. Eine zwischenmenschliche Komponente, wie sie bei den Phänomenen Telefonbetrug und Romance Scam beobachtet werden kann, ist beim Online Anlagebetrug demnach nicht in gleichem Ausmass vorhanden. Besonders hervorzuheben ist hier die Professionalität der Täterschaft in Bezug auf unterschiedliche Komponenten. In technischer Hinsicht wird deutlich, dass die Online Plattformen täuschend echt aussehen. Die darauf abgebildeten Börsenkurse korrespondieren in Echtzeit mit den realen Börsenkursen. Auch die involvierten Supportpersonen und Broker sind professionell, aber auch sehr bestimmt im Umgang.

> „Okay, Sie haben Angst", sagt Klaus, „wenn man eine erste Investition macht, fühlt es sich immer so an."[11]

Professionell findet insbesondere auch die Vermarktung statt. So werden Prominente eingesetzt, die (gegen ihren Willen) für die Plattform werben und (gefälschte) positive Google Rezensionen geladen. Erste Erkenntnisse der Kantonspolizei Zürich deuten darauf hin, dass die Betroffenen in Bezug auf Alter, Geschlecht und Bildungsstatus eine sehr heterogene Gruppe bilden.

Die drei beispielhaften Social Engineering Phänomene werden in den nachfolgenden Kapiteln herangezogen um die theoretischen Grundlagen zu veranschaulichen, Zusammenhänge zu beleuchten und Präventionsansätze aufzuzeigen.

II. Social Engineering: Begriff und Definition

Der Begriff Social Engineering ist keinesfalls eine neue Erscheinung. In der Hacker Community tauchte er bereits in den 1970er Jahren, also kurz nach der Entstehung des Internets[12] auf. Heute handelt es sich beim Social Engineering

---

10 Zahlen und Erkenntnisse gemäss Fall-Monitoring der Präventionsabteilung der Kantonspolizei Zürich, basierend auf dem Jahr 2019 und gemäss polizeipräventiven Interventionen.

11 Schopp/Baumgartner.

12 Hegemann.

um eine der verbreitetsten Angriffsmethoden.[13] Es existiert jedoch keine allgemeingültige Definition des Begriffs – vielmehr werden je nach Disziplin unterschiedliche Schwerpunkte gesetzt. Anhand der Definition des Nationalen Zentrums für Cybersicherheit des Bundes soll auf ein paar wesentliche Punkte eingegangen werden.

> Social Engineering ist eine zwischenmenschliche Beeinflussung mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie z. B. zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um schutzwürdige Informationen oder unbezahlte Dienstleistungen zu erlangen.[14]

Bevor eine inhaltliche Auseinandersetzung erfolgt, soll hier die Quelle der Definition thematisiert werden. Diese legt den Schluss nahe, es handle sich bei Social Engineering Angriffen immer um Phänomene mit Bezug zur Cyberkriminalität. Aus einer inhaltlichen Perspektive greift dies jedoch zu kurz – ist doch in der Definition selbst nirgends die Rede von Cyberdelikten oder Ähnlichem. Ein Beispiel für ein Phänomen mit starker Social Engineering Komponente ausserhalb der Cyberkriminalität ist der eingangs erläuterte Telefonbetrug. Trotzdem wird Social Engineering in der Praxis und in der Fachliteratur fast ausschliesslich mit Cyberkriminalität in Verbindung gebracht. Dies hat mehrere Gründe. Mit dem erstmaligen Auftauchen des Begriffs in der Hacker Community ist die Verankerung im Cyberbereich historisch gewachsen. Zudem hat der technische Fortschritt die Aktivitäten von Social Engineers stetig vereinfacht. Mit zunehmendem Anschluss von alltäglichen Anwendungen ans Internet (z.B. smart home), der Ausbreitung sozialer Netzwerke, dem ständigen Zugriff auf Mobile Devices und flexiblen öffentlichen Arbeitsplätzen werden nicht nur grössere Mengen an sensiblen Daten produziert, sondern auch die Gelegenheiten für Angreifer vervielfacht. Teilweise bedienen sich Social Engineers zudem neueren Technologien wie Machine Learning oder Artificial Intelligence, welche es erlauben, tausende von Personen, zum Beispiel mit einem Phishing Mail, gleichzeitig zu erreichen und damit effizienter und aggressiver anzugreifen.[15] Als theoretische Grundlage dieser Entwicklung kann der Routine Activity Approach, begründet durch Cohen und Felson herangezogen werden, wonach sich Kriminalität an die Routineaktivitäten einer Gesellschaft anpasst: Mit dem technischen Fortschritt ergeben sich somit auch neue Tat-

---

13 Wang/Sun/Zhu, 85094.

14 Nationales Zentrum für Cybersicherheit.

15 Wang/Zhu/Sun, 11895 ff.

gelegenheiten.[16] Trifft ein motivierter Täter auf ein geeignetes Tatobjekt, welches nicht ausreichend geschützt ist, wird Kriminalität nach diesem Ansatz wahrscheinlicher.

Aus einer inhaltlichen Perspektive weist die Definition des Nationalen Zentrums für Cybersicherheit zunächst auf den zentralen Punkt der *zwischenmenschlichen Beeinflussung* hin, auf welche im nachfolgenden Kapitel näher eingegangen wird. Ziel des Social Engineers ist immer Bereicherung, wobei finanzielle Mittel oder persönliche Informationen im Fokus stehen können. Auch persönliche Informationen können rasch zu Geld gemacht werden, im (Dark-)Netz besteht ein regelrechter Handel mit persönlichen Daten.[17] Die Beeinflussung geschieht, indem gezielt auf *Personeneigenschaften* (in der Definition als Verhaltensweise bezeichnet) Einfluss genommen wird und auch das *Umfeld entsprechend analysiert und modelliert* wird. Je nach Phänomen und Person stehen ganz unterschiedliche Personeneigenschaften im Fokus. So spielt die in der Definition beispielhaft genannte Autoritätshörigkeit beim Telefonbetrug eine wichtige Rolle (gerade ältere Personen sehen Polizistinnen und Polizisten als Autoritätspersonen an), während diese beim Romance Scam eine untergeordnete spielt. Auch das Ausspionieren des Umfelds einer Person erfolgt je nach Phänomen sehr unterschiedlich. Während beim Telefonbetrug das Opfer einzig bis zur Geldübergabe vom Umfeld ferngehalten wird (in der Regel wenige Stunden), kommt dem Umfeld beim Romance Scam eine viel zentralere Bedeutung zu. So werden die Betroffenen gezielt von ihrem (potentiell schützenden) Umfeld ferngehalten.

Häufig kommen die Angreifer ganz ohne technische Hilfsmittel aus – vielmehr bedienen sie sich grundlegender psychologischer Strategien. Umso erstaunlicher ist es, dass sich die Disziplin der Psychologie bisher nur wenig mit Social Engineering auseinandergesetzt hat.[18] Wie im nächsten Kapitel dargelegt wird zeigt sich jedoch, dass bestehende sozialpsychologische Modelle dazu geeignet sind, einzelne Komponenten des Funktionsmechanismus von Social Engineering zu erklären.

III. Verhalten ist komplex

Wie entsteht Verhalten? Unter welchen Gegebenheiten lassen wir uns beeinflussen? Die Beantwortung dieser zentralen Fragen kann die Psychologie nicht anhand eines einzelnen Modelles liefern. Vielmehr handelt es sich um ein

16 Cohen/Felson, 588 ff., Clarke, 39 ff.

17 Schwanebeck, 11 ff.

18 Schaab/Beckers/Pape, 241 ff.

Gefüge von komplexen Einflussfaktoren. Es besteht jedoch Einigkeit darüber, dass sowohl Eigenschaften der Person als auch ihrer Umwelt relevant sind.[19] Diese Grundlagenerkenntnis steht im Einklang mit der Definition von Social Engineering, wonach Betrüger auf beide Komponenten Einfluss nehmen.

1. Personeneigenschaften

Im Zusammenhang mit Social Engineering kommt rasch die Frage auf, ob es gewisse „Risiko-Persönlichkeitsprofile" gibt. Die polizeiliche Fallarbeit zeigt, dass die Persönlichkeitseigenschaften von Betroffenen je nach Phänomen sehr unterschiedlich sind. Ebenfalls ist innerhalb gewisser Phänomene eine grosse Vielfalt an Persönlichkeitseigenschaften zu beobachten. So kann beispielsweise beobachtet werden, dass Geschädigte eines klassischen Enkeltrickbetruges mehrheitlich hilfsbereite und gewissenhafte Personen sind. Im Phänomen Romance Scam fällt es hingegen schwerer, typische Persönlichkeitseigenschaften auszumachen.

Wählt man nicht die praktische Fallarbeit, sondern den Fachbereich der Persönlichkeitspsychologie als Ausgangslage, stellt sich zunächst die Frage nach einer geeigneten Klassifizierung von Persönlichkeitseigenschaften. In der Persönlichkeitspsychologie hat sich ein sogenannter lexikalischer Ansatz durchgesetzt.

> Im lexikalischen Ansatz wird das gesamte Lexikon einer Sprache nach Eigenschaftsworten durchforstet. Ungebräuchliche Worte werden weggelassen, und von Worten sehr ähnlicher Bedeutung wird nur eines behalten. Wenn so eine überschaubare Menge von ca. 100 Eigenschaftsworten entstanden ist, wird eine große Gruppe von Personen gebeten, sich selbst oder andere bezüglich aller dieser Eigenschaftsworte zu beurteilen (z.B. mit Hilfe von Likert-Skalen). Jedem Wort entspricht also eine Eigenschaftsvariable. Diese Eigenschaftsvariablen werden dann mit Hilfe der Faktorenanalyse auf möglichst wenige Faktoren reduziert. Sie beschreiben auf effiziente Weise alltagspsychologisch wahrnehmbare Persönlichkeitsunterschiede.[20]

Auf diese Art sind die heute sehr gebräuchlichen *Big Five* entstanden. Demnach kann die Persönlichkeit durch fünf Faktoren beschrieben werden.[21]

1. *Offenheit gegenüber neuen Erfahrungen*: intellektuelle Neugier, Gefühl für Kunst und Kreativität
2. *Gewissenhaftigkeit*: Ordentlichkeit, Beharrlichkeit, Zuverlässigkeit

---

19 Für eine Übersicht zu Person-Umwelt Ansätzen siehe Eckardt.

20 Asendorpf, 54.

21 Asendorpf, 54.

3. *Extraversion*: Geselligkeit, Ungehemmtheit, Aktivität
4. *Verträglichkeit*: Freundlichkeit, Hilfsbereitschaft, Wärme im Umgang mit anderen
5. *Neurotizismus*: Nervosität, Ängstlichkeit, Gefühlsschwankungen

Ein anderes Persönlichkeitskonstrukt ist die sogenannte *Selbstkontrolle*, welche durch die allgemeine Kriminalitätstheorie (General Theory of Crime) von Gottfredson und Hirschi eine zentrale Bedeutung erlangt hat. Die Begründer der Theorie gehen davon aus, dass sich Selbstkontrolle in der frühen Kindheit entwickelt und mit etwa acht Jahren abgeschlossen ist. Wie stark die Selbstkontrolle ausgeprägt ist, ist davon abhängig, wie Eltern auf abweichendes Verhalten reagieren. Erfolgt keine Reaktion, so entwickelt sich keine oder nur geringe Selbstkontrolle. Die Autoren gehen davon aus, dass die Selbstkontrolle nach abgeschlossener Entwicklung ein stabiles Persönlichkeitsmerkmal darstellt, unabhängig von Umgebungseinflüssen.[22] Kern der Theorie ist, dass wer über eine hohe Selbstkontrolle verfügt, auch eher auf kriminelles Verhalten verzichtet.[23] Auf Basis der Annahme, dass sich Personen mit geringer Selbstkontrolle auch weniger schützen, soll Selbstkontrolle nicht nur ein Prädiktor bezüglich Ausübung von Kriminalität, sondern auch bezüglich Opferwerdung sein.[24] Dies gilt insbesondere für hands-off Delikte wie Betrug, da für deren Erfolg meist ein minimales Zutun der Betroffenen nötig ist, welches bei geringer Selbstkontrolle eher erfolgt.[25]

Hinsichtlich der Erklärung von Social Engineering Phänomenen stellt sich die Frage, ob Betroffene spezifische Persönlichkeitsprofile (Big Five und Selbstkontrolle) aufweisen. Empirische Hinweise dazu sind jedoch nur sehr wenig vorhanden. Eine Metaanalyse von Pratt et al. zeigt jedoch, dass Selbstkontrolle ein robuster Prädiktor für die Opferwerdung von hands-off Delikten im Bereich Cyberkriminalität darstellt.[26] Van Gelder und De Vries untersuchten den Zusammenhang zwischen Selbstkontrolle und den Faktoren Verträglichkeit und Gewissenhaftigkeit der Big Five und fanden eine positive Korrelation. So geht hohe Selbstkontrolle vermehrt mit hoher Gewissenhaftigkeit und hoher Verträglichkeit einher.[27] Inwiefern hohe Gewissenhaftigkeit und hohe Verträglichkeit jedoch tatsächlich mit einer höheren Viktimisierungswahrscheinlichkeit korrelieren, muss im Zuge künftiger Forschung differenziert untersucht

22 Gottfredson/Hirschi, 90.
23 Gottfredson/Hirschi.
24 Schreck, 633.
25 Holtfreter/Reisig/Pratt, 189.
26 Pratt et al., 87.
27 Van Gelder/De Vries, 637.

werden. Van de Weijer und Leukfeldt fanden in Bezug auf die Viktimisierung im Bereich Cyberkriminalität lediglich einen Zusammenhang mit Gewissenhaftigkeit, nicht jedoch mit Verträglichkeit.[28] Diese heterogenen ersten Befunde deuten darauf hin, dass Cyberkriminalität bzw. Kriminalität mit starker Social Engineering Komponente differenziert (phänomenespezifisch) betrachtet und untersucht werden sollte.

2. Umwelteigenschaften

Personeneigenschaften dürfen nicht losgelöst von der Umwelt, in welcher sich eine Person befindet, betrachtet werden, denn auch sie beeinflusst das aktuelle Erleben und Verhalten einer Person. Dabei geht es zum einen um die Häufigkeit und Dauer von Situationen. Wie viel Zeit verbringt eine Person auf den sozialen Medien, wie viel Zeit verbringt sie bei der Arbeit, wie oft kommt es zu Streit mit dem Partner? Zum anderen sind hier einschneidende Erlebnisse und Lebensbedingungen zu nennen. So beeinflussen beispielweise eine Scheidung oder der Verlust einer Arbeit das aktuelle Erleben und Verhalten einer Person ebenfalls.[29]

Ausgehend von der Fallarbeit mit Betroffenen soll hier ein wesentlicher Punkt vertieft werden. Diese zeigt, dass die hohe und stetig zunehmende *Online Präsenz* ein wesentlicher Risikofaktor zu sein scheint.[30] Dies hat zu einem grossen Teil mit den bereits erwähnten zahlreichen Angriffsmöglichkeiten im Internet zu tun. Es stellt sich dennoch die Frage, welche Faktoren darüber entscheiden, ob eine Person einen Angriff erkennt oder nicht. Im Auftrag unterschiedlicher behördlicher und nicht-behördlicher Institutionen wurde im Jahr 2019 eine repräsentative Befragung der Deutsch- und Westschweizer Bevölkerung zur Sicherheit im Internet in Auftrag gegeben. Als zentrale Elemente wurde erfasst:

Frageelemente	**Kernresultat**
Wissensstand: Wie gut schätzen die Befragten ihr Wissen über Sicherheit im Internet ein?	59% schätzen ihr Wissen als eher gut bis sehr gut ein.

28 Van de Weijer/Leukfeldt, 411.

29 Asendorpf, 119 ff.

30 Bundesamt für Statistik (BFS), Internetnutzung in den Haushalten im Jahr 2019, <https://www.bfs.admin.ch/bfs/de/home/statistiken/kataloge-datenbanken/medienmitteilungen.assetdetail.11127962.html>.

Frageelemente	**Kernresultat**
Sicherheitsgefühl: Wie sicher fühlen sich die Befragten im Umgang mit dem Internet?	80% fühlen sich eher sicher bis sehr sicher.
Betroffenheit: War die befragte Person schon einmal von einem Angriff betroffen?	15% waren bereits von einem Angriff betroffen, der ihnen finanziellen oder emotionalen Schaden angerichtet hat.
Schutzmassnahmen: Setzen die Befragten Schutzmassnahmen ein?	Häufigste angewendete Schutzmassnahme Antivirusprogramm (61%), gefolgt von Verhaltensregeln (nicht auf seltsame Links klicken, Mails mit unbekanntem Absender genau prüfen (je 27%)).

Die Interpretation der Ergebnisse fällt insofern schwer, als dass keine vergleichbaren Daten aus anderen Ländern vorliegen. Zudem muss beachtet werden, dass es sich um subjektive Angaben handelt. Zusätzlich zu den dargestellten deskriptiven Ergebnissen wurden Zusammenhänge zwischen den vier Frageelementen eruiert, welche auf komplexe Interaktionen hinweisen. So fühlten sich beispielsweise auch 67% der Personen mit tief selbst eingeschätztem Wissensstand sicher und Personen mit hoch eingeschätztem Wissensstand zeigten unsicheres Verhalten (z.B. im Umgang mit Passwörtern).[31] Die Resultate der Befragung zeigen auf, dass weitere Forschung nötig ist, um das komplexe Themenfeld weiter auszuleuchten. Die Kantonpolizei Zürich unterstützt derzeit eine Studie des Instituts für Informatik der Universität Zürich, welche die mentalen Modelle von Personen bezüglich Sicherheit im Internet untersucht.

IV. Soziale Beeinflussung

Die Psychologie hat erst nach der Jahrtausendwende damit begonnen, die mentalen Prozesse und Tätertaktiken, welche sich Social Engineers zunutze machen, zu untersuchen. Hierzu wurden nicht neue Modelle entwickelt – vielmehr wurden bestehende sozialpsychologische[32] Modelle und Konzepte zur Erklärung von Social Engineering herangezogen.[33]

---

31 gfs, 2 ff.

32 Sozialpsychologie ist der Versuch, zu verstehen und zu erklären, wie die Gedanken, Gefühle und Verhaltensweisen von Personen durch die tatsächliche, vorgestellte oder implizite Anwesenheit anderer Menschen beeinflusst werden, Allport, 5.

33 Steinmetz/Goe/Pimentel, 173 ff.

Am häufigsten werden wohl die sogenannten *Persuasionsstrategien* von Cialdini genannt, welche ihre Hauptanwendung in der Werbepsychologie finden.[34] Die Ähnlichkeit liegt nahe: Statt Personen dazu zu motivieren, ein Produkt zu kaufen, sollen Personen zur Freigabe von Finanzmitteln oder Preisgabe persönlicher Informationen gebracht werden. Die Verhaltenssteuerung steht bei beiden Anwendungsbereichen im Vordergrund. Nachfolgend werden die sechs Persuasionsstrategien dargelegt. Zudem wird aufgezeigt, welche Strategien bei welchen der einleitend erläuterten Social Engineering Phänomene zur Anwendung kommen (Einschätzung der Autorin. Es ist zu beachten, dass auch innerhalb der Phänomene, das heisst von Fall zu Fall, unterschiedliche Strategien wirken).

Persuasionsstrategie	**Telefonbetrug**	**Romance Scam**	**Online-Anlagebetrug**
1. Reziprozität Menschen sind eher dazu gewillt etwas zu geben, wenn sie vorab bereits etwas Kleines erhalten haben. Dabei kann es sich um finanzielle Mittel oder Informationen handeln.	x	x	x
2. Konsistenz Menschen haben das Bedürfnis, in ihrem eigenen Verhalten konsistent zu sein. Je länger man also beispielsweise nicht auf ein schlechtes Bauchgefühl hört, desto schwieriger wird es, eine Situation zu verlassen.	x	x	x
3. Soziale Bewährtheit Menschen orientieren sich stark daran, was andere tun. Entsteht der Eindruck, andere Personen hätten sich gleich verhalten (z.B. gute Erfahrung mit einem Anlageprodukt gemacht), so folgen wir dieser Mehrheit mit grosser Wahrscheinlichkeit.			x
4. Autorität / Expertenstatus Menschen folgen der Überzeugung, dass bestimmte Personengruppen glaubwürdiger sind als andere – sei dies aufgrund ihrer Funktion (Polizei als Autoritätsinstanz) oder ihres Wissens (erfahrener Broker als Experte auf seinem Gebiet)	x		x
5. Sympathie Menschen sind soziale Wesen. Entsprechend schliessen wir automatisch von positiv konnotierten Personeneigenschaften wie Sympathie auf andere positive Personeneigenschaften wie Vertrauenswürdigkeit.	x	x	x
6. Knappheit Je knapper die Zeit oder ein Produkt, desto eher lassen wir uns unter Druck setzen und handeln sofort.	x	x	x

[34] Steinmetz/Goe/Pimentel 173 ff., Archer, Quiel.

Mit dem Versuch, die drei Phänomene den Persuasionsstrategien zuzuordnen zeigt sich zunächst, dass die Persuasionsstrategien dazu geeignet sein könnten, die Verhaltenssteuerung durch die Social Engineers partiell zu erklären. Dabei kommen nicht immer alle Strategien gleichzeitig zum Zug. Vielmehr zeigt sich ein phänomenespezifisches Muster, wobei nicht auszuschliessen ist, dass die Strategien gar von Fall zu Fall variieren können. So mag ein falscher Polizist in einem Fall sympathisch auftreten, während er in einem anderen Fall als unsympathisch, aber umso autoritärer wahrgenommen wird. Unterschiedliche Kombinationen der Persuasionsstrategien sind demnach zwischen und innerhalb der Phänomene zu beobachten. Weiter stellt sich die Frage, ob gewisse Strategien besonders häufig oder besonders erfolgreich zur Anwendung kommen. Die Fallarbeit mit unterschiedlichen Phänomenen legt nahe, dass die Knappheit bei sämtlichen Phänomenen in der einen oder anderen Art eine Rolle spielt. Geht es um die Übergabe von Finanzmitteln oder Informationen, so wird praktisch immer zeitlicher und meist zusätzlich emotionaler Druck ausgeübt. Diese Vermutung müsste jedoch – wie auch die Anwendbarkeit der Persuasionsstrategien auf Social Engineering Phänomene im Allgemeinen – empirisch überprüft werden. Interessanterweise fand eine solche trotz häufiger Nennung der Persuasionsstrategien im Zusammenhang mit Social Engineering nur sehr vereinzelt und eher im Kontext anderer psychologischer Wirkmechanismen statt.[35] So konnte Workman einen positiven Zusammenhang zwischen *normative commitment* (Verpflichtungsgefühl, sich an Regeln zu halten), *continuance commitment* (Konsistenz und Integrität im Verhalten) sowie *affective commitment* (Sympathie, emotionale Verbundenheit mit anderen) und der Wahrscheinlichkeit, Opfer eines Social Engineering Angriffes zu sein, finden.[36]

Weiter muss beachtet werden, dass die Persuasionsstrategien nicht die einzigen psychologischen Konzepte darstellen, die sich Social Engineers zunutze machen. Vielmehr sind unterschiedliche *sogenannte kognitive Verzerrungen* dafür verantwortlich, dass wir Menschen nicht immer rational denken, entscheiden und handeln.

> Kognitive Verzerrung (englisch: cognitive bias) ist ein Sammelbegriff für systematische, unbewusste und fehlerhafte Prozesse der menschlichen Informationsverarbeitung.[37]

---

35 Steinmetz/Goe/Pimentel, 187.

36 Workman, 662 ff.

37 Begründer dieses Ansatzes sind Tversky/Kahnemann, welche die erste Publikation dazu 1974 im Magazin Science veröffentlichten. Siehe auch Weber/Knorr, 103 ff.

In seinem Buch *schnelles Denken, langsames Denken*, beschreibt Kahnemann, dass unser Denken, unsere Entscheidungen und unser Verhalten durch zwei unterschiedliche Systeme gesteuert werden. *System 1* arbeitet intuitiv, schnell und vor allem ohne bewusste Steuerung. Muss schnell auf ein Ereignis reagiert werden, befähigt uns System 1 dazu, indem wir beispielsweise fliehen, wenn wir Schüsse hören oder Ähnliches. Die kognitive Verarbeitung von Informationen erfolgt ganz ohne Anstrengung. *System 2* hingegen arbeitet nur mit bewusster Steuerung. Relevante Informationen werden von irrelevanten getrennt, bewertet und zusammengefügt. Dieser Prozess dauert um ein vielfaches länger als die Verarbeitung durch System 1. Wenn immer möglich, geht unser Gehirn den Weg des geringsten Widerstandes und setzt System 1 ein, um Ressourcen zu sparen. Dies ist im Alltag auch sehr sinnvoll, denn es wäre unmöglich, sämtliche Informationen, die tagtäglich auf uns einprasseln, analytisch nach System 2 zu verarbeiten.[38]

Social Engineers machen sich zunutze, dass unsere Entscheidungen und unser Verhalten häufig nicht durch unsere Ratio, sondern durch unsere Emotionen gesteuert werden. Mit den Persuasionsstrategien und anderen psychologischen Mechanismen versuchen sie zu verhindern, dass das kognitive System 2 zum Zuge kommen könnte. Denn die Persuasionsstretgien appellieren nicht an das rationale Denken – im Gegenteil. Wenn Mechanismen wie Reziprozität oder Sympathie wirken, braucht es eine bewusste Steuerung der Gedanken auf System 2.

Zusammenfassend kann gesagt werden, dass Personeneigenschaften, Umwelteigenschaften und Beeinflussungsstrategien der Täterschaft darüber entscheiden dürften, ob Social Engineers mit ihren Angriffen Erfolg haben oder nicht. Dabei ist zu beachten, dass es in allen drei Bereichen sowie deren Interaktion weitere Forschung braucht, um differenzierte Aussagen dazu machen zu können, wie Social Engineering funktioniert. Als Basis könnten die beiden Denksysteme nach Kahnemann dienen. So dürften auch Personeneigenschaften die Verarbeitung im einen oder anderen System vereinfachen. Denkbar wäre, dass Extraversion, Offenheit für neue Erfahrungen und Verträglichkeit eine Verarbeitung nach System 1 begünstigen, während Gewissenhaftigkeit und Neurotizismus eher eine Verarbeitung nach System 2 wahrscheinlicher machen. Auch die Umwelteigenschaften dürften einen Einfluss auf die kognitive Verarbeitung haben. So sind Personen, die sich in einer schwierigen Lebenssituation befinden generell mental ausgelasteter, was eine rasche, unbewusste Verarbeitung wahrscheinlicher macht.

---

[38] Kahnemann.

V. Prävention

1. Evidenzbasierte Vorgehensweise

Angesichts der Vielfalt, Komplexität und Schnelllebigkeit von Social Engineering basierten Phänomenen stellt sich die Frage nach einer geeigneten Präventionsstrategie und wirksamen Präventionsmassnahmen. Eine strukturierte, *evidenzbasierte Herangehensweise* scheint wichtiger denn je.[39] Im Zuge der sogenannten problemorientierten Polizeiarbeit[40] entstand das SARA-Modell, welches von der systematischen Problemerfassung (Scan) über eine Problemanalyse (Analysis) und Massnahmenableitung (Response) bis zur Evaluation der Massnahmen (Assessment) führt.

Diese Vorgehensweise klingt in der Theorie trivial, ist aber in der praktischen Umsetzung – gerade wenn es um die Bekämpfung neuer Phänomene geht – oftmals eine Herausforderung. Das zentrale Element der evidenzbasierten Vorgehensweise ist die Ausrichtung von Entscheidungen über Vorgehensweisen an möglichst aktuellen Auswertungen der verfügbaren kriminologischen Indikatoren wie beispielsweise Kriminalstatistiken, Opfer-, Täter- und allgemeine Bevölkerungsbefragungen. Für neue Phänomene bedeutet dies, dass in einem ersten Schritt eine aufwändige Datensammlung und -auswertung nötig ist. Dabei sollten wenn immer möglich nicht nur objektive, sondern auch subjektive Daten berücksichtigt werden. Subjektive Indikatoren sind Daten, welche durch die Wahrnehmung von Personen beeinflusst werden (beispielsweise Angaben aus Geschädigten-Interviews oder die oben thematisierte Umfrage zur Sicherheit im Internet, siehe III.2.) während objektive Indikatoren frei von der Wahrnehmung einzelner Personen sind (beispielsweise erbeutete Deliktsumme). In der praktischen Umsetzung bedeutet dies meist die Installation eines umfassenden Monitorings, welches Daten aus den vorhandenen polizeilichen Systemen und Informationen aus anderen Quellen wie Geschädigten-Interviews konsolidiert. Auf der Basis solch spezifischer Daten werden in einem weiteren Schritt gezielte präventive Massnahmen abgeleitet und entwickelt, worauf im Folgekapitel separat eingegangen wird.

Die Datenerhebung und -analyse ist nicht nur für die Planung von Präventionsmassnahmen wichtig, sondern insbesondere auch für deren Wirksamkeitsüberprüfung (Assessment). Dazu sind in einem ersten Schritt sogenannte Erfolgskriterien festzulegen: Welche Konditionen müssen erfüllt sein, damit eine Präventionsmassnahme als wirksam eingestuft werden kann? Wie können

---

39 Koziarski/Lee, 198.

40 Eck/Spelman.

diese Konditionen messbar gemacht werden? Die Sozialwissenschaften halten unterschiedliche Methoden bereit, die – im Idealfall – eine Aussage zum Kausalzusammenhang zwischen der Präventionsmassnahme und dem definierten Erfolgskriterium machen.

Sogenannte Quasi-Experimente wurden in der Praxis verschiedentlich umgesetzt. Dabei wird das definierte Erfolgskriterium (beispielsweise die Anzahl polizeilich registrierter Telefonbetrugsdelikte) über einen längeren Zeitraum in zwei unterschiedlichen, jedoch vergleichbaren, Gruppen untersucht. Nach ersten Messungen wird eine der beiden Gruppen (die Experimentalgruppe) präventiven Massnahmen ausgesetzt, während die andere Gruppe (Kontrollgruppe) keinen Massnahmen ausgesetzt wird. Der Vergleich der Anzahl registrierter Telefonbetrugsdelikte in beiden Gruppen ermöglicht dann eine Aussage zur Wirksamkeit der umgesetzten Massnahmen. Einschränkend ist hier jedoch darauf hinzuweisen, dass Deliktphänomene mit grossem Dunkelfeld eher ungeeignet für ein solches Design sind. So könnte eine präventive Massnahme auch dazu führen, dass betroffene Personen vermehrt Anzeige erstatten und die Zahlen somit gemäss polizeilicher Statistik steigen, was aber auf eine Aufhellung des Dunkelfeldes zurückzuführen wäre. In einem solchen Fall müsste das Erfolgskriterium um Angaben aus einer Dunkelfeldstudie (subjektiver Indikator) ergänzt werden. Eine weitere Herausforderung bei der Anwendung von Quasi-Experimenten ist die Schwierigkeit, intervenierende Variablen konstant zu halten. Intervenierende Variablen sind Einflussfaktoren, die das Erfolgskriterium ebenfalls beeinflussen können. Dies können beispielsweise gesellschaftliche Entwicklungen sein, ein verändertes Tätervorgehen oder andere Faktoren, welche (ungewollt) auf die Testpersonen einwirken. Durch die zunehmende Präsenz des Internets im Alltag nehmen auch die potentiellen intervenierenden Variablen zu. In der Praxis ist es häufig nicht möglich, sämtliche Einflussfaktoren konstant zu halten oder zu vermeiden. Weiter besteht die Schwierigkeit, dass Quasi-Experimente mit grossem Aufwand verbunden sind und aufgrund Ressourcenknappheit oftmals nicht umgesetzt werden.[41]

Dies bedeutet jedoch nicht, dass Präventionsmassnahmen nicht evaluiert werden können. Vielmehr muss phänomene- und massnahmenspezifisch eruiert werden, welche objektiven und subjektiven Indikatoren geeignet erscheinen, um Aussagen zur Wirksamkeit machen zu können. Dies beginnt bei der Definition der Erfolgskriterien. Ziel der heutigen evidenzbasierte Kriminalprävention sollte ein systematisches, datengeleitetes Vorgehen sein, welches in der Praxis umsetzbar ist und zum Schutz der Bevölkerung beiträgt.

---

41 Scott/Kirby.

2. Präventionsdreieck und Präventionsebenen

Präventive Massnahmen sollen aufgrund einer umfassenden Problemanalyse entwickelt werden (siehe V.1.). Dabei stellt sich die Frage, wie die Fülle von Präventionsmassnahmen strukturiert und geordnet werden kann. Die klassische Kriminalprävention stellt dafür zwei kombinierbare Strategien zur Verfügung: Die Anwendung des Präventionsdreiecks und der Präventionsebenen.

Das *Präventionsdreieck* zeigt auf, dass präventive Massnahmen grundsätzlich auf die Veränderung dreier Komponenten zielen können: Die Situation, die Täterschaft und die (potentiellen) Opfer beziehungsweise Geschädigten. Metaanalytische Befunde zeigen, dass kriminalpräventive Massnahmen, welche auf eine *Veränderung der Situation* zielen, die höchste Wirksamkeit aufweisen.

> It is easier to alter environmental conditions than individual behavioutal tenedencies.[42]

Gerade bei Phänomenen mit Bezug zum Cyberbereich hat die technologische Entwicklung viel zur Sicherheit der Nutzerinnen und Nutzer beigetragen: Firewalls, Antivirenprogramme oder die Zweifaktoren-Authentifizierung tragen massgeblich dazu bei, Hackern das Leben schwerer zu machen. Diese wichtigen Massnahmen vermögen die Social Engineering basierten Phänomene jedoch nicht einzudämmen – denn selbst die besten technischen Schutzprogramme werden durch Menschen kontrolliert.

Auch die *Einflussnahme auf das Verhalten der Täterschaft* verspricht, zumindest einen unmittelbaren, präventiven Nutzen: Gelingt es, die Täterschaft durch Strafverfolgung vom Delinquieren abzuhalten, werden weniger Personen geschädigt. Dies gilt umso mehr, wenn es sich um Organisierte Kriminalität handelt und ein ganzes Netzwerk ausgehoben werden kann. Die Strafverfolgung zeigt sich jedoch bei Social Engineering basierten Delikten als eine grosse Herausforderung. Zum einen ist die Täterschaft meist unbekannt und fast nicht zu eruieren, zum anderen erfordert die sehr häufig vorhandene internationale Verortung der Täterschaft eine internationale Zusammenarbeit der Strafverfolgungsbehörden, welche sich teils schwierig und langwierig gestaltet. Nichts desto trotz werden auch in der Strafverfolgung neue Wege beschritten und Erfolge verzeichnet.[43]

Gerade wenn die Schwachstelle Mensch durch die Täterschaft ausgenutzt wird und die technischen Möglichkeiten an ihre Grenzen stossen, kommt man

---

42 De Waard, 5.

43 So wurden vor kurzem die Hintermänner des Phänomens „falscher Polizist" entlarvt und festgenommen, siehe Hans.

nicht ohne die *Einflussnahme auf das Verhalten von (potentiellen) Opfern oder Geschädigten* aus. Die Schwierigkeiten dieses Ansatzpunktes wurden bereits anhand der einführenden Phänomene des Telefonbetrugs, Romance Scams und Online Anlagebetruges sowie den Ausführungen zur unbewussten Verarbeitung von Informationen (System 1) deutlich: Das subjektive Gefühl einer tatsächlichen Bedrohung bleibt bei Social Engineering basierten Phänomenen häufig aus und die Bereitschaft, präventive Massnahmen zu ergreifen, ist gering. Um potentielle Opfer beziehungsweise Geschädigte dennoch zu erreichen, ist eine Kombination auf unterschiedlichen *Präventionsebenen* vielversprechend.

- *Primärprävention*: Massnahmen, die sich an die Allgemeinheit richten.
- *Sekundärprävention*: Massnahmen, die sich an besonders gefährdete Personen richten.
- *Tertiärprävention*: Massnahmen, die sich an bereits geschädigte Personen richten.

Nachfolgend werden die einzelnen Ebenen in Bezug auf Social Engineering basierte Delikte diskutiert, Herausforderungen dargelegt und mögliche neue Wege aufgezeigt. Dabei ist zu beachten, dass die Grenzen zwischen den drei Ebenen fliessend sind.

3. Primärprävention

Das zentrale Element der Primärprävention besteht in der Stärkung des Sicherheitsverhaltens der Bevölkerung. Eine Grundproblematik dabei ist, dass die wenigsten Personen einen Leidensdruck empfinden, es sei denn sie oder eine sehr nahe stehende Person wurden geschädigt. Awareness Kampagnen sind breit angelegte Präventionskampagnen, welche das Ziel haben, die Aufmerksamkeit der Bevölkerung hinsichtlich sicherheitsrelevantem Verhalten zu schärfen. Die Anpassung von Verhalten ist jedoch immer mit Anstrengung und Aufwand verbunden, weshalb Awareness Kampagnen, welche sich alleine auf die Informationsübermittlung stützen, oftmals keine Wirkung zeigen.[44] Bada, Sasse und Nurse haben anhand bestehender Security Awareness Kampagnen untersucht, welche Kampagnen Faktoren hinsichtlich Verhaltensänderung von Bedeutung und welche gar hinderlich sind.[45] Erstes Kernresultat ist, dass das empfohlene Sicherheitsverhalten *leicht umsetzbar* sein muss. Werden beispielsweise dem Ratschlag, starke Passwörter zu verwenden, keine zusätzlichen Informationen (Empfehlung und Anleitung zur Verwendung eines Passwortmanagers oder Ähnliches) hinzugefügt, wird der Ratschlag nicht um-

44 Information Security Report (ISF).

45 Bada/Sasse/Nurse.

gesetzt.[46] Weiter wurde gefunden, dass Verhalten eher geändert wird, wenn *Botschaften positiv formuliert* werden. Die Verwendung von angsteinflössenden Inhalten, wie sie häufig verwendet werden, führt jedoch nicht zur gewünschten Verhaltensänderung und kann gar zu einer Verhaltensblockade führen. Auch Warnmeldungen sind keine effektiven Präventionsstrategien, da sie oftmals keinen Bezug zur Lebenssituation der Zielgruppe aufweisen.[47] Schliesslich muss beachtet werden, dass Awareness Kampagnen mit *wiederholtem Training* und *unmittelbarem Feedback* kombiniert werden sollten, um Verhalten nachhaltig zu ändern. Je leichter der Einstieg in ein Training und je mehr Erfolgserlebnisse zu Beginn eines Trainings gemacht werden, desto eher wird Verhalten verändert.[48]

Praxisansätze, welche diese motivationspsychologischen Komponenten berücksichtigen, jedoch im Bereich der Kriminalprävention noch wenig Anwendung finden, sind Nudging und Gamification. *Nudging* (auf Deutsch: jemandem einen Schubs/einen Denkanstoss geben) ist ein Begriff aus der Verhaltensökonomie und wurde durch Richard Thaler und Cass Sunstein entwickelt. Im Kern geht es darum, erwünschtes Verhalten mental verfügbar und die Umsetzung so einfach wie möglich zu machen.[49] Im Rahmen der Gesundheitsprävention wird dieser Ansatz bereits erfolgreich umgesetzt.[50] Auch im Bereich Littering wurde eine erfolgreiche Kampagne durchgeführt (siehe Abbildung 1). Um Kippen auf der Strasse zu reduzieren, wurden Personen dazu animiert, mittels ihren Kippen über den besten Fussballspieler abzustimmen. Es geht demnach nicht einzig darum, Verhalten mental verfügbarer zu machen, sondern im Idealfall auch so zu auszugestalten, dass Personen Spass am erwünschten Verhalten haben. Eine ähnliche Zielsetzung verfolgen *Gamification-Ansätze*. Als Gamification wird „die Verwendung von Elementen aus Unterhaltungsspielen in einem spielfremden Kontext" verstanden.[51] Der grundlegende Gedanke dahinter besteht darin, Elemente aus dem Spiel in den Lernprozess zu integrieren, um so die Motivation und Leistung zu fördern. Solche Elemente können beispielsweise Online-Quiz, Checklisten, Wettbewerbe oder Ähnliches sein. In Übereinstimmung mit Brown, welcher Faktoren für wirkungsvolle Kampagnen untersuchte, wirken Gamification-Ansätze dann motivations- und leistungsfördernd, wenn die Anwenderin oder der Anwender ein unmittelbares Feed-

46 Siehe dazu auch Coventry et al.

47 Junger/Montoya/Overink, 75.

48 Siehe dazu auch Brown, 193 ff.

49 Thaler/Sunstein.

50 So wird in einer Kantine beispielsweise mehr Obst konsumiert, wenn dieses gut ersichtlich auf Augenhöhe platziert wird.

51 Sailer, 2.

back zu seiner Leistung erhält.[52] Ein Vorteil von Nudging und Gamification Umsetzungen ist zudem die Umsetzungsmöglichkeit im digitalen Raum. Die Online-Präsenz von Kampagnen ist aufgrund der zunehmenden Internetnutzung eine Voraussetzung, um definierte Zielgruppen überhaupt erreichen zu können. Vor dem Hintergrund dieser Erkenntnisse ist von neueren Ansätzen wie Nudging oder Gamification auch für Social Engineering basierte Phänomene ein Mehrwert zu erwarten.[53]

Abbildung 1: Anwendungsbeispiel Nudging im Bereich Littering.

4. Sekundärprävention

Die Sekundärprävention richtet sich an besonders gefährdete Personengruppen. Wie bereits ausgeführt, ist niemand vor Social Engineering Delikten gefeit. Nichts desto trotz gilt es phänomenespezifisch zu eruieren, ob es gewisse Personengruppen gibt, die besonders häufig angegriffen werden und demnach spezifisch aufgeklärt werden müssen. Die Sekundärprävention beschränkt sich jedoch nicht auf das Informieren besonders gefährdeter Personen. Viel-

52 Sailer, 31.

53 Bundesamt für Statistik (BFS).

mehr sollten der betroffenen Person Hilfestellungen angeboten werden, wenn der Angriff bereits gestartet hat. Zu diesem Zeitpunkt ist die betroffene Person empfänglicher für präventive Informationen und Hilfestellungen, da häufig bereits innere Dissonanzen – also Ungereimtheiten, ein mulmiges Bauchgefühl – vorhanden sind und Personen den Drang haben, diese Dissonanzen aufzulösen.[54] Eine aus dem Marketing bekannte Vorgehensweise – die *Customer Journeys* – kann helfen, gezielte Präventionsmassnahmen abzuleiten. Unter dem Begriff Customer Journey versteht man die Reise, die ein Kunde zurücklegt, bis er eine definierte Aktion tätigt. Klassischerweise ist dies der Kauf eines Produktes. Ein Kunde informiert sich vor einem Kauf womöglich im Internet über das Produkt und vergleicht Konkurrenzprodukte, bis er sich schliesslich für oder gegen einen Kauf entscheidet. Gerade wenn diese Recherchen online stattfinden, kann gezielt analysiert werden, an welchen Punkten im Kaufprozess die meisten Personen abspringen und dann versucht werden, diesen heiklen Schritt anders auszugestalten. Die möglichen Einflusspunkte werden dabei als Touchpoints bezeichnet.[55]

Angewendet auf Social Engineering basierte Delikte bedeutet dies in einem ersten Schritt anhand von Fallanalysen die „Reise" einer betroffenen Person – von der Kontaktaufnahme des Social Engineers bis zur Vollendung der Tat, üblicherweise einer Geldübergabe – zu eruieren. In einem zweiten Schritt werden dann die sogenannten Touchpoints ausfindig gemacht. Das Vorgehen eignet sich insbesondere bei online-basierten Delikten, welche sich über einen längeren Zeitraum erstrecken, da über das Internet am meisten Einfluss auf die betroffenen Personen genommen werden kann. Die Umsetzung des Customer Journey Ansatzes erfolgt aktuell auf der Webseite cybercrimepolice.ch, welche durch die Kantonspolizei Zürich betrieben wird. Dabei handelt es sich um eine Informations- und Meldeplattform, welche tagesaktuell bewirtschaftet wird. Die Meldungen von Betroffenen werden in Präventionsbeiträge umgewandelt, so dass andere betroffene Personen, welche aufgrund innerer Dissonanzen im Internet nach Hinweisen suchen, relativ rasch auf die Inhalte von cybercrimepolice.ch gelangen. Die Besucherzahlen und Betroffenheitsmeldungen der Webseite zeigen, dass neu auftretende Phänomene auf diese Art rasch erkannt und unterbrochen werden können. Einschränkend ist darauf hinzuweisen, dass die Plattform cybercrimepolice.ch nur für Phänomene mit Cyberbezug genutzt wird (welche jedoch einen grossen Teil der Social Engineering Phänomene ausmachen). Customer Journeys können ohne weiteres auch für analoge Phänomene verwendet werden. Ein analoger Touchpoint

54 Stroebe, 260.

55 Für eine Übersicht über Customer Journeys siehe z.B. Böven.

für das Phänomen Telefonbetrug wäre beispielsweise der Bankmitarbeitende, welcher die Möglichkeit hat, bei einem allfälligen Geldbezug auf die betroffene Person Einfluss zu nehmen.

5. Tertiärprävention

Die Tertiärprävention ist auch heute noch ein polizeilich wenig abgedecktes Feld, insbesondere was Social Engineering basierte Delikte betrifft. Gerade wenn es sich um psychologisch komplexe Phänomene handelt, die sich über einen längeren Zeitraum erstrecken, ist der Ausstieg aus der Spirale für Betroffene teilweise sehr schwierig. Aktuell werden Betroffene eines Romance Scams im Rahmen der einleitend erwähnten polizeipräventiven Interventionen nicht nur darüber aufgeklärt, dass sie einem Betrug zum Opfer gefallen sind, sondern es werden wenn nötig auch protektive Ressourcen aktiviert. Ein wichtiger Schutzfaktor stellt dabei das Umfeld dar. Idealerweise ist eine Vertrauensperson bei der polizeipräventiven Intervention dabei, um so eine wichtige Wissensgrundlage bezüglich dem Phänomen Romance Scam, aber auch der bestehenden Situation der betroffenen Person zu schaffen.

Im Fokus muss jedoch die psychologische Arbeit stehen – sämtliche Massnahmen nützen nichts, wenn sich die betroffene Person weiterhin in Abhängigkeit des Scammers befindet und immer wieder Geld überweist. Die psychologische Betreuungs- und Überzeugungsarbeit kann nicht alleine polizeiliche Aufgabe sein. Wichtig ist jedoch, dass die Polizei bei der Fallaufnahme um die psychologischen Wirkmechanismen weiss und sich insbesondere bewusst ist, dass sich viele Betroffene – trotz Anzeigeerstattung – nicht als Opfer erkennen (können). Deshalb müssen die Schnittstellen zwischen der Polizei als häufig erste Anlaufstelle und psychologisch spezialisierten Institutionen noch besser definiert werden, so dass eine fallbezogene Zusammenarbeit wirkungsvoll stattfinden kann. Aktuell besteht eine solche Schnittstelle zu einer Selbsthilfegruppe für Opfer von Romance Scam in Winterthur. Wünschenswert wäre zudem eine Schnittstelle zur Opferhilfe. Diese richtet sich gemäss Art. 1 Abs. 1 OHG an Personen, die durch eine Straftat in ihrer körperlichen, psychischen oder sexuellen Integrität unmittelbar beeinträchtigt wurden. Somit greift das OHG für das Phänomen Romance Scam, welches einen Betrug darstellt und sich damit gegen das Vermögen richtet, nicht, es sei denn, dass nebst dem Betrug ein OHG würdiger Tatbestand wie beispielsweise Erpressung, Drohung oder Nötigung herangezogen werden kann. Um die Rapportierung entsprechend dieser Tatbestände ausrichten zu können, wurden spezifische Fragenkataloge für die Fallbearbeitenden entwickelt und im polizeilichen Rapportsystem eingestellt. Eine solch intensive Tertiärprävention findet momentan in keinem anderen Social Engineering basierten Phänomen statt.

VI. Fazit

Im Rahmen des vorliegenden Beitrages wurde anhand der Phänomene Telefonbetrug, Romance Scam und Online Anlagebetrug zunächst die Vielfalt von Social Engineering basierten Delikten aufgezeigt. Dabei ist zu beachten, dass es sich dabei nur um eine sehr kleine und unvollständige Auswahl handelt. Die Gemeinsamkeit aller Social Engineering Phänomene ist die Ausnutzung der Schwachstelle Mensch. Die meisten Personen unterschätzen die Wahrscheinlichkeit, selbst durch Social Engineers manipuliert zu werden. Diese Annahme steht im Widerspruch zu den hohen Betroffenheitszahlen.

Eine allgemeingültige Definition des Begriffs Social Engineering ist nicht vorhanden. Dies hat damit zu tun, dass sich unterschiedliche Disziplinen mit Social Engineering beschäftigen. Auf der einen Seite sind die eher technischen Disziplinen wie Informatikwissenschaften um das Thema bemüht, auf der anderen Seite versuchen die Sozialwissenschaften, insbesondere die Psychologie und Soziologie, einen Beitrag zu leisten. Diese Interdisziplinarität ist einerseits eine Herausforderung für die Forschung, andererseits eine wichtige Grundlage für ein ganzheitliches Verständnis von Social Engineering. Je nach Phänomen sind die technischen Komponenten mehr oder weniger vorhanden. So beinhalten Phishing Attacken zusätzlich zu psychologischen Strategien immer Malware und somit eine technische Komponente, wobei andere Phänomene wie der Telefonbetrug oder Romance Scam ohne diese technischen Komponenten, also durch reine Verhaltensbeeinflussung funktionieren.

In einem weiteren Schritt erfolgte eine Annäherung an mögliche Erklärungen für die weite Verbreitung von Social Engineering Phänomenen und dem Paradox der Unterschätzung der eigenen Viktimisierungswahrscheinlichkeit. Die Psychologie geht davon aus, dass menschliches Verhalten durch die Interaktion von Personen- und Umwelteigenschaften zustande kommt und diese beiden Komponenten durch Social Engineers anvisiert und zur Beeinflussung genutzt werden können.

Hinsichtlich Personeneigenschaften sind empirische Hinweise vorhanden, welche die Wichtigkeit des Konzepts der *Selbstkontrolle* unterstreichen. Wer sein Verhalten gut kontrollieren kann, ist demnach weniger anfällig für Beeinflussungen durch Social Engineers.[56] Für andere persönlichkeitspsychologische Eigenschaften wie den *Big Five* ist aktuell nur wenig und teils widersprüchliche Empirie vorhanden.[57] Dies könnte auf die Vielfalt der untersuchten

[56] Dieser Zusammenhang konnte zumindest für den Bereich der Cyberkriminalität festgestellt werden, siehe Pratt et al., 87 ff.

[57] Van de Weijer/Leukfeldt, 411.

Phänomene zurückzuführen sein. Social Engineering funktioniert jedoch über die Anwendung massgeschneiderter Psychologie, welche deshalb auch sehr differenziert untersucht werden sollte.

Hinsichtlich Umwelteigenschaften konnte gezeigt werden, dass die *zunehmende Online-Präsenz* unserer Gesellschaft ein Risikofaktor zu sein scheint. Auch hier ist weitere Forschung nötig, um beispielsweise Unterschiede in mentalen Sicherheitsmodellen – online versus offline – zu eruieren.

Weiter wurden die Beeinflussungsstrategien der Social Engineers ausgeleuchtet. Grundsätzlich gibt es *zwei Wege der menschlichen Informationsverarbeitung*.[58] Wenn immer möglich, kommt System 1 zum Zuge, deren Verarbeitung ohne bewusste Steuerung und deshalb sehr schnell und mühelos funktioniert. Die Verarbeitung von Informationen über System 2 erfordert hingegen eine bewusste Steuerung: Argumente werden rational verarbeitet, was Zeit und Mühe kostet. Im Alltag funktioniert die Nutzung von System 1 sehr gut: Meistens ist eine sympathische Person auch vertrauenswürdig und ein Produkt zu kaufen, das viele andere Personen nutzen, ist meist keine schlechte Option. Social Engineers versuchen ihre Opfer mit unterschiedlichen Strategien auf das Verarbeitungssystem 1 zu lenken, um auf diese Weise eher zum Ziel zu gelangen. Diese Beeinflussungsstrategien sind vielfältig und noch nicht ausreichend empirisch untersucht. Ein weit diskutierter Ansatz sind jedoch die *Persuasionsstrategien* von Cialdini, welche insbesondere für den Bereich der Werbepsychologie empirisch geprüft wurden und in diesem Praxisbereich Anwendung finden.[59]

Die Prävention von Social Engineering basierten Delikten erfordert eine differenzierte Betrachtung. Zunächst ist ein *systematisches, evidenzbasiertes Vorgehen* von zentraler Bedeutung. Tendenziell wird der differenzierten Analyse eines Phänomens zu wenig Beachtung geschenkt. Eine solche ist jedoch, z.B. im Rahmen eines Monitorings, unabdingbar, um phänomenespezifische Personen- und Umwelteigenschaften und insbesondere Beeinflussungsstrategien der Social Engineers festzustellen. Nur so können spezifische Massnahmen abgeleitet werden.

Es wurde deutlich, dass die Sensibilisierung potentieller Opfer zwar eine grössere Herausforderung darstellt, als Situationskomponenten zu verändern (beispielsweise die Umsetzung technischer Massnahmen), dies jedoch häufig die einzige Präventionsmöglichkeit darstellt. Vielversprechend ist dabei die Kombination unterschiedlicher Ebenen. Auf primärpräventiver Ebene, also der

---

58 Kahnemann.

59 Steinmetz/Goe/Pimentel, 173 ff., Archer, Quiel.

Sensibilisierung aller potentiellen Opfer, kann die Wichtigkeit neuerer aus dem Marketing bekannter Ansätze wie *Nudging* oder *Gamification* unterstrichen werden. Diese Ansätze zielen nicht alleine auf die Informationsübermittlung, sondern zusätzlich auf die Motivation der Personen, sich überhaupt mit einer Thematik auseinanderzusetzen. Nur wenn die Motivation gegeben ist, wird der anstrengende Weg einer Verhaltensänderung in Angriff genommen. Auch im Bereich der Sekundärprävention versprechen Ansätze aus dem Marketing, z.B. *Customer Journeys*, Wirkung.[60] Dabei wird versucht, die Dissonanzen (innere Ungereimtheiten) von Personen zum richtigen Zeitpunkt (meist wenn bereits ein Angriff erfolgte) und über den passenden Kanal (häufig das Internet) aufzulösen. Der Tertiärprävention kommt bei länger andauernden und emotional komplexen Social Engineering Phänomenen eine wichtige Rolle zu. Zentral ist dabei die Vernetzung mit Partnerorganisationen, welche von Phänomen zu Phänomen zu definieren sind.

Angesichts des technischen Fortschritts ist davon auszugehen, dass uns das Hacking der menschlichen Psyche je länger je stärker beschäftigen wird. Umso wichtiger scheint es, die noch wenig vorhandene Forschung zur Ausnutzung der Schwachstelle Mensch, der Beeinflussungsstrategien von Tätern und der Prävention voranzutreiben. Für den Erfolg scheint sowohl die Interdisziplinarität als auch der Austausch zwischen Wissenschaft und Praxis entscheidend zu sein.

[60] Böven.

Literaturverzeichnis

Allport Gordon W., The historical background of modern social psychology, in: Lindzey Gardner (Hrsg.), handbook of social psychology, 2. A., London 1954, 3 ff.

Archer Aaron, „I made a choice“: exploring the persuasion tactics used by online romance scammers in light if Cialdini's compliance principles, Regis University 2017.

Asendorpf Jens B., Persönlichkeitspsychologie, 4. A., Berlin 2019.

Bada Maria/Sasse Angela M./Nurse Jason R.C., cyber security awareness campaigns – why do they fail to change behavior?, Global Cyber Security Capacity Centre, 2014, <https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf>

Brown Stephan L., emotive health advertising and message resistance, Australian Psychologist 2001, 193 ff.

Böven Elisa, Customer Journey und User Experience in der Anwendungsentwicklung, Wien 2020.

Cohen Lawrence E./Felson Marcus, social change and crime rate trends: a routine activity approach, American Sociological Review 1979, 588 ff.

Coventry Lynne et al., using behavioral insights to improve the public's use of cyber security best practices, 2014, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf.

Clarke Ronald V., seven misconceptions of situational crime prevention, in: Tilley Nick (Hrsg.), handbook of crime prevention and community safety, London 2005, 39 ff.

de Waard Jaap, what works? a systematic overview of recently published meta evaluations, synthesis studies within the knowledge domains of Situational Crime Prevention, Policing, and Criminal Justice Interventions, 1997–2019. <https://www.researchgate.net/publication/320519021_What_Works_A_systematic_overview_of_recently_published_meta_evaluations_synthesis_studies_within_the_knowledge_domains_of_Situational_Crime_Prevention_Policing_and_Criminal_Justice_Interventions_1997->.

Eck John E./Spelman William, problem-solving: problem-oriented policing in newport news, Washington, D.C. 1982.

Eckardt Georg, Sozialpsychologie – Quellen zu ihrer Entstehung und Entwicklung, Wiesbaden 2015.

gfs-zürich, Sicherheit im Internet, 2019, <https://www.satw.ch/fileadmin/user_upload/documents/04_Footer/03_Medien/01_Medienmitteilungen/Bevoelkerungsumfrage_Sicherheit-im-Internet_Schlussbericht_2019_03_18.pdf>.

Gottfredson Michael R./Hirschi Travis, a general theory of crime, Stanford 1990.

Hans Julian, Mutmaßlicher Senioren-Betrüger in der Türkei festgenommen, Süddeutsche Zeitung vom 3. Dezember 2020, <https://www.sueddeutsche.de/muenchen/tuerkei-razzia-falsche-polizisten-muenchen-1.5136061>.

Habermeyer Elmar/Guldimann Angela, Opfer aus Überforderung – zur Bedeutung abnehmender geistiger Fähigkeiten für die Opferwerdung von älteren Menschen, in: Schwarzenegger Christian/Nägeli Rolf (Hrsg.), 6. Zürcher Präventionsforum – ältere Menschen und ihre Erfahrungen mit der Kriminalität, Zürich 2013, 25 ff.

Hegemann Lisa, Ohne Netz, Zeit Online vom 29. Oktober 2019, <https://www.zeit.de/digital/internet/2019-10/50-jahre-internet-digitalisierung-vernetzung-echtzeit-innovation?utm_referrer=https://www.google.com/>.

Holtfreter Kristy/Reisig Michael D./Pratt Travis C., low self-control, routine activities, and fraud victimization, Criminology 2008, 189 ff.

Information Security Forum (ISF), from promoting awareness to embedding behaviours, 2014, <https://www.security-finder.ch/fileadmin/dateien/pdf/news/ISFReportAwarenesstoEmbeddingBehaviours.pdf>.

Junger Marianne/Montoya Lorena/Overink F.J., priming and warnings are not effective to prevent social engineering attacks, Computers in human behavior 2017, 75 ff.

Kahnemann Daniel, schnelles Denken, langsames Denken, 18. A., Berlin 2012.

Koziarski Jacek/Lee Jin Ree, connecting evidence-based policing and cybercrime, Policing: An International Journal 2020, 198 ff.

Loewe-Baur Mirjam/Eggli Daniel, Telefonbetrug: Erkenntnisse aus Opferinterviews und Prävention, Kriminalistik 2019, 163 ff.

Marx Konstanze/Rüdiger Thomas-Gabriel, Romancescamming: Eine kriminologisch-linguistische Betrachtung, Kriminalistik 2017, 211 ff.

Nationales Zentrum für Cybersicherheit, Social Engineering – lassen Sie sich nicht ausfragen, <https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/bundesinterne-kampagnen/social_engineering.html>.

Pratt Travis C. et al., self-control and victimization: a meta-analysis, Criminology 2014, 87 ff.

Quiel Susanne, social engineering in the context of Cialdini's psychology of persuasion and personality traits, Hamburg University of Technology 2013.

Sailer Michael, die Wirkung von gamification auf Motivation und Leistung, Wiesbaden 2016.

Schaab, Peter/Beckers, Kristian/Pape, Sebastian, a systematic gap analysis of social engineering defence mechanisms considering social psychology, proceedings of the tenth international symposium on Human Aspects of Information Security & Assurance (HAISA) 2016, 241 ff. <https://pape.science/paper/SBP16haisa/>.

Scott, Michael S./Kirby Stuart, implementing POP: leading, structuring and managing a problem-oriented police agency, Washington, DC 2012.

Schopp Florian/Baumgartner Fabian, „Okay, Sie haben Angst", sagt Klaus, „wenn man eine erste Investition macht, fühlt es sich immer so an." – mit welchen Tricks uns Anlagebetrüger in die Falle locken wollen, NZZ vom 27. Juli 2020, <https://www.nzz.ch/zuerich/bitcoin-betrug-wie-uns-kriminelle-in-die-falle-locken-wollen-ld.1567753>.

Schreck Christopher J., criminal victimization and low self-control: an extension and test of a general theory of crime, Justice Quarterly 1999, 633 ff.

Schwanebeck Axel, Gefangen im Netz – medialer Wandel und kontinuierliche Überwachung in digitalen Welten, in: Schröder Michael/Schwanebeck Axel (Hrsg.), Big Data – In den Fängen der Datenkraken, 2. A., Baden Baden 2019, 11 ff.

Steinmetz Kevin/Goe Richard/Pimentel Alexandra, on social engineering, in: Leukfeldt Rutger/Holt Thomas J. (Hrsg.), the human factor of cybercrime, London 2020, 173 ff.

Stroebe Wolfgang, Strategien zur Einstellungs- und Verhaltensänderung, in: Jonas Klaus/Stroebe Wolfgang/Hewstone Miles (Hrsg.), Sozialpsychologie, 6. A., Berlin 2014, 231 ff.

Thaler Richard H./Sunstein Cass R., nudge, 16. A., Berlin 2010.

Tversky Amos/Kahnemann Daniel, judgment under uncertainty: heuristics and biases, Science 1974, 1124 ff.

Van de Weijer Steve G.A./Leukfeldt E. Rutger, big five personality traits of cybercrime victims, Cyberpsychology, Behavior, and Social Networking 2017, 407 ff.

Van Gelder Jean-Louis/De Vries Reinout E., traits and states: integrating personality and affect into a model of criminal decision making, Criminology 2012, 637 ff.

Wang Zuoguang/Zhu Hongsong/Sun Limin, social engineering in cybersecurity: effect mechanisms, human vulnerabilities and attack methods, IEEE Access 2021, 11895ff. <https://ieeexplore.ieee.org/document/9323026>.

Wang Zuoguang/Sun Limin/Zhu Hongsong, defining social engineering in cybersecurity, IEEE Access 2020, 85094ff. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9087851>.

Weber Silvana/Knorr Elena, kognitive Verzerrungen und die Irrationalität des Denkens, in: Appel Markus (Hrsg.), die Psychologie des Postfaktischen, Berlin 2020, 103 ff.

Whitty Monica T., do you love me, psychological characteristics of romance scam victims, Cyberpsychology, Behavior, and Social Networking 2018, 105 ff.

Workman Michael, wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security, Journal of the Association for Information Science and Technology 2007, 662 ff.

Online-Sicherheit – Sichere Passwörter & Co.

Oliver Hirschi

Inhalt

I. Einleitung

In der fortschreitenden Digitalisierung werden immer mehr Daten bearbeitet, übertragen und gespeichert, welche geschützt werden müssen. Die Daten liegen auf lokalen Datenträgern oder im Netzwerk und der Cloud. Zum Schutz der Zugänge zu diesen Daten und der Daten selbst, werden vielfach Passwörter eingesetzt.

Die Passwort-Thematik ist ein zweischneidiges Schwert: Auf der einen Seite ein wichtiges Sicherheitselement, auf der anderen Seite ein viel geschasstes Thema aufgrund unzuträglicher Usability. Nichtsdestotrotz sind Passwörter nach wie vor die gängigsten und am meisten verwendeten Schlüssel im digitalen Zeitalter. Sie schützen den Zugriff auf sensible und private Daten.

Die Authentifizierung, beispielsweise bei einem Internetdienstleister erfolgt in der Regel mittels Benutzername oder E-Mail-Adresse und einem Passwort. Das Passwort ist zwar in vielen Fällen nicht mehr das einzige, aber dennoch ein sehr wichtiges Sicherheitselement.

II. Anwendungsbereiche

Passwörter werden primär in zwei Bereichen eingesetzt. Einerseits bei Logins, beispielsweise als Geräteschutz und sehr oft als Zugangsschutz zu Betriebssystemen, Anwendungen und Online-Diensten. In all diesen Fällen erfolgt die Passwortprüfung in der Regel über eine sogenannte Hashfunktion und Hashwert (mehr dazu findet sich im nachfolgenden Kapitel). Andererseits werden Verschlüsselungen (z.B. einzelne Dokumente oder komplette Datenträger) sehr oft mittels Passwörtern geschützt. Hierbei schützt das Passwort entweder direkt den Verschlüsselungsschlüssel oder es dient für die Schlüsselerzeugung.

III. Herausforderungen

Bei der Anwendung von Passwörtern als Sicherheitselement gilt es verschiedenen Herausforderungen zu begegnen, sei es bei der Aufbewahrung/Speicherung, der Übertragung bis hin zur Erzeugung sicherer Passwörter.

1. Hashwerte und Hashfunktionen

Passwörter werden grundsätzlich nicht in Klartext gespeichert, das wäre sehr fahrlässig, sondern als sogenannte *Hashwerte*. Dies, damit niemand ausser dem Benutzer selbst das Passwort kennt – auch der Anbieter/Dienstleister nicht – und das Passwort nicht einfach so gestohlen und missbraucht werden kann.

Hashfunktionen sind sogenannte Einwegfunktionen und dienen dazu einen Text beliebiger Länge (beispielsweise ein Passwort als Input) auf eine „kurze" Zeichenfolge (Hashwert als Output) einer fixen Länge zu transformieren.

Nachfolgende Abbildung zeigt eine vereinfachte Hashfunktion (moderne Hashfunktionen werden in der Regel zusätzlich mit einem sogenannten Salz angereichert, was aber fürs einfachere Verständnis hier vernachlässigt wird).

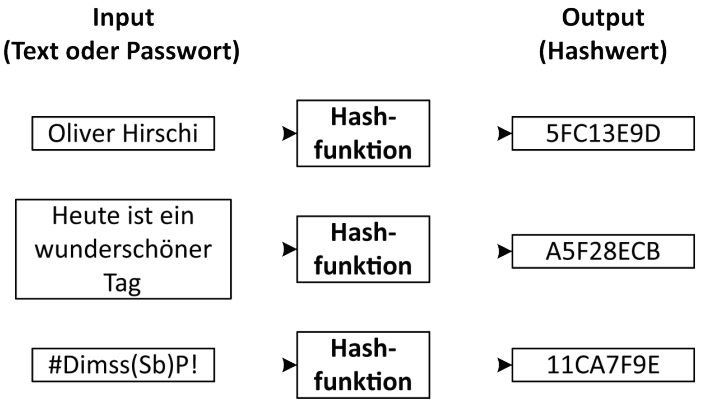


Abbildung 1 – Hashwerte und -funktionen

An Hashwerte und -funktionen werden ganz bestimmte Anforderungen gestellt. Eindeutigkeit, Reversibilität und Kollisionsresistenz stehen dabei im Zentrum:

- **Eindeutigkeit**
  Eine identische Zeichenfolge (Input) soll immer zum selben Hashwert (Output) führen.
- **Reversibilität**
  Der Hashwert (Output) soll nicht in die ursprüngliche Zeichenfolge (Input) zurückberechnet werden können.
- **Kollisionsresistenz**
  Zwei unterschiedliche Zeichenfolgen (Input) sollen nicht den gleichen Hashwert (Output) ergeben.

Sowohl beim Setzen eines Passwortes, als auch beim Authentifizieren wird das eingegebene Passwort durch die Hashfunktion geschleust und entweder abgespeichert (Setzen eines neuen Passwortes) oder mit dem bereits gespeicherten Hashwert überprüft – stimmt dieser überein, hat der Benutzer das korrekte Passwort eingegeben.

2. Angriffe auf Passwörter

Wird die Sicht der Angreifer eingenommen, stellt sich die Frage, wie diese an Passwörter gelangen.

Eine bekannte und sehr weit verbreitete Methode ist das sogenannte *Phishing*, wobei das Passwort beim Opfer direkt „abgefragt" wird (üblicherweise per E-Mail): „Mittels Phishing versuchen Angreifer an Zugangsdaten ahnungsloser Internetbenutzer z.B. zum E-Banking oder zu Online-Shops zu gelangen. Die Täter täuschen dabei eine falsche Identität vor und nutzen so die Gutgläubigkeit ihrer Opfer aus."[1]. Weiter kann ein Angreifer, insbesondere im Mobile-Zeitalter relevant, die Passworteingabe physisch beobachten (sogenanntes *Shoulder Surfing*). Die Abwehrmassnahme dieser beiden Angriffsmethoden ist nicht technischer, sondern menschlicher Natur – das Benutzerverhalten: Der Benutzer ist dafür besorgt, dass er das Passwort nur auf der Website des echten Anbieters eingibt und er dabei nicht beobachtet wird.

Es ist weiter möglich, den Datenverkehr beim Übertragen des Passwortes zum Dienstleister auszuspähen und so das übertragene Passwort mitzulesen (sogenanntes *Sniffing*). Hier hilft als Abwehrmassnahme eine verschlüsselte Datenübertragen mittels TLS/SSL-Protokoll.

Eine weitere, stark verbreitete Methode ist das *Passwort-Hacking*. Dabei werden zuvor beim Dienstleister gestohlene Hashwerte (siehe vorangegangenes Kapitel) gehackt. Brute Force ist dabei nebst weiteren (Wörterbuchangriff und Rainbow Tables hier als Randnotiz) die am weitesten verbreitete Angriffsart.

Beim *Brute Force Angriff* werden alle möglichen Passwort-Kombinationen durchprobiert, bei einem einfachen (enthält nur Zahlen und Kleinbuchstaben) 8-stelligen Passwort z.B. von 00000000 über 9999zzzz bis zzzzzzzz.

Die nachfolgende Tabelle zeigt wie lange es dauert bis ein Passwort mit entsprechender Länge und Komplexität geknackt wird. Als Berechnungsgrundlage wurde eine optimistische (nicht alle Hashfunktionen sind gleich performant), aber für gewisse Hashfunktionen realistische Annahme von 100 Milliarden Versuche pro Sekunde herangezogen.

[1] <www.ebas.ch/phishing>.

Wie lange dauert es bis ein Passwort gehackt wird?

Anzahl Zeichen	Nur Zahlen	Nur Klein- oder nur Grossbuchstaben	Zahlen, Gross- und Kleinbuchstaben	Zahlen, Gross- und Kleinbuchstaben, Sonderzeichen
	10	26	62	95
4	0 Sek.	0 Sek.	0 Sek.	0 Sek.
5	0 Sek.	0 Sek.	0 Sek.	0 Sek.
6	0 Sek.	0 Sek.	1 Sek.	7 Sek.
7	0 Sek.	0 Sek.	35 Sek.	12 Min.
8	0 Sek.	2 Sek.	36 Min.	18 Std.
9	0 Sek.	54 Sek.	38 Std.	73 Tage
10	0 Sek.	24 Min.	97 Tage	19 Jahre
11	1 Sek.	10 Std.	17 Jahre	1804 Jahre
12	10 Sek.	11 Tage	1023 Jahre	171347 Jahre
13	2 Min.	287 Tage	63429 Jahre	16277971 Jahre
14	17 Min.	20 Jahre	3932575 Jahre	1546407214 Jahre
15	3 Std.	532 Jahre	243819668 Jahre	146908685363 Jahre
16	1 Tage	13828 Jahre	15116819415 Jahre	13956325109455 Jahre
17	12 Tage	359534 Jahre	937242803724 Jahre	1325850885398200 Jahre
18	116 Tage	9347891 Jahre	58109053830869 Jahre	125955834112829000 Jahre
19	3 Jahre	243045175 Jahre	3602761337513900 Jahre	11965804240718800000 Jahre
20	32 Jahre	6319174561 Jahre	223371202925862000 Jahre	113675140286828000000 Jahre

Abbildung 2 – Wie lange dauert es bis ein Passwort mittels Brute Force gehackt ist?

Die Abwehrmassnahme gegen Brute Force Angriffe auf Benutzerseite ist die Verwendung starker Passwörter. Bereits die „19 Jahre“ für ein komplexes 10-stelliges Passwort scheinen sicher genug. Es gilt allerdings zu beachten, dass im Zeitalter des Cloud-Computings verteilte und damit effiziente Berechnungen in der Cloud möglich sind – deshalb die aktuelle Empfehlung der Mindestlänge von zwölf Stellen.

Immer wieder werden Tausende, Millionen Passwort-Hashes gestohlen und anschliessend mittels verschiedener Methoden geknackt (sogenannte Password Breaches). Auf der kostenlosen Website „Have I Been Pwned“ (https://haveibeenpwned.com) sind etliche solche gehackten Passwortlisten hinterlegt und es kann eruiert werden, ob Login-Daten zu einem Online-Konto kompromittiert oder bei einer Datenpanne veröffentlicht wurden.

IV. Sichere Passwörter

Das Hasso-Plattner-Institut (HPI)[2] publiziert jährlich die beliebtesten deutschen Passwörter. Für das Jahr 2020 wurden als Datengrundlage 3.1 Millionen Zugangsdaten aus dem Datenbestand des HPI Identity Leak Checkers analysiert, welche auf E-Mail-Adressen mit .de-Domäne registriert sind und 2020 geleakt wurden. Auf den Plätzen eins bis fünf der beliebtesten Passwörter stehen „123456“, „123456789“, „passwort“, „hallo123“ und „12345678“.[3] Und auch auf den weiteren Plätzen wird es nicht viel kreativer, sprich sicherer.

2 <https://hpi.de>.

3 <https://hpi.de/news/jahrgaenge/2020/die-beliebtesten-deutschen-passwoerter-2020-platz-6-diesmal-ichliebedich.html>.

1. Anforderungen

Wie sich ein starkes Passwort zusammensetzt, hat sich im Verlauf der Zeit immer wieder geändert und die Regeln für ein sicheres Passwort wurden jeweils den neusten Gegebenheiten angepasst. Wo vor rund zehn Jahren noch 8-stellige und vor rund fünf Jahren 10-stellige Passwörter als sicher galten, werden heute mindestens zwölf Stellen gefordert. Dies insbesondere aufgrund immer performanteren Technologien, welche zum Hacken von Passwörtern eingesetzt werden.

Verdeutlicht wird dies mit folgendem kleinen Rechenbeispiel: Ein einfaches, 6-stelliges Passwort, welches aus lediglich Kleinbuchstaben und Zahlen besteht ist mit jedem handelsüblichen Notebook innert Minuten knackbar. Für ein komplexes, 12-stelliges Passwort, welches aus Klein-, Grossbuchstaben, Zahlen und Sonderzeichen besteht werden hingegen tausende von Jahren benötigt.

Aus heutiger Sicht gelten nachfolgende sechs Regeln zum sicheren Passwort – verwenden Sie…[4]

- mindestens 12 Zeichen
- Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen
- keine Tastaturfolgen wie z.B. „asdfgh“ oder „45678“
- kein Wort einer bekannten Sprache, d. h. das Passwort sollte keinen Sinn ergeben und in keinem Wörterbuch vorkommen
- überall ein anderes Passwort
- speichern Sie Ihr Passwort nicht unverschlüsselt ab

2. Generierung

Für jeden Dienst unterschiedliche und gleichzeitig starke Passwörter zu verwenden stellt eine Herausforderung dar. Nachfolgende zwei Tipps zum Umgang mit Passwörter helfen dabei: Merksatz und Passwort-Tresor.

Mittels eines *Merksatzes*, den man sich gut merken kann, bildet sich mit den jeweiligen Anfangsbuchstaben sowie Ziffern und Satzzeichen das Passwort:

- „**M**eine **T**ochter **T**amara **M**eier **h**at **a**m **J**anuar **G**eburtstag**!**“
- So entsteht ein starkes Passwort aus einer beliebigen Zeichenfolge, das Sie sich gut merken können:
  „**MTTMha19.JG!**“

[4] <www.ebas.ch/step4>.

Um auch für jeden Dienst ein unterschiedliches Passwort zu verwenden, kann beispielsweise irgendwo im Passwort aus dem Merksatz z.B. die ersten zwei oder drei Buchstaben des Anbieters integriert werden – für den LinkedIn-Zugang entstünde mit obenstehenden Merksatz dann beispielsweise das Passwort „MTTMhaLi19.JG!".

Mit einem *Passwort-Tresor* (auch Passwort-Manager genannt) können automatisch beliebig lange und starke Passwörter generiert und diese auf sichere Art und Weise (verschlüsselt) gespeichert werden. Ein weiterer Vorteil: Man muss sich lediglich noch ein Passwort merken – das starke Passwort zum Öffnen des Tresors.

V. Erweiterte Authentifizierung

Im Bankenumfeld ist die Multi-/Zwei Faktor Authentifizierung (MFA/2FA) schon längst nicht mehr wegzudenken. Zusätzliche zu einem starken Passwort sorgt sie für noch mehr Sicherheit.

Bei der Multi-/Zwei Faktor Authentifizierung wird zusätzlich zum ersten Sicherheitselement (meistens ein Passwort) ein zweites, unabhängiges Sicherheitselement abgefragt. Mögliche Faktoren sind die drei Bereiche *Wissen* (etwas, das der Benutzer weiss), *Haben* (etwas, das nur der Benutzer besitzt) und *Sein* (etwas, das der Benutzer ist). In der Praxis werden sie beispielsweise wie folgt umgesetzt:

- **Wissen**
  Passwort, PIN, Sicherheitsfrage, …
- **Haben**
  Chip-Karte, Schlüssel, Mobiltelefon, Zertifikat, …
- **Sein**
  Fingerabdruck, Gesichtserkennung, Spracherkennung, …

Mittlerweile bieten nebst Banken auch viele weitere Online-Dienstleister (z.B. Google, Facebook) eine Zwei-Faktor-Authentifizierung an.

VI. Ausblick

Wie sieht die Zukunft der Passwörter als Sicherheitselement aus? Hoffentlich nicht 14-, 16- oder gar 18-stellige Passwörter. Die Herausforderung einer sicheren und benutzerfreundlichen Authentifizierung ist gross. Es gibt verschiedene Bestrebungen, Passwörter überflüssig zu machen, allerdings ist *die Lö-*

sung noch nicht gefunden. Der FIDO2 Standard der FIDO Alliance[5] hat sich (noch) nicht durchgesetzt, vielleicht könnte auch das allgegenwärtige Smartphone und/oder die Mobile-Nummer genutzt werden, oder etwas ganz anderes/neues.

Bis dahin gilt es starke Passwörter zu erstellen, verwenden und verwalten, um die Zugänge und Daten bestmöglich zu schützen.

[5] <https://fidoalliance.org>.

Wandel der Kriminalität in den letzten 20 Jahren: Von offline zu online?

Nora Markwalder

Inhalt

I. Einleitung

Die im März 2021 veröffentlichte polizeiliche Kriminalstatistik der Schweiz hat für das Jahr 2020 im Bereich der Delikte gegen das Strafgesetzbuch einen Rückgang der Kriminalität von insgesamt 2.4% im Vergleich zum Vorjahr ausgewiesen. Damit wird der rückläufige Trend fortgesetzt, der in der Schweiz seit 2012 beobachtet werden kann.[1] Sinkende Kriminalitätstrends lassen sich aber nicht nur in der Schweiz, sondern auch in den umliegenden europäischen Ländern sowie in weiteren westlichen Industrienationen wie etwa den USA oder Kanada beobachten.[2] In den USA zeigte sich diese Entwicklung bereits zu Beginn der 1990er Jahre, weshalb dort in den letzten 20 Jahren verschiedene Theorien entwickelt wurden, um das Phänomen des „Crime Drop" zu erklären.[3] So wurden etwa demographischen Überlegungen angeführt, näm-

1 Bundesamt für Statistik (BFS), Strafgesetzbuch (StGB): Straftaten und beschuldigte Personen, abrufbar unter https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/polizei/straftaten.assetdetail.15844440.html.

2 Farrell/Tilley/Tseloni, 424 ff.; Rosenfeld/Weisburd, 329 ff.; Aebi/ Linde, 251 ff.; Caneppele/ Aebi, 67.

3 Für eine Übersicht über bestehende Erklärungsansätze siehe Farrell/Tilley/Tseloni, 438.

lich dass eine sinkende Geburtenrate ab 1970 zu geburtenschwächeren Kohorten und demnach zu weniger jungen Delinquenten geführt habe.[4] Des Weiteren wurden ein Rückgang des illegalen Drogenmarktes, wirtschaftlich positive Entwicklungen in den USA sowie spezifische Regulierungen (wie z.B. schärfere Waffengesetze, die Todesstrafe, eine vermehrte Inhaftierung von Straftätern, die Legalisierung von Abtreibungen oder auch verbesserte Polizeistrategien) als Gründe für den „Crime Drop" genannt – wobei zu Recht kritisiert wird, dass diese US-spezifischen Gegebenheiten in sämtlichen anderen Ländern, die ebenfalls einen Rückgang der Kriminalität aufweisen, nicht vorhanden waren und somit nicht als Erklärung für den allgemeinen Rückgang der Kriminalität in westlichen Industrienationen dienen können.[5] Als weiterer Grund wurden verbesserte Sicherheitsmassnahmen wie z.B. Diebstahlsicherungen bei Autos oder das vermehrte Aufkommen von privaten Sicherheitsdiensten, sowie veränderte Lebensgewohnheiten genannt.[6] Solche situativen Veränderungen können Gelegenheiten für Delikte reduzieren bzw. das Risiko für Straftäter erhöhen oder dazu führen, dass sich gewisse Delikte in den Online-Raum verlagern.[7] Als makrotheoretische Grundlage für die Erklärung solcher Verlagerungseffekte kann die Breschentheorie hinzugezogen werden, wonach die Digitalisierung neue Sicherheitslücken (sog. „Breschen") geschaffen hat, welche sich Kriminelle zunutze machen, solange sie nicht mittels neuer Sicherungsmethoden geschlossen werden.[8] Auf individueller Handlungsebene kann die Ausnützung neuer Gelegenheitsstrukturen mit dem „Routine-Activities-Ansatz" erklärt werden, wonach eine Straftat begangen wird, wenn ein potenzieller Täter auf ein geeignetes Tatobjekt trifft und dieses nicht geschützt ist.[9] Das Internet und die Digitalisierung bieten demnach vielfältige, neue Gelegenheiten zur Deliktsbegehung und attraktive Tatobjekte, welche oftmals nicht ausreichend geschützt sind, weshalb diesbezüglich eigentlich von einer Zunahme der Kriminalität ausgegangen werden müsste. Gewisse Autoren erklären den Rückgang der Kriminalität daher zumindest teilweise damit, dass Verschiebungen von Delikten in den Online-Raum stattgefunden hätten, die durch offizielle Kriminalitätsstatistiken nicht richtig erfasst worden seien – so dass der „Crime Drop" demnach zumindest teilweise durch einen „Crime Recording Flop" bei den Cyberdelikten erklärt werden könne.[10]

---

4 Farrell/Tilley/Tseloni, 452 f.

5 Farrell/Tilley/Tseloni, 438 ff.

6 Farrell/Tilley/Tseloni, 455 f.; Caneppele/Aebi, 67.

7 Farrell/Tilley/Tseloni, 455 f.; Caneppele/Aebi, 67 ff.

8 Zur Breschentheorie siehe Killias, 11 f.

9 Cohen/Felson, 598.

10 Caneppele/Aebi, 75 f.

Der vorliegende Beitrag bezweckt die Beantwortung der Frage, wie sich die Kriminalität im Zuge der Digitalisierung in der Schweiz entwickelt hat. Dazu werden zunächst die Kriminalitätstrends in der Schweiz in den letzten 20 Jahren analysiert, und zwar mittels offizieller Statistiken und verfügbarer Dunkelfelddaten. Danach wird anhand sämtlicher erhältlicher Indikatoren auf die Frage nach den Digitalisierungstendenzen in der Kriminalität eingegangen, wobei neben der Entwicklung der eigentlichen Cyberdelikte vor allem auf eine Verschiebung des Modus Operandi von ehemals klassischen „Offline-Delikten" in den Online-Bereich fokussiert wird. Der Beitrag interessiert sich also nicht nur für Cyberdelikte im engeren Sinn – sprich all jene Delikte, deren Tatbestandsmässigkeit das Nutzen von Daten resp. eines Netzwerks beinhalten (sog. Computerdelikte) – sondern versteht unter der Cyberkriminalität sämtliche Straftaten, die im digitalen Raum bzw. mittels digitaler Hilfsmittel begangen werden (sog. Cyberdelikte im weiteren Sinn).[11]

II. Entwicklung der Kriminalität im Hell- und Dunkelfeld

1. Messinstrumente der Kriminalitätsentwicklung

Für die Messung von Kriminalität und deren Entwicklung stehen verschiedene Indikatoren zur Verfügung. Am häufigsten werden hierfür offizielle Statistiken wie polizeiliche Kriminalstatistiken, Urteilsstatistiken oder Vollzugsstatistiken verwendet.[12] Offizielle Kriminalstatistiken eignen sich besonders gut für die Beobachtung der Kriminalitätsentwicklung, wenn sie bereits einen längeren Zeitraum zurückreichen und jährlich aufdatiert werden. Grundvoraussetzung für die Validität dieser Statistiken ist allerdings, dass sich die Erhebungsmethode im Laufe der Zeit nicht ändert.[13] Ein gewichtiger Nachteil der Kriminalitätsstatistiken besteht aber darin, dass sie nur polizeilich bekannte Delikte umfassen und somit keine Auskunft über das wirkliche Ausmass der Kriminalität geben können. Die sog. Dunkelziffer, sprich sämtliche nicht entdeckte oder

---

11 Vgl. auch Isenring/Maybud/Quiblier, 440; Gyarmati, 87; Caneppele/Aebi, 69 f.; für die Definition der Cyberkriminalität im weiteren Sinn siehe auch Bundesamt für Statistik (BFS,) Digitale Kriminalität, 2021, <https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/polizei/digitale-kriminalitaet.assetdetail.16244808.html>.

12 Für einen Überblick über die offiziellen Kriminalstatistiken siehe Bundesamt für Statistik (BFS), Kriminalität und Strafrecht, <https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht.html>. Zu den Kriminalstatistiken siehe auch Killias/Aebi/Kuhn, Rz. 76 ff.

13 Die polizeiliche Kriminalstatistik in der Schweiz wurde im Jahre 2009 revidiert und die Erfassungsweise der Delikte vereinheitlicht, weshalb Daten vor 2009 nicht unbedingt vergleichbar sind. Dies muss auch für die nachfolgenden Analysen berücksichtigt werden.

nicht zur Kenntnis der Polizei gebrachte Delikte, werden damit nicht erfasst. Um dieses Dunkelfeld zu messen, sind Opferbefragungen nötig, welche mittels einer für ein gewisses Gebiet oder Land repräsentativen Bevölkerungsstichprobe die Viktimisierungserfahrung der allgemeinen Bevölkerung abfragen.[14] Solche gesamtschweizerischen Opferbefragungen existieren seit 1984/86 und erlauben daher, auch die Entwicklung der Kriminalität im Dunkelfeld über die letzten Jahrzehnte zu beobachten.[15]

2. Entwicklungen im Hellfeld

Schaut man sich nun die Entwicklung der Kriminalität in der Schweiz anhand der polizeilichen Kriminalstatistik des Bundesamtes für Statistik (BFS) an, so kann insgesamt ein Rückgang der Anzahl begangener Delikte in den letzten 20 Jahren festgestellt werden. Allerdings ist die Gesamtmenge der Straftaten sehr stark abhängig von einzelnen, häufig vorkommenden Delikten wie etwa dem Diebstahl, weshalb eine Analyse der Entwicklung einzelner Deliktsgruppen sinnvoller erscheint.

Im Bereich der Delikte gegen Leib und Leben kann zunächst ein deutlicher Rückgang bei den vollendeten Tötungsdelikten festgestellt werden. Diese sind im Vergleich zum Niveau in den 1980er und 1990er Jahren um rund die Hälfte zurückgegangen. Dieser Rückgang ist nicht nur in der Schweiz, sondern auch in umliegenden europäischen Ländern zu beobachten.[16] Bemerkenswert ist aber, dass die versuchten Tötungen in der Schweiz wie auch in anderen europäischen Ländern gleichzeitig stark zugenommen haben. Als Erklärung für diesen Trend wird neben anderen Faktoren vermutet, dass eine bessere medizinischen Versorgung einen Einfluss auf die Sterblichkeit bei Tötungsdelikten haben könnte und somit die Anzahl der vollendeten Tötungsdelikte gesunken und diejenige der versuchten Tötungsdelikte gestiegen ist, weil mehr Personen auch bei schweren Verletzungen gerettet werden können.[17] Eine abnehmende Tendenz lässt sich in der Schweiz ab 2009 aber auch bei den Körperverletzungen feststellen, nachdem zuvor eine Zunahme verzeichnet worden war.

Bei den Vermögensdelikten ist insb. die deutliche Abnahme von Diebstählen augenfällig. Weil diese wie erwähnt einen grossen Teil vom Gesamtvolumen der Kriminalität ausmachen, hat die Kriminalität in der Schweiz in den letzten Jahren auch analog zur Entwicklung beim Diebstahl insgesamt abgenommen.

---

14 Killias/Aebi/Kuhn, Rz. 101.

15 Für einen Überblick über die Kriminalitätsbefragungen in der Schweiz siehe Biberstein et al., 45 ff.; Killias/Haymoz/Lamon, 13 f.

16 Siehe dazu Suonpää et al. (in Vorb.).

17 Siehe dazu Linde, 101 ff.

Auch Einbruchdiebstähle und Raub sind seit 2012 rückläufig, wobei bei Raub eine Stabilisierung bzw. in den letzten zwei Jahren eine leichte Zunahme zu verzeichnen ist. Allerdings sinken nicht alle Vermögensdelikte: Betrugsdelikte haben in den letzten Jahren wieder stark zugenommen. Ein Grund für diese steigende Tendenz könnte im vermehrten Aufkommen von Online-Betrügereien liegen. Da der Betrug bei den hier gemessenen Vermögensdelikten der einzige Tatbestand ist, bei dem kein direkter Kontakt zum Opfer bzw. keine physische Wegnahme des Tatobjekts benötigt wird, kann er problemlos online ausgeführt werden. Dasselbe gilt für die Ehrverletzungsdelikte, die ebenfalls stark gestiegen sind und bei denen die Vermutung nahe liegt, dass sie in den letzten Jahren hauptsächlich online begangen worden sind. Diese Hypothese, wonach insb. Delikte zugenommen haben, die leicht im digitalen Raum begangen werden können, soll unter Kap. III noch genauer untersucht werden.

Bei den Sexualdelikten sind sexuelle Handlungen mit Kindern und sexuelle Nötigungen konstant geblieben. Allerdings haben wir auch hier wieder einen Ausreisser: Pornografie-Straftaten sind in den letzten Jahren stark gestiegen. Das könnte dadurch erklärt werden, dass mit der Umsetzung der Lanzarote-Konvention im Jahr 2014 auch der Tatbestand der Pornografie angepasst und erweitert wurde.[18] Allerdings ist ein steigender Trend schon vor dieser Änderung der Strafnorm ersichtlich. Deswegen liegt auch bei der Pornografie der Schluss nahe, dass die Digitalisierung dem Tatbestand Vorschub geleistet haben dürfte.

[18] Siehe dazu Botschaft des Bundesrates vom 4. Juli 2012 zur Genehmigung des Übereinkommens des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (Lanzarote-Konvention) sowie zu seiner Umsetzung (Änderung des Strafgesetzbuchs), BBl 2012, 7615 ff.

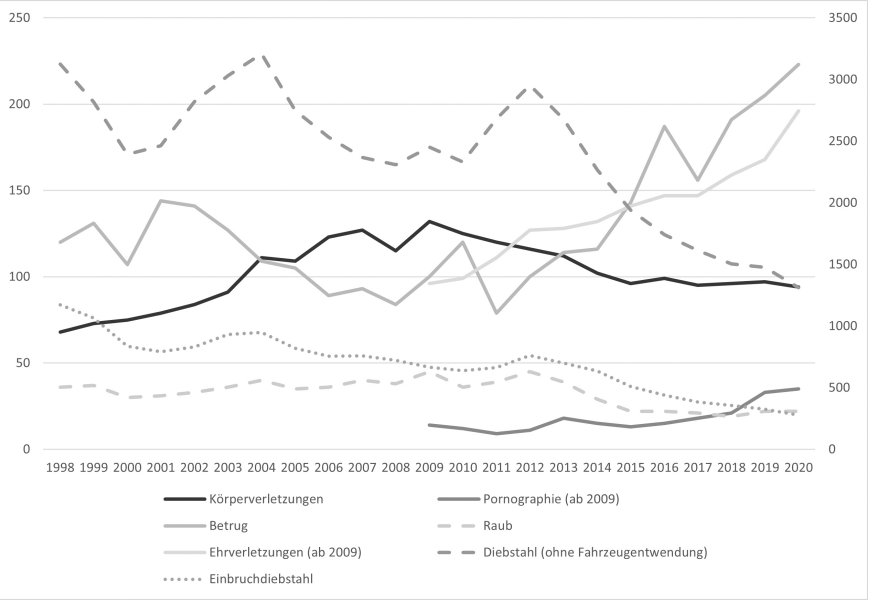


Abb. 1: Anzahl verschiedener Delikte pro 100'000 Einwohner (Jahre 1998-2020), Einbruch- und Diebstahl Skala rechte y-Achse, übrige Delikte Skala linke y-Achse (Quelle: Bundesamt für Statistik (BFS), Polizeiliche Kriminalstatistik, 2021, <https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/erhebungen/pks.html>)

Um allfällige Digitalisierungstendenzen aus den Statistiken herauszulesen, soll auch ein Blick auf die Entwicklung der Cyberdelikte im engeren Sinn geworfen werden. Dies betrifft die unbefugte Datenbeschaffung (Art. 143 StGB), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), die Datenbeschädigung (Art. 144bis StGB) sowie der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB). Bei all diesen Delikten kann die Entwicklung in den letzten 10 Jahren als stabil angesehen werden – mit Ausnahme gewisser Schwankungen beim betrügerischen Missbrauch einer Datenverarbeitungsanlage, wo nach einem starken Rückgang zwischen 2012 und 2014 wieder eine konstante Zunahme auf das Niveau von 2012 zu verzeichnen ist.

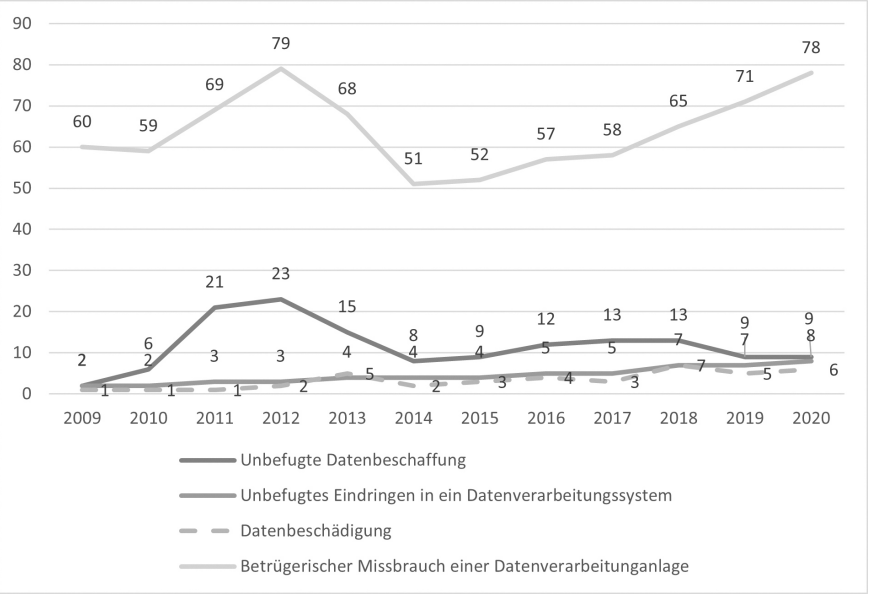


Abb. 2: Anzahl Cyberdelikte pro 100'000 Einwohner (Jahre 2009-2020) (Quelle: BFS, Polizeiliche Kriminalstatistik, 2021)

Aus den Hellfelddaten kann somit folgendes Fazit gezogen werden: Während vollendete Tötungsdelikte, Körperverletzungen sowie Vermögensdelikte wie Einbruchdiebstahl, Diebstahl und Raub in den letzten Jahren deutlich zurückgegangen sind, haben Betrug, Ehrverletzungsdelikte und Pornografie deutlich zugenommen. Die Cyberdelikte im engeren Sinn sind, mit Ausnahme einer Zunahme beim betrügerischen Missbrauch einer Datenverarbeitungsanlage, insgesamt relativ stabil geblieben. Als Interpretation dieser Trends steht die Hypothese im Raum, dass klassische Offline-Delikte", also solche, die nur in direktem physischem Kontakt mit dem Opfer begangen werden können, im öffentlichen Raum zurückgehen, während dafür Delikte zunehmen, die auch im Cyberraum ausgeführt werden können (sog. Cyberdelikte im weiteren Sinn).

3. Entwicklungen im Dunkelfeld

In der Schweiz werden seit 1984/86 Opferbefragungen auf nationaler Ebene durchgeführt. Sie basieren auf Fragebögen, die auch international im Rahmen der International Crime Victimization Surveys (ICVS) verwendet werden, und gewährleisten somit auch eine Vergleichbarkeit der Daten mit ausländischen

Befragungen. Die letzte gesamtschweizerische Erhebung wurde im Jahre 2015 durchgeführt und basiert auf einer Stichprobe von 2000 telefonisch sowie online befragten Personen.[19]

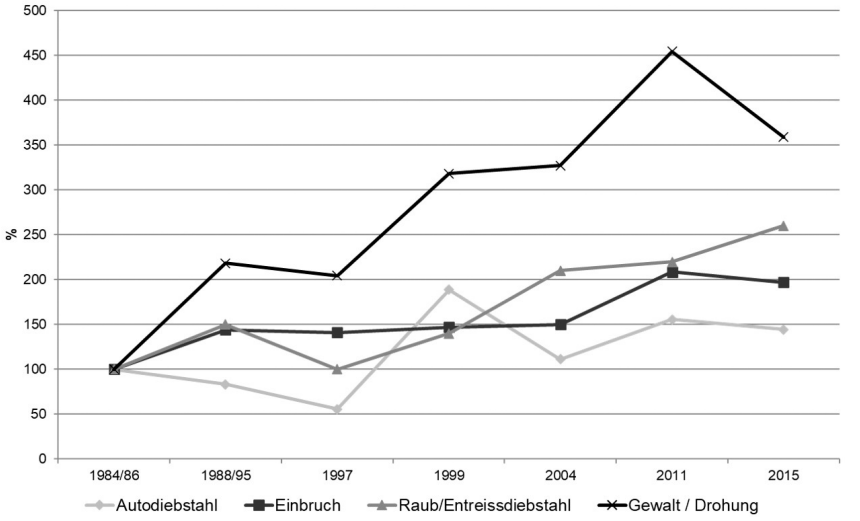


Abb. 3: Entwicklung der Opferraten in der Schweiz gem. Opferbefragungen (1984/86 – 2016, indexiert, 1984/86 = 100%) (Quelle: Crime Victim Surveys, unveröffentlichte Grafik von Biberstein/Killias)

Aus Abb. 3 ist ersichtlich, dass sich der in den Statistiken beobachtete rückläufige Trend bei Gewalt- und Vermögensdelikten auch in den Befragungsdaten widerspiegelt, denn dort ist ein Rückgang dieser Delikte zwischen der Befragung 2011 und der letzten Befragung im Jahre 2015 ersichtlich. Beim Raub sind die Tendenzen allerdings unterschiedlich: Während die offiziellen Statistiken einen Rückgang der Raubdelikte zwischen 2012 und 2018 und erst ab 2019 wieder eine Zunahme festhalten, haben diese Delikte in den Opferbefragungen seit 1997 konstant zugenommen. Allerdings könnte dieses Ergebnis auch damit zusammenhängen, dass Raub in den Opferbefragungen etwas breiter definiert wurde und demnach auch Diebstähle mit niederschwelliger Gewaltanwendung unter diese Kategorie gefallen sind (z.B. Entreissdiebstähle), während solche Vorkommnisse in der Statistik vermutlich häufiger als einfache Diebstähle vermerkt wurden.[20]

---

19 Biberstein et al., 4 f.

20 Als Raub wurden in der Befragung von 2015 sämtliche Diebstähle mit Anwendung oder Androhung von Gewalt verstanden, siehe dazu Biberstein et al., 10.

III. Digitalisierungstendenzen in der Kriminalität?

1. Cyberdelikte in den offiziellen Statistiken

Wie viele der „klassischen" Delikte werden nun nicht mehr offline, sondern im digitalen Raum ausgeübt? Bis im Frühling 2021 konnten die offiziellen Statistiken darauf keine Antwort geben. Nun aber wurde zum ersten Mal in der polizeilichen Kriminalstatistik der Anteil der digital verübten Straftaten für verschiedene Deliktskategorien ausgewiesen. Das BFS versteht unter digitaler Kriminalität „alle sogenannten 'digitalen' Straftaten, die im Wesentlichen den Straftaten entsprechen, die in Telekommunikationsnetzen, insbesondere im Internet, begangen werden".[21] Dabei gilt der Modus Operandi als massgebend für die Identifizierung einer Straftat als Cyberdelikt.[22] Die digitale Kriminalität wird vom BFS in 5 Kategorien eingeteilt, nämlich Cyber-Wirtschaftskriminalität, Cyber-Sexualdelikte, Cyber-Rufschädigung und unlauteres Verhalten, Darknet und eine Residualkategorie „Anderes".[23] Im Jahr 2020 wurden von der Polizei gesamthaft 24'398 Straftaten mit einer digitalen Komponente und 5481 beschuldigte Personen registriert, was einen digitalen Anteil von 31.6% ausmacht. Die Aufklärungsrate lag dabei bei insgesamt 44.1%.[24] Die nachfolgenden Abb. 4 und 5 zeigen diesen Anteil für ausgewählte Delikte auf.

Wie bereits vorgängig vermutet haben sich gewisse Delikte stark in den Cyberraum verlagert. So wurden etwa 79.3% der Geldwäschereihandlungen, 70.4% der Betrugstaten sowie 60.9% der Erpressungen online begangen. Der Modus Operandi bei Hehlerei hingegen bleibt hauptsächlich offline. Cyberdelikte im engeren Sinn wie etwa die die unbefugte Datenbeschaffung, das unbefugte Eindringen in ein Datenverarbeitungssystem oder die Datenbeschädigung werden ebenfalls hauptsächlich im digitalen Raum ausgeübt (68.0% resp. 71% resp. 82.7%), während dies beim betrügerischen Missbrauch einer DVA nicht der Fall zu sein scheint, denn dort haben nur 29.2% der Delikte einen Cyberbezug. Bei diesen Zahlen stellt sich allerdings die Frage, wie Datendelikte überhaupt offline begangen werden können. Hier hätte man eigentlich einen Cyber-Anteil von 100% erwarten müssen, weshalb Zweifel an der Genauigkeit und Aussagekraft dieser neuen Statistik angebracht sind.

---

21 BFS, Digitale Kriminalität.

22 BFS, Digitale Kriminalität.

23 BFS, Digitale Kriminalität.

24 BFS, Digitale Kriminalität.

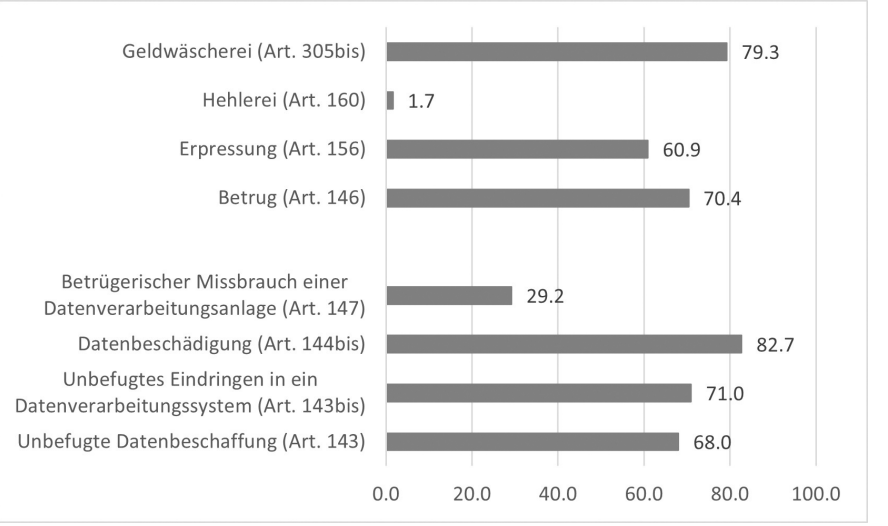


Abb. 4: Cyberanteil für Cyberdelikte i.e.S. sowie ausgewählte Vermögensdelikte und Geldwäscherei, in % (Quelle: BFS, Polizeiliche Kriminalstatistik, 2021)

Gemäss Angaben des BFS sind Ehrverletzungsdelikte sowie Fälle von Diskriminierung und Aufruf zu Hass (Art. 261bis StGB, ehem. Rassendiskriminierungsartikel) erstaunlich wenig häufig im Cyberraum begangen worden. Gerade einmal 20% der üblen Nachrede und 15.3% der Verleumdungen sowie ein verschwindend geringer Anteil von 2% aller Beschimpfungen wurden online begangen. Diese Zahlen bestätigen demnach die vorgängig formulierte These nicht, wonach insb. Delikte, die einfach online begangen werden können, zugenommen haben (siehe dazu Kap. II.2.). Es ist allerdings fraglich, ob diese Zahlen den tatsächlichen Anteil dieser Delikte im Online-Raum wiedergeben. Möglich wäre, dass gewisse ehrverletzenden Aussagen gar nicht erst bei der Polizei angezeigt werden, wenn die Täterschaft von Anfang an unbekannt ist, was bei Online-Fällen aufgrund der Anonymität des Internets wohl häufig der Fall sein dürfte. Wie bereits bei den Cyberdelikten im engeren Sinn erwähnt könnten aber auch diese Zahlen mit Ungenauigkeiten bei der Erhebungspraxis der Statistik erklärt werden, so dass Delikte im digitalen Raum nicht als solche erkannt und registriert werden.

Bei Sexualdelikten sowie Drohungen und Nötigungen sind die Anteile der Deliktsbegehung im Cyberraum ebenfalls sehr gering, mit Ausnahme der Pornografie, die in 81.3% der Fälle online begangen wurde. Dieser hohe Anteil bei der Pornografie erstaunt nicht, ist das Angebot an verbotenen Fotos resp. Vi-

deos im Internet doch umfassend und weitaus einfacher zugänglich, als dies früher bei Printmedien der Fall war. Dieser einfachere Zugang zu verbotenem pornografischem Material dürfte sicherlich auch zur Zunahme dieser Delikte in den Statistiken beigetragen haben. Bei den übrigen Sexualdelikten wie auch bei der Drohung und Nötigung wäre es hingegen aufgrund der Digitalisierung nahe liegend gewesen, dass mehr solcher Delikte im Internet stattfinden, auch wenn man an verschiedene Arten von Online-Belästigungen denkt. Diese Anteile erscheinen demnach sehr tief, weshalb auch hier die Hypothese nahe liegt, dass es wohl eine grössere Dunkelziffer im Online-Bereich gibt oder gewisse Verhaltensweisen im digitalen Raum strafrechtlich noch gar nicht ausreichend erfasst sind.[25]

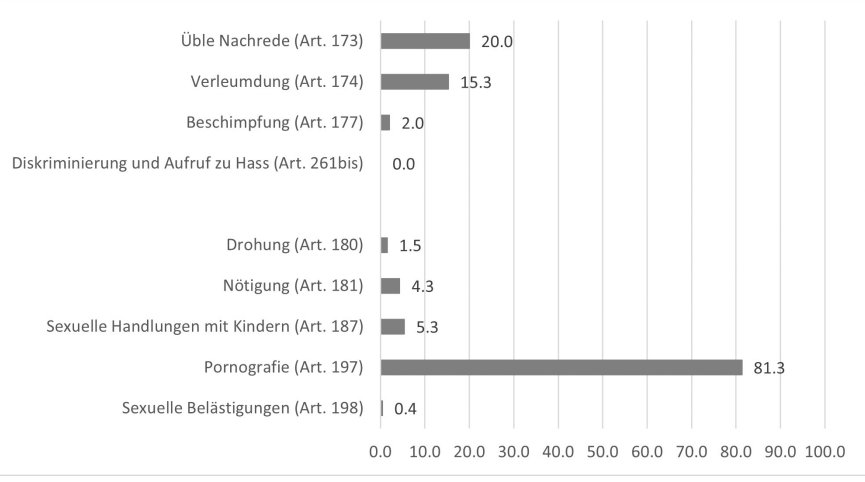


Abb. 5: Cyberanteil für ausgewählte Sexualdelikte, Delikte gegen die Freiheit, Ehrverletzungsdelikte und Diskriminierung und Aufruf zu Hass, in % (Quelle: BFS, Polizeiliche Kriminalstatistik, 2021)

Neben der seit 2021 bestehenden Information zum digitalen Bezug bei den Delikten in der PKS gibt es in den offiziellen Statistiken keine weiteren detaillierten Informationen zum Cyberbezug. Wir wissen zwar nun seit 2021, wie häufig Delikte online begangen worden sind, allerdings ist diese Information in den vorherigen Jahren nicht ausgewiesen worden. Dementsprechend können keine längerfristigen Trends und auch keine weiterführenden Informationen bei Delikten im Cyberbereich ausgemacht werden. Offizielle Statistiken

[25] Vgl. die Diskussion zu Cybergrooming und Online-Belästigung in Fontanive/Simmler, 485 ff.

sind somit wenig geeignet, detaillierte Angaben zu diesem Verschiebungsmechanismus von offline zu online sowie zur Ausgestaltung der Delikte im Onlineraum zu liefern. Ausnahme bilden einige Delikte, bei denen die Datenlage aufgrund spezieller Vorgaben besser ausgestaltet ist. Beim Tatbestand der Diskriminierung und Aufruf zu Hass z.B. hat die Eidgenössische Kommission gegen Rassismus (EKR) seit dem Jahr 1995 eine spezifische Datenbank mit Angaben zu sämtlichen Entscheiden der Strafbehörden, die zu Art. 261bis StGB ergangen sind, aufgebaut. Basierend auf diesen Daten konnte eine Studie von Beeler/Markwalder aufzeigen, dass sich der Modus Operandi in den letzten Jahren hauptsächlich in den Online-Bereich und dort schwerpunktmässig auf die Sozialen Medien verschoben hat.[26] Diese Ergebnisse aus der EKR-Datenbank stehen allerdings im Widerspruch zu den neusten Zahlen des BFS, wonach keines dieser Delikte im digitalen Raum verübt worden war (siehe dazu Abb. 5).

2. Cyberdelikte in den Opferbefragungen

Ein grosser Vorteil von Opferbefragungen ist, dass Variablen zu Tätern, Opfern und Tatumständen inkl. Modus Operandi detaillierter und von juristischen Kategorien unabhängig erhoben werden können. Demnach sind auch Informationen zum Cyberbezug bei den erlittenen Delikten relativ einfach zu erheben. Allerdings werden solche Informationen erst seit kurzem abgefragt, weshalb Daten aus früheren Jahren fehlen. Basierend auf den erhältlichen Daten ist es daher schwierig, Aussagen zu Trends von Cyberdelikten resp. der Verschiebung von Delikten in den Cyberraum zu treffen. Die vorliegend zusammengetragenen Daten dienen somit hauptsächlich zur Auslegeordnung von bestehendem Wissen über digitale Delikte.

Zu den Cyberdelikten im engeren Sinn bestehen seit 2011 Befragungsdaten. Im Crime Victim Survey von 2011 wurde erhoben, ob die Befragten bereits einmal Opfer eines Übergriffs im Internet geworden waren (sog. Lebenszeitprävalenz), was in 22.8% der Fälle bejaht wurde.[27] Als Übergriff im Internet wurde Phising,[28] Viren, Missbrauch der eigenen Website resp. des eigenen E-Mails sowie „Anderes" verstanden. Diese Definition wurde 2015 durch Cyberbully-

26 Beeler/Markwalder, 243 ff.

27 Biberstein et al., 18.

28 Phishing wurde in der Befragung 2015 definiert als Versuche, über gefälschte Websites, E-Mails oder Kurznachrichten an persönliche Daten oder Passwörter zu gelangen.

ing,[29] Sextortion,[30] und Sexting[31] ergänzt. Im Jahre 2015 wurde allerdings nicht mehr die Lebenszeitprävalenz, sondern nur noch Opfererfahrungen der letzten 5 Jahren abgefragt, weshalb diese mit 6.6% deutlich tiefer ausgefallen und nicht mehr direkt mit den Zahlen von 2011 vergleichbar sind. Es kann jedoch auch nicht ausgeschlossen werden, dass nicht nur der unterschiedliche Befragungsraum für diese deutliche Reduktion verantwortlich war, sondern Übergriffe im Internet in diesem Zeitraum auch tatsächlich zurückgegangen sind.[32] Innerhalb der Kategorie der Online-Übergriffe war Phising mit 35.9% am häufigsten angegeben worden, gefolgt von Viren (35.7%) und Missbrauch des eigenen E-Mails (12.3%) resp. der eigenen Webseite (3.8%). Opfer von Cyberbullying, Sexting und Sextortion waren jeweils nur 1.8% der Befragten geworden.[33]

Für die übrigen Delikte, die in den Crime Victim Surveys abgefragt wurden, ist jeweils nur punktuell ein Cyberbezug ersichtlich, so etwa beim Kreditkartenmissbrauch oder beim Verbraucherschwindel. Beide Delikte beinhalten neben dem Online-Missbrauch der Kreditkarte bzw. Betrügereien bei Käufen im Internet auch verschiedenen Offline-Varianten der Deliktsbegehung, so etwa das Stehlen der Kreditkarte zwecks Missbrauch oder Betrügereien bei Käufen in Läden sowie bei Erhalt von Dienstleistungen.[34] Schaut man sich diese Delikte an, sind keine eindeutigen Trends ersichtlich: Die jährliche Opferrate bei Verbraucherschwindel liegt für das Jahr 2009 bei 3.8% und für 2015 fast gleichauf bei 3.7%, mit einigen Schwankungen zwischenzeitlich. Ein Blick auf die verschiedenen Arten von Verbraucherschwindel zeigt, dass sich Betrügereien bei Einkäufen im Internet zwischen der Befragung aus dem Jahre 2011 und der letzten aus dem Jahre 2015 gar von 41.8% auf 28.6% reduziert haben. Hier scheint also keine Digitalisierungstendenz vorzuliegen, sondern ein gegensätzlicher Trend. Grund dafür könnte eine vermehrte Achtsamkeit der Online-Shopper in Bezug auf Risiken im Online-Handel oder auch eine Etablierung gewisser Gütesiegel, Ratings oder Schutzvorkehren beim Bezahlungsvorgang sein. Auch der Kreditkartenmissbrauch hat im erhobenen Zeitraum nicht zugekommen, sondern schwankt zwischen 0.4% und 1%.

---

29 Bullying, Mobbing, Schlechtmachen im Internet auf Chats, Foren, Facebook etc.

30 Erpressung mit der Drohung, sexuelle Bilder oder Videos zu veröffentlichen.

31 Verschicken von unerwünschten Nachrichten mit sexuellem Inhalt.

32 Biberstein et al., 19.

33 Biberstein et. al., 18 f.

34 Weiterführende Informationen zu Delikten im Cyberbereich werden daher erst im Crime Survey 2021, der aktuell gerade angelaufen ist, erhältlich sein.

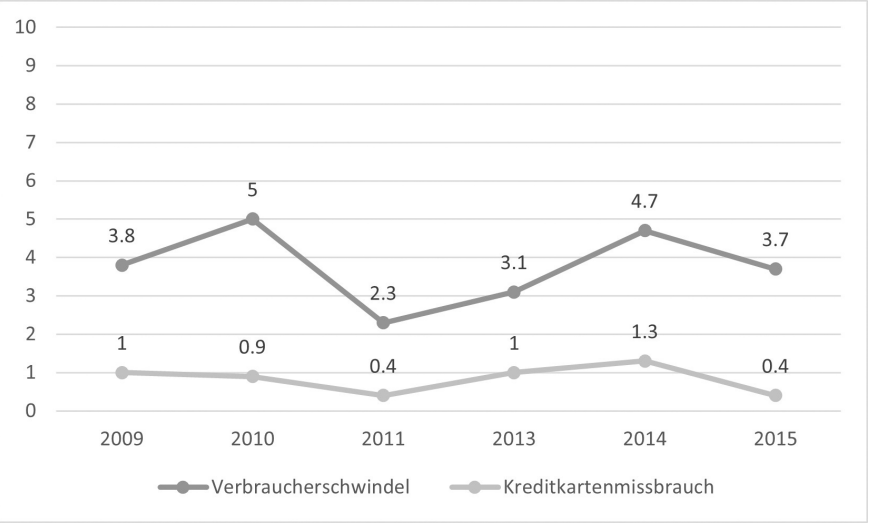


Abb. 6: Anzahl Opfer von Verbraucherschwindel und Kreditkartenmissbrauch (Jahresprävalenz in %, Quelle: CVS 2015, Biberstein et al. 2016)

Neben den auf der ICVS-Methodik basierenden Crime Surveys sind weitere Opferbefragungen durchgeführt worden, welche auch Cyberdelikte erhoben haben. Erwähnenswert ist zum einen die Studie von Baier, der in einer gesamtschweizerischen[35] Untersuchung die Betroffenheit durch Cyberdelikte wie etwa dem Datenverlust durch Viren, Datenmissbrauch, Internetbetrug oder Angriffe auf das Online-Banking untersucht hat. Insgesamt hatten 11.5% der Befragten angegeben, im letzten Jahr schon einmal Opfer solcher Cyberdelikte geworden zu sein[36]. Zusätzlich dazu wurden auch Opfererfahrungen für Cyberbullying sowie sexuelle Online-Belästigung abgefragt. 7.7% der Befragten gaben diesbezüglich an, im letzten Jahr Cyberbullying erlebt zu haben, und 7.0% waren in diesem Zeitraum online sexuell belästigt geworden.[37] Neben der Opfererfahrung wurde in dieser Studie auch die Wahrnehmung der Entwicklung verschiedener Kriminalitätsphänomene erfragt. Hierbei zeigte sich, dass 95.3% der Befragten angaben, gemäss ihrer Einschätzung habe die Internet- und Cyberkriminalität zugenommen.[38] Es ist hier also ersichtlich, dass

35 Aufgrund einer Unterrepräsentation von jüngeren sowie weiblichen Personen kann die Stichprobe nur als bedingt repräsentativ angesehen werden, was allerdings mittels Gewichtung der Stichprobe zu korrigieren versucht wurde; siehe dazu Baier, 19 ff.

36 Baier, 27 f.

37 Baier, 38 f.

38 Baier, 49.

neben einer doch bedeutsamen Anzahl an Betroffenen die Cyberkriminalität auch seitens der Bevölkerung als zunehmendes Problem wahrgenommen wird.

Neben gesamtschweizerischen Studien ist auch noch eine auf die Stadt Lugano beschränkte repräsentative Befragungsstudie aus dem Jahr 2019 zu erwähnen, die Cyber-Opfererfahrungen der Luganeser Bevölkerung im Bereich der Virusattacken, des Onlinebetrugs sowie der unbefugten Verwendung von persönlichen Daten untersuchte.[39] Von den insgesamt 6'580 Personen, die bei der Befragung teilgenommen hatten, gaben 18.0% an, in den letzten 5 Jahren vor der Befragung bereits einmal Opfer eines Internetbetrugs geworden zu sein, 20% erlitten eine Virusattacke und 13.0% wurden schon einmal Opfer einer unbefugten Verwendung von persönlichen Daten. Insgesamt hatten 35.0% der Befragten angegeben, in den letzten 5 Jahren mindestens einmal Opfer eines der obgenannten Cyberdelikte geworden zu sein.[40]

Studie	**Opfererfahrungen (in %)**	**Deliktszeitraum**	**Deliktsdefinition**
ICVS 2011 (Gesamte Schweiz)	22.8	Lebenszeitprävalenz	Phising, Viren, Missbrauch der eigenen Website resp. des eigenen E-Mails sowie „Anderes"
ICVS 2015 (Gesamte Schweiz)	6.6	5-Jahres-Prävelenz	Phising, Viren, Missbrauch der eigenen Website resp. des eigenen E-Mails, Cyberbullying, Sextortion, Sexting und Sonstiges
Baier 2019 (Gesamte Schweiz)	11.5 (32.9)	Jahresprävalenz (Lebenszeitprävalenz)	Datenverlust durch Viren etc., Datenmissbrauch, Angriff Onlinebanking, Internetbetrug
	7.7	Jahresprävalenz	Cyberbullying
	7.0	Jahresprävalenz	Sexuelle Online-Belästigung
Milani et al. 2019 (Lugano)	35.0	5-Jahres-Prävelenz	Virusattacke, Internetbetrug und unbefugte Verwendung von persönlichen Daten

Tabelle 1: Übersicht über Opferraten aus verschiedenen Befragungsstudien (Quellen: Biberstein et al., 2016; Baier, 2019; Milani/Caneppele/Burkhardt, 2019)

39 Milani/Caneppele/Burkhardt, 3.

40 Milani/Caneppele/Burkhardt, 3 f. Die Jahresprävalenz betrug 14.6% für Virusattacken, 15.2% für Internetbetrug und 10.8% für die unbefugte Verwendung von persönlichen Daten.

Aufgrund der unterschiedlichen Definitionen und der ungleichen Zeiträume der Deliktserfassung können hier keine direkten Vergleiche zwischen den Studien gezogen werden. Allerdings ist basierend auf den Resultaten der verschiedenen Studien klar, dass Online-Delikte keine Randerscheinung mehr darstellen, sondern dass in der Bevölkerung teilweise beachtliche Opferraten vorliegen.

IV. Fazit

Die Digitalisierung hat unsere Lebensgewohnheiten stark beeinflusst, und dieser Einfluss macht sich auch im Bereich der Kriminalität bemerkbar. Während bei klassischen Offline-Delikten wie Körperverletzungen oder Diebstahl in den letzten Jahren sowohl in den offiziellen Statistiken wie auch in den Opferbefragungen ein Rückgang ersichtlich ist, haben Delikte wie Betrug oder Pornografie, die neuerdings hauptsächlich im Cyberraum begangen werden, stark zugenommen. Die Digitalisierung beeinflusst demnach nicht unbedingt die Entwicklung der Cyberdelikte im engeren Sinn, sondern leistet insbesondere der Verschiebung von Delikten in den digitalen Raum Vorschub. Diese Digitalisierungstendenz ist auch für die Präventionsarbeit von höchster Bedeutung. Sie bedingt z.B. einen vermehrten Fokus der Polizeiarbeit und Strafverfolgung auf den digitalen Raum, was durch die Schaffung von spezialisierten Abteilungen bei Strafverfolgung und Polizei in verschiedenen Kantonen teilweise bereits umgesetzt wurde.[41] Die zunehmenden Gefahren der Viktimisierung im Cyberraum sollte aber auch dazu führen, dass bei der Präventionsarbeit auf Risiken im Online-Bereich sowie auf Sensibilisierung und Aufklärung der Internet-Nutzerinnen und -Nutzern fokussiert wird.[42]

Für die Erforschung von Digitalisierungstendenzen innerhalb der Kriminalität ist es nötig, auf detailliertere Kriminalstatistiken zurückgreifen zu können. Insb. die Tatbegehung sollte als relevante Kernvariable bei sämtlichen Delikten registriert werden, um so den Cyberbezug beim Modus Operandi feststellen zu können. Das BFS hat mit der Publikation des Anteils der digitalen Deliktsbegehung im Jahre 2021 einen ersten Schritt gemacht und es ist zu hoffen, dass diese Informationen für sämtliche Delikte auch in Zukunft erhoben werden. Kriminalstatistiken allein reichen allerdings nicht aus, um das Ausmass der De-

41 Für eine nicht abschliessende Liste siehe z.B. Bundesamt für Kommunikation (BAKOM), Bekämpfung der Internetkriminalität, <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html.>.

42 So z.B. die Aufklärungsarbeit im Bereich der Internetdelikte der Schweizerischen Kriminalprävention (SKP), siehe dazu Schweizerischen Kriminalprävention (SKP), Fokus Internet, <https://www.skppsc.ch/de/themen/internet/>.

likte im digitalen Raum zu erfassen, da sie lediglich die polizeilich bekannten Delikte beinhalten. Zudem haben sie den Nachteil, dass die Informationen in den Statistiken zu Beginn des Verfahrens erhoben werden, also zu einem Zeitpunkt, in welchem der Sachverhalt oftmals noch ungewiss ist und Tatumstände und Motivation des Täters unklar sind. Es besteht demnach die Gefahr, dass keine Informationen zu den Umständen der Tat vorliegen oder sich diese im Laufe der Ermittlungen ändern, was die Validität der Statistik beeinträchtigt.[43] Dazu kommt, dass Fälle in den Statistiken durch unterschiedliche Personen in unterschiedlichen Polizeicorps erhoben werden. Gerade bei Variablen wie der digitalen Komponente eines Delikts, die sich nicht immer eindeutig kategorisieren lassen, ist eine einheitliche Erhebungsmethodik schwierig und die Reliabilität, d.h. die intersubjektive Reproduzierbarkeit der Statistik, demnach beeinträchtigt.[44] Aus diesen Gründen sind neben den offiziellen Kriminalstatistiken unbedingt auch Befragungsdaten zu Viktimisierungserfahrungen von spezifisch im Internetraum begangenen Delikten nötig, um das wahre Ausmass der Cyberkriminalität (inkl. der Dunkelziffer) erkennen zu können. Wir haben also in der Forschung wohl erst die sprichwörtliche Spitze des Eisbergs erfasst, und es bleibt Aufgabe zukünftiger Forschungsbemühungen, den Rest des Eisbergs zu entdecken.

Literaturverzeichnis

Aebi Marcelo F./Linde Antonia, Is There a Crime Drop in Western Europe?, European Journal on Criminal Policy and Research 16, 2010, 251 ff.

Baier Dirk, Kriminalitätsopfererfahrungen und Kriminalitätswahrnehmungen in der Schweiz: Ergebnisse einer Befragung, Zürich 2019.

Beeler Nina/Markwalder Nora, Rassendiskriminierung im digitalen Zeitalter: Von offline zu online? ContraLegem, 2019/2, 239 ff.

Biberstein Lorenz et al., Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung. Analysen im Rahmen der schweizerischen Sicherheitsbefragung 2015, 2016.

Caneppele Stefano/Aebi Marcelo F, Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes, Policing: A Journal of Policy and Practice 13 (1), 2019, 66 ff.

Cohen Lawrence E./Felson Marcus, Social change and crime rate trends: A routine activity approach, American Sociological Review 1979, 588 ff.

Farrell Graham/Tilley Nick/Tseloni Andromachi, Why the Crime Drop? Crime and Justice, 43(1), 2014, 421 ff.

[43] Zur Validität eines Indikators siehe Killias/Aebi/Kuhn, Rz. 69.

[44] Zur Reliabilität eines Indikators siehe Killias/Aebi/Kuhn, Rz. 68 ff.

Fontanive Karin/Simmler Monika, Gefahr im Netz: Die unzeitgemässe Erfassung des Cybergroomings und des Cyberharassments im schweizerischen Sexualstrafrecht: Zur Notwendigkeit der Modernisierung von Art. 198 StGB. Zeitschrift Für Schweizerisches Recht = Revue De Droit Suisse = Rivista Di Diritto Svizzero 135, 2016, 485 ff.

Gyarmati Nikolaus, Phänomen Cybercrime und seine Bekämpfung, SZK 1-2/2019, 86 ff.

Isenring Bernhard/Maybud Roy D./Quiblier Laura, Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick, SJZ 115/2019 S. 439 ff.

Killias Martin, The Opening and Closing of Breaches. A Theory on Crime Waves, Law Creation and Crime Prevention, European Journal of Criminology 2006, 11 ff.

Killias Martin/Haymoz Sandrine/Lamon Philippe, Die Kriminalität in der Schweiz im Lichte der Opferbefragung von 1984 bis 2005, Bern 2007.

Killias Martin/Aebi Marcelo F./Kuhn André, Précis de Criminologie, 4. A., Bern 2019.

Linde Antonia, The Impact of Improvements in Medical Care Resources on Homicide Trends: The Case of Germany (1977–2011). European Journal on Criminal Policy and Research 24, 2018, 99 ff.

Milani Riccardo/Caneppele Stefano/ Burkhardt Christine, Exposure to Cyber Victimization: Results from a Swiss Survey, Deviant Behavior, 2020.

Rosenfeld Richard/Weisburd David, Explaining Recent Crime Trends: Introduction to the Special Issue. Journal of Quantitative Criminology 32, 2016, 329 ff.

Suonpää Karoliina et al. Homicide Drop in Seven European Countries: General or Specific across Countries and Crime Types? (In Vorb.).

Opfererfahrungen im Internet – Schutz- und Risikofaktoren

Rutger Leukfeldt/Susanne van't Hoff-de Goede/Rick van der Kleij/
Steve G.A. van der Weijer

Inhalt

Zusammenfassung

Der Anstieg der Opfererfahrungen durch Internetkriminalität unterstreicht die Notwendigkeit zu verstehen, wie sich Menschen online verhalten und wie unsicheres Online-Verhalten mit Viktimisierung zusammenhängen kann. Bisherige Studien haben sich oft auf selbstberichtete Verhaltensweisen oder Einstellungen zu vorsichtigem Online-Verhalten verlassen. Studien, die sowohl das tatsächliche Online-Verhalten als auch erklärende Faktoren in einer grossen Stichprobe gemessen haben, sind rar. In diesem Beitrag wird das Forschungsinstrument der *Online Behaviour and Victimization Study* vorge-

stellt. Das Kapitel skizziert die Entwicklung dieses Instruments, das ein bevölkerungsbasiertes Befragungsexperiment verwendet. Mit diesem Instrument kann das tatsächliche Verhalten von Internetnutzern gemessen werden. Während des Ausfüllens der Umfrage werden die Befragten mit (fiktiven) Cyber-Risikosituationen konfrontiert, wodurch die Forscher analysieren können, wie die Befragten mit diesen Situationen umgehen. Darüber hinaus wurden auf der Grundlage von Theorien und einer umfangreichen Literaturstudie, die in diesem Beitrag kurz skizziert wird, Messungen für zahlreiche erklärende Faktoren in die Studie aufgenommen, darunter Wissen (Bewusstsein), Gelegenheit und Motivation. Schließlich wird die frühere Viktimisierung durch Cyberkriminalität gemessen, was es ermöglicht, den Zusammenhang zwischen dem tatsächlichen Online-Verhalten und der Online-Viktimisierung zu untersuchen.

I. Einleitung

Cyberkriminalität ist weit verbreitet und ihre Auswirkungen können für die Opfer erheblich sein.[1] Cybersecurity-Experten haben versucht, die Viktimisierung mit technischen Maßnahmen wie Antivirenscannern und Firewalls zu reduzieren. Diese Maßnahmen haben jedoch oft nur eine begrenzte Wirkung und ein Großteil der Viktimisierung kann auf menschliches Verhalten zurückgeführt werden.[2] Beispielsweise geben Internetnutzer auf einer Phishing-Website[3] möglicherweise Informationen ein, die sie nicht eingeben sollten, und ermöglichen es Kriminellen so, diese Informationen zu missbrauchen. Daher ist die Erforschung von Internetnutzern unerlässlich, um die Viktimisierung zu reduzieren.[4]

Wenn wir Viktimisierung durch Cyberkriminalität verhindern wollen, müssen wir zunächst die Viktimisierung erklären. Frühere Studien zur Viktimisierung durch Cyberkriminalität haben sich auf die Erstellung eines Risikoprofils für die Opfer konzentriert und versucht, Faktoren zu identifizieren, die das Risiko einer Viktimisierung erhöhen könnten. In diesen Studien stehen oft persönliche Merkmale und Routinetätigkeiten im Mittelpunkt, indem z. B. angenommen wird, dass bestimmte Routinetätigkeiten, wie die Nutzung sozialer Medien, potenzielle Opfer für Cyberkriminelle sichtbarer machen. Mit Blick auf

1 Cross/Richard/Smith; Jansen/Leukfeldt, cybercrime; Leukfeldt/Notté/Malsch.

2 Jansen; Leukfeldt, Research.

3 Phishing ist eine Form des Online-Betrugs, bei der Kriminelle die E-Mails oder Websites bekannter Unternehmen und Organisationen imitieren, um die Opfer in die Irre zu führen, damit sie an Benutzernamen und Passwörter gelangen und Zugang zu den Online-Konten erhalten.

4 Leukfeldt, Research; Rhee/Kim/Ryu; Talib/Clarke/Furnell.

alle bisherigen Studien scheint es jedoch nicht möglich zu sein, ein eindeutiges Risikoprofil zu erstellen.[5] Cyberkriminelle sind offenbar nicht allzu wählerisch und suchen sich ihre Opfer nicht besonders aus: Jede Person ist ein potenzielles Opfer von Cyberkriminalität. Ausserdem scheinen bestimmte Online-Aktivitäten nur mit dem Risiko verbunden zu sein, Opfer bestimmter Formen von Cyberkriminalität zu werden. Es scheint keine Routineaktivitäten zu geben, die per Definition risikoerhöhend sind.[6] Es ist daher nicht möglich, ein Profil risikobehafteter persönlicher Merkmale oder Routinetätigkeiten für die Viktimisierung durch Cyberkriminalität zu benennen.

Die aktuelle Studie konzentriert sich auf das Verhalten von Internetnutzern, um damit Online-Viktimisierungen zu erklären. Es ist weithin anerkannt, dass der Mensch das „schwächste Glied" in der Cybersecurity ist. Unsicheres Online-Verhalten, wie z. B. die Verwendung von schwachen Passwörtern und nicht regelmäßig aktualisierte Software, kann das Risiko einer Viktimisierung durch Cyberkriminalität erhöhen.[7] Das Wissen darüber, wie sich Bürger gegen Cyberkriminalität schützen, ist jedoch spärlich[8] Es ist immer noch unbekannt, wie gut sich Internetnutzer vor Cyberkriminalität schützen, zum Teil weil das, was Menschen über ihr Online-Verhalten sagen oder denken, nicht immer mit dem tatsächlichen Online-Verhalten übereinstimmt.[9] Dieses Wissen ist jedoch für die empirische Fundierung möglicher Verhaltensinterventionen unerlässlich. Es ist daher notwendig, mehr Erkenntnisse darüber zu gewinnen, wie sich Internetnutzer tatsächlich online verhalten und welche Faktoren damit verbunden sind.

In diesem Beitrag wird die Entwicklung des Forschungsinstruments für die *Online Behaviour and Victimization Study* skizziert, das das tatsächliche Online-Verhalten zusammen mit möglichen erklärenden Faktoren messen kann. Der Mehrwert dieses Forschungsinstruments liegt auf der Hand: Wir gehen über bestehende Studien hinaus, die oft auf Selbstberichten basieren, indem wir sowohl das wahrgenommene als auch das tatsächliche Verhalten in einer gross angelegten Stichprobe messen. Außerdem zielen wir nicht nur auf die Erklärung der Viktimisierung bestimmter Formen von Cybercrime ab, sondern auch auf mehrere Cluster von Online-Verhalten. Schließlich gibt es viele Verhaltensweisen, die das Risiko für bestimmte Cyberkriminalität erhöhen. Ausserdem muss es nicht gleichzeitig so sein, dass ein bestimmtes Verhalten

5 Bossler/Holt, On-Line Activities; Bossler/Holt, effect; Holt/Bossler;Sheng et al.; van de Weijer/Leukfeldt.

6 Leukfeldt/Yar.

7 Leukfeldt, Phishing; Shillair et al.

8 Für einen Überblick siehe z.B. Leukfeldt, Research.

9 Crossler et al.; Debatin et al.

immer zu einer bestimmten Form der Viktimisierung führt. Einmal auf eine Phishing-E-Mail hereinzufallen, kann zu einem leeren Bankkonto führen, ein anderes Mal kann es zu einer Ransomware-Infektion[10] führen oder der Beginn eines Spear-Phishing-Angriffs[11] auf das Unternehmen sein, in dem das Opfer arbeitet.[12] Daher misst das in diesem Kapitel vorgestellte Forschungsinstrument objektiv eine Reihe von Verhaltensweisen, von denen wir wissen, dass sie in direktem Zusammenhang mit der Viktimisierung verschiedener Cyberkriminalität stehen, wie z. B. die Weitergabe persönlicher Informationen und die Verwendung schwacher Passwörter. Darüber hinaus ist dieses Forschungsinstrument innovativ, weil es verschiedene Erklärungen für Online-Verhalten und Viktimisierung misst, während bestehende Studien oft nur Einstellungen oder Wissen untersuchen. Schliesslich beinhaltet das Instrument mehrere Experimente, um beispielsweise zu ermitteln, ob von Kriminellen verwendete Überredungstechniken die Wahrscheinlichkeit erhöhen, dass sich Personen online unsicher verhalten.

II. Online-Verhalten und Viktimisierung durch Cyberkriminalität

1. Unsicheres Online-Verhalten als Prädiktor für Online-Viktimisierung

Unsicheres Online-Verhalten kann direkt zu einem erhöhten Risiko der Viktimisierung beitragen. Opfer von Online-Banking-Betrug scheinen beispielsweise oft versehentlich ihre persönlichen Daten an Betrüger weitergegeben zu haben, z. B. durch Klicken auf einen Hyperlink in einer Phishing-E-Mail oder die Eingabe von Informationen auf einer Phishing-Website.[13]

Eine wichtige Voraussetzung für Online-Sicherheit ist daher sicheres Online-Verhalten (d. h. Cyber-Hygiene-Verhalten).[14] Menschen, die sich online sicher – oder cyberhygienisch – verhalten, halten sich an „goldene" Regeln (Best Practices). Sie meiden zum Beispiel unsichere Webseiten, vermeiden das Klicken auf unzuverlässige Hyperlinks, verwenden starke Passwörter und halten ihre technischen Sicherheitsmassnahmen auf dem neuesten Stand.[15] Basie-

---

10 Ransomware ist eine Schadsoftware, die einen Computer blockiert oder Dateien verschlüsselt. Erst wenn die betroffene Person ein Lösegeld zahlt, kann sie den Computer oder die Dateien wieder nutzen.

11 Spear-Phishing ist ein gezielter Phishing-Angriff gegen eine Person oder eine bestimmte Gruppe von Personen.

12 Siehe z.B. Leukfeldt/Kleemans/Stol; Lusthaus.

13 Jansen; Jansen/Leukfeldt, People; Jansen/Leukfeldt, Phishing.

14 Cain/Edwards/Still.

15 Cain/Edwards/Still; Crossler/Bélanger/Ormond; Symantec.

rend auf früheren empirischen Studien haben wir für diese Studie sieben zentrale Verhaltenscluster identifiziert: das Passwortmanagement, das Sichern wichtiger Dateien, das Installieren von Updates, die Verwendung von Sicherheitssoftware, die Aufmerksamkeit im Internet, die Offenlegung von persönlichen Informationen im Internet und der Umgang mit Anhängen und Hyperlinks in E-Mails. Wenn Internetnutzer innerhalb der einzelnen Cluster ein sicheres Verhalten an den Tag legen, kann es sie vor der Viktimisierung durch Cyberkriminalität schützen.[16]

Frühere Studien, die sowohl auf selbstberichteten Verhaltensweisen als auch auf tatsächlichem Verhalten in experimentellen Umgebungen basieren, haben gezeigt, dass viele Menschen sich online nur in begrenztem Masse sicher verhalten oder sogar offensichtlich unsicheres Online-Verhalten zeigen, und zwar bei jedem der sieben Verhaltenscluster. Viele Menschen haben keinen Malware-Scanner[17] oder eine Firewall auf ihrem Heimcomputer oder halten diese nicht auf dem neuesten Stand.[18] Darüber hinaus sind junge Menschen lax mit der Sicherheit ihres Smartphones.[19]

Obwohl die Verwendung von einzigartigen, starken Passwörtern eine wichtige Sicherheitsmassnahme ist, haben Studien gezeigt, dass 50-60% der Passwörter plattformübergreifend wiederverwendet werden und dass viele Menschen ihre Passwörter mit anderen teilen würden.[20] Ein weiteres Beispiel für unsicheres Online-Verhalten ist, dass Menschen in grossem Umfang persönliche Informationen in sozialen Medien teilen,[21] die genutzt werden können, um Phishing-E-Mails glaubwürdiger zu machen (Spear-Phishing) oder um Identitätsbetrug zu begehen. Zum Beispiel gaben viele der Befragten in der Studie von Talib/Clarke/Furnell ihren vollständigen Namen und ihre E-Mail-Adresse (62%), ihr Geburtsdatum (45%) oder ihre vollständige Adresse (7%) in einem sozialen Online-Netzwerk an. Schliesslich sind abweichende Online-Verhaltensweisen, wie illegales Herunterladen, Online-Mobbing und Bedrohung anderer, weit verbreitet und tragen zur Online-Viktimisierung bei, möglicherweise insbesondere bei jungen Menschen.[22]

---

16 Für weitere Informationen siehe Cain/Edwards/Still; Crossler/Bélanger/Ormond; van Schaik et al.

17 Malware ist bösartige Software, die sich unaufgefordert und meist unbemerkt auf Ihrem Computer installiert. Beispiele für Malware sind Viren, Trojanische Pferde, Würmer und Spyware.

18 Cain/Edwards/Still; van Schaik et al.

19 Jones/Heinrichs; Tan/Aguilar.

20 Alohali et al.; Cain/Edwards/Still;Kaye.

21 Christofides/Muise/Desmarais; Debatin et al.; Talib/Clarke/Furnell.

22 Bossler/Holt, On-Line Activities; Holt/Bossler; Maimon/Louderback; Ngo/Paternoster.

Eine weitere Schlussfolgerung, die aus der Literatur gezogen werden kann, ist der Mehrwert der Fokussierung auf das Verhalten und nicht auf spezifische Cyberkriminalität. Hacking-Viktimisierung kann zum Beispiel durch viele verschiedene Verhaltensweisen verursacht werden. Zum Beispiel können Menschen gehackt werden, weil sie persönliche Informationen weitergegeben, Malware heruntergeladen oder ihre Sicherheitsvorkehrungen nicht auf dem neuesten Stand gehalten haben. Darüber hinaus können diese Verhaltensweisen auch zur Viktimisierung anderer Formen von Cyberkriminalität führen, wie z. B. Online-Betrug oder Identitätsbetrug. Studien, die sich auf spezifische Straftaten konzentrieren, geben nur einen kleinen Einblick in die Komplexität von Online-Verhalten und Cyberkriminalität. Durch die Fokussierung auf das Online-Verhalten hingegen kann potenziell einer breiten Palette von Cyberkriminalität entgegengewirkt werden.

2. Erklärung des Online-Verhaltens

Obwohl sicheres Online-Verhalten von grosser Bedeutung sein kann, um die Viktimisierung durch Cyberkriminalität zu verhindern, ist unsicheres Online-Verhalten weit verbreitet. Wie lässt sich dies erklären?

Auf der Grundlage von zwei Theorien, die zuvor zur Erklärung von Verhalten entwickelt wurden, der Protection Motivation Theory (PMT)[23] und dem COM-B-Framework (Capability, Opportunity, Motivation, Behaviour),[24] können mehrere Elemente unterschieden werden, die jeweils eine Rolle bei unsicherem Online-Verhalten spielen können. Dabei handelt es sich um die *Motivation* für sicheres Online-Verhalten, das *Wissen* über sicheres Online-Verhalten (d. h. das Bewusstsein) und die *Gelegenheit* für sicheres Online-Verhalten. Nach der Erörterung dieser Faktoren und früherer Studien über ihre Beziehungen zum Online-Verhalten wird sich dieses Kapitel auch mit anderen potenziell relevanten Faktoren befassen.

a) Motivation

Nach der Protection Motivation Theory wird unser Schutzverhalten davon beeinflusst, inwieweit wir motiviert sind, uns zu schützen.[25] Es ist anzunehmen, dass Menschen mit einer hohen Schutzmotivation vorsichtiger handeln und Massnahmen zum Schutz ihrer Sicherheit ergreifen.[26] Die Theorie argumen-

23 Floyd/Prentice-Dunn/Rogers; Norman/Boer/Seydel.

24 Michie/van Stralen/West.

25 Floyd/Prentice-Dunn/Rogers; Norman/Boer/Seydel.

26 Crossler/Bélanger; Floyd/Prentice-Dunn/Rogers.

tiert, dass die Schutzmotivation von der Bewertung der eigenen Bewältigungsmöglichkeiten und der Bewertung der Bedrohung beeinflusst wird, d. h. von der Bewertung der Bedrohung durch eine Person und den Massnahmen gegen diese Bedrohung.[27] Sowohl die Bewertung der Bedrohung als auch die Bewertung der Bewältigungsmöglichkeiten haben mehrere Komponenten. Die Komponenten der Bedrohungsbeurteilung sind die wahrgenommene Verwundbarkeit (Einschätzung der eigenen Verwundbarkeit gegenüber der Bedrohung) und der wahrgenommene Schweregrad (Einschätzung des Schweregrads der Bedrohung). Die Bewertung der Bewältigungsmöglichkeiten umfasst die Komponenten Reaktionswirksamkeit (ob eine Massnahme gegen die Bedrohung wirksam sein wird), Selbstwirksamkeit (ob man in der Lage ist, eine wirksame Massnahme einzusetzen) und Reaktionskosten (ob sich die geschätzten Kosten der Massnahmen lohnen).

Die Protection Motivation Theory wurde bereits auf das Online-Verhalten angewandt. Frühere Studien ergaben, dass die geschätzte Reaktionswirksamkeit, die Selbstwirksamkeit und die Reaktionskosten wichtige Prädiktoren für sicheres Online-Verhalten zu sein scheinen.[28] Allerdings steht die wahrgenommene Gefährdung möglicherweise nicht in der erwarteten Weise mit sicherem Online-Verhalten in Zusammenhang. Personen, die sich selbst als anfällig für Online-Angriffe einschätzen, verhalten sich nicht anders[29] und verhalten sich möglicherweise sogar weniger sicher.[30] Im Zusammenhang mit der wahrgenommenen Verwundbarkeit fanden Boss et al.[31] heraus, dass die Angst vor Viktimisierung die Motivation von Computernutzern, ihre Dateien zu sichern, nicht zu beeinflussen scheint, während sie ihre Bereitschaft, Anti-Malware-Software zu verwenden, zu erhöhen scheint. Schliesslich finden die meisten Studien einen Zusammenhang zwischen wahrgenommener Schwere und Online-Verhalten.[32] Downs, Holbrook und Cranor[33] fanden jedoch in ihrer Stichprobe von 232 Computernutzern nicht, dass die geschätzte Schwere der Folgen eines erfolgreichen Phishing-Angriffs ein Prädiktor für das Vorsichtsverhalten ist.

Leider gibt es nur sehr wenige Studien, die über die Untersuchung der Schutzmotivation und -einstellung hinausgehen und das Online-Verhalten messen.

---

27 Floyd/Prentice-Dunn/Rogers.

28 Arachchilage/Love; Crossler/Bélanger; Crossler/Bélanger/Ormond; Jansen/van Schaik; Rhee/Kim/Ryu; van Schaik et al.; Workman/Bommer/Straub.

29 Jansen.

30 Crossler/Bélanger.

31 Boss et al.

32 Crossler/Bélanger/Ormond; Jansen; Jansen/van Schaik.

33 Downs/Holbrook/Cranor.

Die wenigen, die dies taten, konzentrierten sich hauptsächlich auf das selbstberichtete Präventivverhalten. Es bleibt unklar, wie die Motivation mit dem tatsächlichen Online-Verhalten zusammenhängen könnte.

b) Wissen/Bewusstsein

Der theoretische COM-B-Framework[34] legt nahe, dass neben der Motivation auch die Fähigkeit (d. h. das Wissen über Online-Sicherheit), die auch als Bewusstsein bezeichnet wird, für ein sicheres Online-Verhalten erforderlich ist. Beispiele dafür sind Wissen über Online-Bedrohungen, Informationssicherheit, Sicherheitsmassnahmen und die Fähigkeit, schädliche URLs zu erkennen.

Frühere Studien, die untersuchten, inwieweit das Wissen über IT- und Cybersicherheit das Online-Verhalten beeinflusst, lieferten widersprüchliche Ergebnisse.[35] Arachchilage und Love[36] zeigten beispielsweise, dass Wissen, wie das Erkennen einer unzuverlässigen URL, die Selbstwirksamkeit erhöht und zu einem Phishing-Risikovermeidungsverhalten beitragen kann. Darüber hinaus sind Personen, die in der Lage sind, URLs zu bewerten, Internet-Symbole und Internet-Begriffe zu verstehen, tendenziell weniger anfällig für Phishing-Angriffe.[37] Darüber hinaus scheinen Personen, die sich als IT-Experten bezeichnen, weniger wahrscheinlich ein unsicheres Online-Verhalten an den Tag zu legen.[38] Andererseits fanden Ovelgönne et al.[39] heraus, dass Softwareentwickler häufiger ein riskantes Online-Verhalten an den Tag legen als andere Befragte. Obwohl dies in einigen Fällen damit zusammenhängen könnte, dass Menschen ihr Wissen über Internetsicherheit überschätzen und sich dadurch zu Unrecht als IT-Experten einstufen,[40] fanden Cain/Edwards/Still[41] heraus, dass Menschen, die sich selbst als IT-Experten einschätzen, sich online weniger sicher verhalten. Darüber hinaus wurde kein Unterschied im Präventivverhalten zwischen Personen, die in IT oder Cybersicherheit geschult waren, und solchen, die dies nicht waren, festgestellt. Diese Studien haben einen wichtigen Schritt zur Erforschung der Beziehung zwischen Wissen und Online-

34 Michie/van Stralen/West.

35 Alohali et al.; Arachchilage/Love; Cain/Edwards/Still; Downs/Holbrook/Cranor; Holt/Bossler; Ovelgönne et al.; Parsons et al., Determining; Shillair et al.

36 Arachchilage/Love.

37 Downs/Holbrook/Cranor.

38 Alohali et al.

39 Ovelgönne et al.

40 Debatin et al.

41 Cain/Edwards/Still.

Verhalten gemacht. Die Ergebnisse sind jedoch noch unschlüssig, und es sind weitere Forschungsarbeiten erforderlich, insbesondere zur Untersuchung des tatsächlichen Online-Verhaltens und seines Zusammenhangs mit dem Wissen.

c) Gelegenheit

Gemäß dem COM-B-Framework reichen Wissen und Motivation allein möglicherweise nicht aus, um ein sicheres Online-Verhalten hervorzurufen. Es werden auch Gelegenheiten benötigt, die sich auf das soziale und materielle Umfeld beziehen, die ein Verhalten möglich oder unmöglich machen.[42] Während der Zusammenhang zwischen Gelegenheit und Verhalten die Aufmerksamkeit von Forschern in anderen Bereichen, wie z. B. dem Ernährungsverhalten, auf sich gezogen hat,[43] ist der Einfluss der Gelegenheit auf das Online-Verhalten nur wenig erforscht. Das soziale Umfeld bezieht sich darauf, wie die Menschen um uns herum unser Verhalten beeinflussen. So stehen beispielsweise die Privatsphäre-Einstellungen der Nutzer sozialer Online-Netzwerke im Zusammenhang mit der Anzahl der Online-Freunde mit privaten Profilen.[44] Darüber hinaus zeigten Herath/Rao,[45] dass der soziale Einfluss von direkten Kollegen und Managern einen großen Einfluss auf sicheres Online-Verhalten in Unternehmen haben kann. Soweit ersichtlich wurde die Beziehung zwischen dem sozialen Umfeld und dem Online-Verhalten im privaten Umfeld jedoch nicht weiter untersucht.

Das materielle Umfeld bezieht sich auf die Verfügbarkeit von finanziellen Ressourcen, Zeit und Hilfsmitteln, die sichere Praktiken unterstützen. Viele Unternehmen bieten ihren Mitarbeitern Hilfsmittel an, wie z. B. Datenschutzbildschirme, die ein sicheres Online-Verhalten ermöglichen sollen. Solche Hilfsmittel und Ressourcen können dazu beitragen, das Selbstvertrauen der Mitarbeiter in das gewünschte Verhalten (Selbstwirksamkeit) zu stärken.[46] Die Rolle, die das materielle Umfeld für das Online-Verhalten außerhalb von Unternehmen spielt, war bisher selten Gegenstand von Studien. Es ist daher unklar, wie das materielle Umfeld das Online-Verhalten in einem privaten Umfeld beeinflusst, in dem nicht die gleichen Hilfsmittel wie in einem Unternehmen zur Verfügung stehen; die Bürgerinnen und Bürger müssen selbst aktiv Sicherheitsmassnahmen beschaffen, installieren und auf dem neuesten Stand halten. Finanzielle Möglichkeiten sind daher ein relevanter Faktor: Personen, die wis-

42 Michie/van Stralen/West.
43 Michie/van Stralen/West.
44 Lewis/Kaufman/Christakis.
45 Lewis/Kaufman/Christakis.
46 Lewis/Kaufman/Christakis.

sen, dass sie keine persönlichen Fotos mit kostenlosen Übertragungswebsites verschicken sollten (Wissen), und die motiviert sind, eine sicherere – kostenpflichtige – Option zu nutzen (Motivation), brauchen auch einen finanziellen Spielraum, um dies tun zu können (Möglichkeit).

d) Andere Faktoren

Ein weiterer Faktor, der das Online-Verhalten beeinflussen kann, sind frühere Erfahrungen, wie z. B. frühere Opfererfahrungen im Internet. Frühere Erfahrungen können ein wichtiger Prädiktor für zukünftiges Verhalten sein.[47] Menschen können ihr Online-Verhalten anpassen, nachdem sie Opfer eines Cyberangriffs geworden sind, und beginnen, sich sicherer zu verhalten. So scheinen sich beispielsweise Facebook-Nutzer, die negative Erfahrungen gemacht haben, weil sie persönliche Informationen auf der Plattform geteilt haben, der Risiken stärker bewusst zu werden und sich besser zu schützen.[48] Allerdings weisen nicht alle Studien in diese Richtung, und eine frühere Viktimisierung führt nicht immer direkt zu einer Änderung des Online-Verhaltens.[49]

Es wurde auch argumentiert, dass Online-Verhalten mit der Selbstkontrolle zusammenhängt.[50] Die Theorie der Selbstkontrolle besagt, dass Menschen mit geringer Selbstkontrolle impulsiv sind, Risiken nicht vermeiden und sich hauptsächlich auf das Kurzfristige konzentrieren,[51] was ihr Risiko erhöht, Opfer von Internetkriminalität zu werden.[52] Der Zusammenhang zwischen Selbstkontrolle und Online-Viktimisierung kann jedoch auch indirekt durch andere Faktoren wie Motivation,[53] größere Online-Aktivität,[54] kriminelles Verhalten und Umgang mit Straftätern bestehen.[55] Es bleibt jedoch unklar, ob und wie die Beziehung zwischen Selbstkontrolle und Online-Viktimisierung durch das Online-Verhalten beeinflusst wird oder wie die Selbstkontrolle mit dem Online-Verhalten zusammenhängt.

Ein weiterer potenziell wichtiger Prädiktor für das Online-Verhalten ist der „locus of control" (Kontrollüberzeugung), ein Begriff, der sich auf das Verant-

---

47 Debatin et al.; Rhee/Kim/Ryu; Vance/Siponen/Pahnila.
48 Christofides, Muise, & Desmarais; Debatin et al.
49 Cain/Edwards/Still.
50 Bossler/Holt, effect; Ngo/Paternoster.
51 Gottfredson/Hirschi.
52 Ngo/Paternoster.
53 Floyd/Prentice-Dunn/Rogers.
54 van Wilsem.
55 Bossler/Holt, effect.

wortungsgefühl der Menschen in Bezug auf ihre eigene Sicherheit bezieht.[56] Ob jemand sich selbst für verantwortlich hält (d. h. „internal locus of control", d.h. der Ort der Kontrolle liegt innerhalb des Individuums) oder diese Verantwortung auf andere überträgt, z. B. auf die Polizei oder die Bank (d. h. „external locus of control", d.h. der Ort der Kontrolle liegt ausserhalb des Individuums), kann sich auf die Massnahmen auswirken, die sie ergreifen, um einen Cyberangriff zu verhindern, d. h. auf die Art und Weise, wie sie sich online verhalten).[57] Es wird erwartet, dass jemand mit einem hohen internen Kontrollzentrum Verantwortung übernimmt und motiviert ist, seine Online-Sicherheit selbst in die Hand zu nehmen. In der Tat haben frühere Studien einen positiven signifikanten Zusammenhang zwischen Kontrollüberzeugung und sicherem Online-Verhalten festgestellt).[58] Es ist jedoch auch möglich, dass eine grössere Kontrollüberzeugung zu einem falschen Gefühl der Sicherheit führt. Wenn Menschen sich zutrauen, Angriffe von Cyberkriminellen selbst abwehren zu können, unterschätzen sie möglicherweise die Online-Risiken,[59] was zu unsicherem Online-Verhalten führen kann.

III. Messung des Online-Verhaltens

Das Online-Verhalten und der Grad, in dem es sicher oder unsicher ist, wurde bisher auf zwei Arten gemessen. Einige Forscher haben das wahrgenommene Verhalten gemessen, indem sie die Befragten gefragt haben, wie sie sich normalerweise verhalten oder wie sie sich in einer fiktiven Online-Situation verhalten würden. In anderen Studien wurde das tatsächliche Online-Verhalten beobachtet. In diesem Abschnitt wird ein Überblick über die in früheren Studien verwendeten Methoden gegeben.

1. Forschung zum selbstberichteten Verhalten

Die meisten früheren Studien zum Online-Verhalten konzentrierten sich auf das selbstberichtete Verhalten. Die Befragten in diesen Studien wurden anhand von Items (z. B. „Ich öffne E-Mails von unbekannten Absendern") oder Fragen („Wie viel Prozent Ihrer Passwörter ändern Sie alle drei Monate?") zu ihrem Verhalten befragt.[60] Ein Beispiel für ein Forschungsinstrument, das mit Antwortvorschlägen arbeitet, ist der Human Aspects of Information Security

---

56 Rotter.

57 Debatin et al.; Jansen; Workman/Bommer/Straub.

58 Jansen; Workman/Bommer/Straub.

59 Rhee/Kim/Ryu.

60 Cain/Edwards/Still; Crossler/Bélanger.

Questionnaire (d. h. HAIS-Q).[61] Dieses Instrument misst insbesondere das Wissen, die Einstellungen und das wahrgenommene Verhalten zu einer Reihe von relevanten Themen, wie z. B. Passwortmanagement.

Selbstberichtete Verhaltensweisen können auch in der Fragebogenforschung mithilfe von Vignetten und Rollenspielen untersucht werden.[62] Diese Methoden ermöglichen es, die Befragten zu dem Verhalten zu befragen, das sie ihrer Meinung nach in einer fiktiven, von den Forschern vorgegebenen Situation zeigen würden.[63] Ein wichtiger Vorteil dieser Forschungsmethode besteht darin, dass sie es den Forschern ermöglicht, situative Faktoren zu ermitteln, die in der Fragebogenforschung zu Verzerrungen führen könnten. In einem Rollenspiel können die Forscher einerseits bestimmte Faktoren bei allen gleichsetzen (z. B. „Stellen Sie sich vor, Ihr Name ist Tom Johnson und Sie arbeiten in einer Bäckerei"). Andererseits können die Forscher Faktoren manipulieren, indem sie Untergruppen von Befragten eine angepasste Situation präsentieren. So können die Forscher beispielsweise zwischen Untergruppe eins („Stellen Sie sich vor, Sie sind noch nie Opfer eines Verbrechens geworden") und Untergruppe zwei („Stellen Sie sich vor, Sie wurden in der Vergangenheit in einem Online-Webshop betrogen") unterscheiden. Basierend auf den skizzierten Umständen werden die Befragten gefragt, wie sie in dieser Situation handeln würden.[64]

Die Fragebogenforschung hat als Forschungsmethode mehrere Vorteile. Zum Beispiel sind die Kosten für Befragungen relativ gering, während damit eine grosse repräsentative Forschungspopulation erreicht werden kann. Die Antworten auf standardisierte Fragen eignen sich auch für die quantitative Analyse, um erklärende Faktoren zu unterscheiden und Antworten zwischen den Befragten leicht vergleichen zu können.

Die Erforschung des Verhaltens anhand von Fragebögen und Vignetten hat jedoch auch Nachteile. Bei Studien zum selbstberichteten Verhalten konzentrieren sich die Forscher darauf, wie sich die Menschen nach eigenen Angaben typischerweise online verhalten oder wie sie sich in einer hypothetischen Situation verhalten würden. Obwohl die meisten Menschen angeben, dass Cybersicherheit wichtig ist,[65] entspricht ihr selbst angegebenes Verhalten nicht

61 Parsons et al., Determining; Parsons et al., Human.

62 Downs/Holbrook/Cranor; Jong/Leukfeldt/van de Weijer; Sheng et al..

63 Vance/Siponen/Pahnila.

64 Downs/Holbrook/Cranor; Jong/Leukfeldt/van de Weijer; Sheng et al..

65 Madden/Rainie.

immer ihrem tatsächlichen Verhalten.[66] Wenn sich die Forschung ausschließlich auf das selbstberichtete Online-Verhalten konzentriert, kann sie ein falsches Bild davon vermitteln, wie sich Menschen tatsächlich online verhalten.

2. Forschung zum tatsächlichen Online-Verhalten

Anstelle des selbstberichteten Verhaltens kann die Forschung auch das tatsächliche Verhalten messen. Bisherige Studien, in denen das tatsächliche Verhalten gemessen wurde, sind im Bereich der Cybersicherheit rar. Die Studien, die durchgeführt wurden, konzentrieren sich meist auf Phishing-Viktimisierung. In diesen Studien werden häufig Phishing-Tests durchgeführt, bei denen sowohl gefälschte Phishing-E-Mails als auch legitime E-Mails verwendet werden, um den Grad der Anfälligkeit für Phishing zu messen, d. h. um die Widerstandsfähigkeit gegenüber Phishing-Angriffen zu testen.[67] Indem gemessen wird, wie oft die Hyperlinks in den E-Mails angeklickt werden und wie oft Personen, die darauf klicken, tatsächlich vertrauliche oder persönliche Informationen auf einer legitimen oder einer Phishing-Website hinterlassen, kann ermittelt werden, wie sicher sich Menschen online in Bezug auf Phishing verhalten. Ein wichtiger Einwand gegen diese Methode ist, dass Menschen zu Forschungszwecken in die Irre geführt werden, da die Teilnehmer an einem Phishing-Test oft nicht im Voraus ihre Zustimmung zur Teilnahme gegeben haben.

Kaptein et al.[68] untersuchten, wie leicht es ist, Menschen dazu zu bringen, persönliche Informationen preiszugeben. Genauer gesagt untersuchten sie E-Mail-Adressen, die Cyberkriminelle bei Phishing-Angriffen verwenden. Die Teilnehmer füllten zunächst eine Umfrage aus, die aus so genannten Dummy-Fragen bestand: Die Fragen spielten keine Rolle. Die eigentliche Messung fand statt, nachdem die Befragten die Umfrage abgeschlossen hatten. Die Befragten wurden gebeten, E-Mail-Adressen von Freunden und Bekannten anzugeben, die möglicherweise ebenfalls an der Umfrage teilnehmen wollten. Bei dieser Aufforderung wurden verschiedene Überredungstechniken angewandt. So wurde den Befragten beispielsweise mitgeteilt, dass andere Befragte bereits verschiedene E-Mail-Adressen an die Forscher weitergegeben hatten (Social Proof) oder dass sie die Ergebnisse der Studie zugeschickt bekämen, wenn sie mindestens eine E-Mail-Adresse angeben würden (Reziprozität). Die Anwendung einer Überzeugungstechnik führte dazu, dass deutlich mehr E-Mail-Adressen gewonnen wurden.

---

66 Smith/Louis; Spiekermann/Grossklags/Berendt.

67 Siehe z.B. Cain/Edwards/Still für einen Überblick.

68 Kaptein et al.

Junger/Montoya Morales/Overink[69] sind noch einen Schritt weiter gegangen. Sie untersuchten, wie einfach es ist, Menschen dazu zu verleiten, persönliche Daten anzugeben, die für eine effektivere Form des Phishings verwendet werden können, nämlich das Spear-Phishing, bei dem die persönlichen Daten des Opfers verwendet werden, um ihm ein falsches Gefühl der Sicherheit zu vermitteln. Im Rahmen der Studie wurden Personen auf der Straße angesprochen, um an einer Umfrage teilzunehmen. In dieser Umfrage wurde eine Reihe von Fragen zum Online-Einkaufsverhalten gestellt: ob sie schon einmal etwas online gekauft hatten, und wenn ja, wo und was. Sie wurden auch gebeten, einen Teil ihrer persönlichen Identifikationsnummer und E-Mail-Adresse anzugeben. Überraschenderweise waren die Menschen bereit, den Interviewern solche persönlichen Informationen zu geben. Mit diesen Informationen lässt sich möglicherweise ein sehr gezielter und effektiver (Spear-)Phishing-Angriff durchführen.

Diese Art von Studien hat jedoch auch einige Nachteile. Obwohl sie bessere Messungen des tatsächlichen Online-Verhaltens liefern, werden die Studien oft in kleinem Massstab durchgeführt und es werden nur wenige andere Faktoren erhoben. Daher kann das beobachtete tatsächliche Online-Verhalten nicht auf erklärende Faktoren zurückgeführt werden. Ausserdem sind Messungen des tatsächlichen Verhaltens nicht in allen Situationen durchführbar, zum Beispiel wenn wir wissen wollen, wie sich Menschen während eines tatsächlichen Ransomware-Angriffs verhalten. Darüber hinaus können solche Messungen kostspielig und zeitaufwändig sein.

3. Selbstberichtetes Verhalten versus tatsächliches Verhalten

Das Online-Verhalten kann also auf verschiedene Weise gemessen werden. Wir argumentieren, dass Messungen des tatsächlichen Verhaltens den Selbstberichten über das Verhalten vorzuziehen sind. Selbstberichte können von der Realität abweichen, weil sie an die Erinnerung der Befragten appellieren oder weil die Befragten möglicherweise sozial erwünschte Antworten geben. Daher können Messungen des tatsächlichen Online-Verhaltens einen wichtigen Beitrag zu unserem Wissen über die Umstände leisten, die das Online-Verhalten beeinflussen.[70] Allerdings haben solche Messungen auch praktische Nachteile. Für jede Studie muss daher die am besten geeignete Methode zur Messung des Online-Verhaltens im Hinblick auf Kosten und Nutzen bestimmt werden.

---

69 Junger/Montoya Morales/Overink.

70 Maimon/Louderback.

Eine Kombination des Besten aus beiden Welten kann durch ein „bevölkerungsbasiertes Umfrageexperiment", auch „experimentelle Umfrage" genannt, erreicht werden.[71] Diese Methode verbindet die Vorteile der Fragebogenforschung, wie die Möglichkeit, eine grosse repräsentative Stichprobe zu untersuchen, mit den Vorteilen der experimentellen Forschung, bei der das tatsächliche Verhalten gemessen und kausale Zusammenhänge ermittelt werden können.[72] In der Praxis besteht eine solche experimentelle Umfrage häufig aus einem Online-Fragebogen mit integrierten Experimenten. Die Befragten können durch diese Experimente manipuliert werden (z. B. durch Auferlegung von Zeitdruck). Darüber hinaus können während der Umfrage Messungen des tatsächlichen Verhaltens vorgenommen werden....

IV. Studie über Online-Verhalten und Viktimisierung

1. Überblick über das Forschungsinstrument

Ziel der Studie über Online-Verhalten und Viktimisierung war es, ein Forschungsinstrument zu entwickeln, mit dem das tatsächliche Online-Verhalten gleichzeitig mit möglichen Erklärungsfaktoren, die sich aus der Literatur ergeben haben, gemessen werden kann. Es wurde ein bevölkerungsbasiertes Erhebungsexperiment verwendet, das aus einem Fragebogen mit Fragen und Vignetten zum selbstberichteten Online-Verhalten und den in Abschnitt II.2. diskutierten Erklärungsfaktoren (in Tabelle 1 dargestellt) sowie aus Messungen des tatsächlichen Online-Verhaltens mit experimentellen Manipulationen besteht. Darüber hinaus werden Hintergrundmerkmale der Befragten (z. B. Alter, Geschlecht, Bildungsniveau, beruflicher Status), die Stimmung der Befragten (z. B. das Ausmaß, in dem sich jemand optimistisch oder deprimiert fühlt) und das verwendete Gerät gemessen, um als Kontrollvariablen einbezogen zu werden. Abbildung 1 zeigt schematisch die Reihenfolge, in der die verschiedenen Abschnitte der Umfrage den Befragten vorgelegt werden.[73] Die verwendeten Items basieren auf bestehenden Fragebögen, die, falls erforderlich, ins Niederländische übersetzt und an den spezifischen Kontext dieser Studie angepasst wurden. Wenn kein Fragebogen zur Verfügung stand, wie z. B. für die Messung der Chancen, wurde ein Fragebogen von den Forschern selbst entwickelt.

---

71 Mutz.

72 Mullinix et al.

73 Eine englische Übersetzung des niederländischen Originalfragebogens ist auf Anfrage bei den Autoren erhältlich.

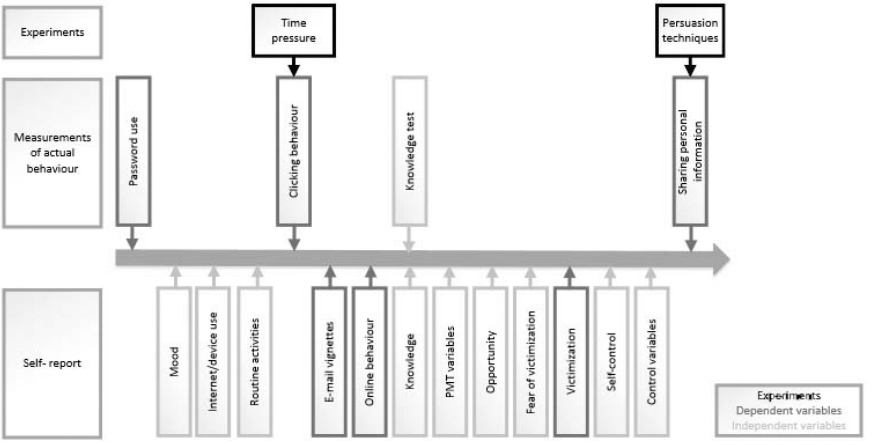


Abbildung 1: Schematischer Überblick über die Reihenfolge der Erhebungsabschnitte

Teil der Befragung	**Theoretische Grundlage**	**Thema**
Motivation	**PMT und COM-B**	**Motivation zum Schutz**
Wissen	COM-B	Selbsteinschätzung des Wissens über Online-Sicherheit
		Wissenstest (objektiv)
Gelegenheit	COM-B	Materielles Umfeld
		Soziales Umfeld
Stimmungslage		Stimmungslage (PANAS)
Viktimisierung		Kriminalitätsfurcht
	PMT	Frühere Online-Viktimisierung
Selbstkontrolle		Self-control (BSCS)
Gerät		Art des Geräts, das zum Ausfüllen der Umfrage verwendet wurde
		Nutzung von Online-Geräten
		Sicherheitsmassnahmen
Zeitdruck		Zeitdruck
Überredungstechnik		Autorität
		Reziprozität

Teil der Befragung	Theoretische Grundlage	Thema
Motivation	**PMT und COM-B**	**Motivation zum Schutz**
Einschätzung der Bedrohung	PMT	Wahrgenommene Verwundbarkeit
		Wahrgenommener Schweregrad
Einschätzung der Coping-Fähigkeiten	PMT	Wirksamkeit der Reaktion
		Selbstwirksamkeit
		Reaktionskosten
Locus of Control		Kontrollüberzeugung
Kontrollierende Faktoren		Geschlecht
		Bildungsgrad
		Alter
		Tägliche Aktivität/Beschäftigung
		Zusammenlebend (ja/nein)
		Kinder (< 16 Jahre) im Haushalt
Routineaktivitäten		Internet-Nutzung
		Online-Aktivitäten

Tabelle 1: Überblick über die Themen der Umfrage, die nicht das Online-Verhalten betreffen

2. Messung von sieben Clustern des Online-Verhaltens

Das in diesem Kapitel vorgestellte Forschungsinstrument misst sieben Verhaltenscluster, die auf der Literaturstudie basieren. In dieser experimentellen Umfrage wird das Online-Verhalten auf drei Arten gemessen. Erstens werden alle Verhaltenskomplexe durch Selbstauskünfte gemessen (siehe Tabelle 2 und Items in Anhang 1). Zweitens wurden echte Phishing-E-Mails so angepasst, dass sie als Vignetten verwendet werden konnten, um den Umgang der Befragten mit (Phishing-)E-Mails zu messen. Den Befragten werden drei E-Mails gezeigt, die an eine fiktive Person adressiert sind: zwei Phishing-E-Mails, die angeblich von einer Bank und einer Festivalorganisation stammen, und eine legitime E-Mail von einem Internetanbieter. Die Befragten wurden gebeten, so zu tun, als seien sie diese fiktive Person. Die Befragten wurden dann gebeten, aus neun Optionen zu wählen, wie sie auf jede dieser E-Mails reagieren wür-

den (z. B. antworten, auf einen Link klicken usw.). Die Befragten verhalten sich unsicher, wenn sie angeben, die verlinkte Website aus einer oder beiden Phishing-E-Mails zu öffnen.

Drittens werden die Befragten beim Ausfüllen der Umfrage mit (fiktiven) Cyber-Risikosituationen konfrontiert (siehe IV.2. für weitere Einzelheiten), um das tatsächliche Online-Verhalten in den Clustern „Passwortmanagement", „Online-Wachsamkeit" und „Online-Weitergabe von persönlichen Informationen" zu messen. Es erwies sich aus mehreren Gründen als unmöglich, das tatsächliche Online-Verhalten innerhalb der anderen Verhaltenskategorien zu messen. Erstens ist die Nachahmung von Cyberkriminalität nicht immer möglich oder moralisch gerechtfertigt, z. B. bei der Prüfung technischer Präventivmassnahmen. In einigen Fällen hat es sich auch als technisch nicht machbar erwiesen, eine Messung in zufriedenstellender Weise in den Fragebogen einzubauen. Daher wurde ein pragmatischer Ansatz gewählt und beschlossen, das Verhalten nur dann objektiv zu messen, wenn dies praktisch machbar und moralisch vertretbar ist. Tabelle 2 gibt einen Überblick über die Art und Weise, wie die einzelnen Online-Verhaltensgruppen in der Erhebung gemessen werden.

Online-Verhalten	**Methode**		
	Selbstauskunft Fragebogen	**Selbstauskunft Vignette**	**Objektive Messung**
1. Passwort-Verwaltung	Ja		Ja: Passwort-Stärke Keine experimentelle Variante
2. Sichern wichtiger Dateien	Ja		
3. Installation von Updates	Ja		
4. Verwendung von Sicherheitssoftware	Ja		
5. Online-Wachsamkeit	Ja		Ja: Klick-Verhalten Experimentelle Variante: Zeitdruck
6. Online-Offenlegung von persönlichen Informationen	Ja		Ja: Offenlegung von persönlichen Informationen Experimentelle Varianten: Überzeugungstechniken

Online-Verhalten	Methode		
	Selbstauskunft Fragebogen	**Selbstauskunft Vignette**	**Objektive Messung**
7. Umgang mit Anhängen und Hyperlinks in E-Mails	Ja	Ja	

Tabelle 2: Überblick über die Messungen des Online-Verhaltens nach Verhaltensclustern

3. Detaillierte Beschreibung der Messungen des tatsächlichen Online-Verhaltens

Die Messungen des tatsächlichen Online-Verhaltens in der experimentellen Erhebung der Online Behaviour and Victimization Study werden nun im Detail beschrieben. Es gibt drei objektive Messungen des Online-Verhaltens, die in der Umfrage enthalten sind (Tabelle 2). Beim Ausfüllen der Umfrage wurden die Befragten ohne ihr Wissen mit drei simulierten Cyber-Risikosituationen konfrontiert, und es wurde erfasst, wie die Befragten mit diesen Situationen umgehen. Zunächst wurden die Befragten zu Beginn des Fragebogens gebeten, aus Gründen des Datenschutzes einen Benutzernamen und ein Passwort zu erstellen (siehe Abbildung 2). Das gewählte Passwort wurde zwar nicht registriert, aber die Stärke des gewählten Passworts wurde gemessen. Dies ermöglicht es, die Stärke der Passwörter zu bestimmen, die die Befragten zum Schutz ihrer persönlichen Daten wählen. Am Ende der Umfrage wurde den Befragten eine Kontrollfrage gestellt, um herauszufinden, ob sie normalerweise eine ähnliche Art von Passwort wählen würden: „Haben Sie ein ähnliches Passwort gewählt wie das, das Sie normalerweise zum Schutz Ihrer persönlichen Daten wählen würden?“

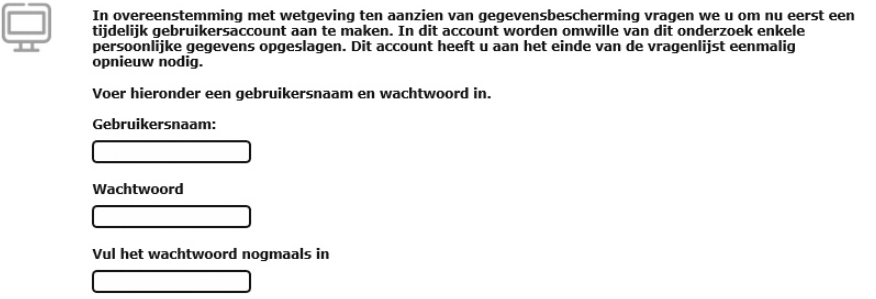


Abbildung 2: Screenshot der Messung der Passwortverwaltung[74]

Im weiteren Verlauf der Umfrage wurde gemessen, inwieweit die Befragten online aufmerksam sind. Die Befragten wurden gebeten, sich ein kurzes Video anzusehen, bevor sie die nächste Frage beantworten. Das Video wurde jedoch nicht abgespielt. Plötzlich erschien ein Pop-up-Fenster mit dem Hinweis, dass eine Software namens „Vidzzplay" heruntergeladen werden muss (siehe Abbildung 3). Diese Software stammt angeblich aus einer unbekannten Quelle (und ist daher unzuverlässig). Hier können die Forscher sehen, welche Wahl die Befragten treffen: die Software herunterladen (unsichere Wahl), nicht herunterladen (sichere Wahl) oder die Frage überspringen (sichere Wahl).

[74] Ransomware ist eine Schadsoftware, die einen Computer blockiert oder Dateien verschlüsselt. Erst wenn die betroffene Person ein Lösegeld zahlt, kann sie den Computer oder die Dateien wieder nutzen.

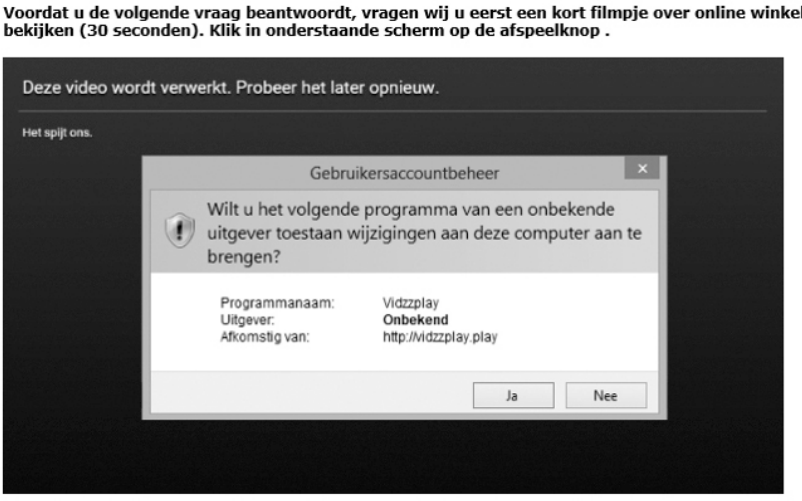


Abbildung 3: Screenshot der Messung der Online-Wachsamkeit[75]

Drittens wurden die Befragten am Ende des Fragebogens gebeten, persönliche Daten anzugeben. Dieser Teil begann mit Standardfragen wie dem Familienstand, aber der Datenschutzwert der Informationen stieg mit jeder Frage, z. B. nach dem vollständigen Namen, dem Geburtsdatum und der E-Mail-Adresse, und endete mit der Frage nach den letzten drei Ziffern ihres Bankkontos. Bei jeder Frage hatten die Befragten die Möglichkeit, auf die Schaltfläche „Ich möchte lieber nichts sagen" zu klicken, was als sichere Wahl gilt. Wenn die Befragten ihre persönlichen Daten ausfüllten, wurde der Inhalt ihrer Antwort nicht registriert, sondern nur, dass sie die Frage beantwortet hatten. Je mehr Arten von persönlichen Informationen die Befragten angaben, desto unsicherer ist ihr Verhalten.

4. Experimente

In zwei der Messungen des tatsächlichen Online-Verhaltens waren experimentelle Bedingungen enthalten (Tabelle 2). In diesen Fällen wurden verschiedenen Untergruppen von Befragten Variationen einer objektiven Messung des tatsächlichen Online-Verhaltens vorgelegt. Im ersten Experiment wurde bei der objektiven Messung des „Klickverhaltens", bei der die Befragten aufge-

[75] Spear-Phishing ist ein gezielter Phishing-Angriff gegen eine Person oder eine bestimmte Gruppe von Personen.

fordert werden, Software herunterzuladen, die Hälfte der Befragten unter Zeitdruck gesetzt. Die Befragten wurden gebeten, einen Teil der Umfrage in höchstens fünf Minuten auszufüllen. In der Versuchsbedingung wurde den Befragten gesagt, dass diese Zeit für frühere Befragte nicht ausreichend war, und sie wurden aufgefordert, schnell zu arbeiten. Die anderen Befragten wurden darüber informiert, dass fünf Minuten ausreichend sind und dass sie in ihrem eigenen Tempo weiterarbeiten können. Dann wurden die Befragten zu ihren Online-Routineaktivitäten befragt. Danach wurden die Befragten gebeten, sich ein Video anzusehen, und es erschien ein Pop-up mit der Bitte um Erlaubnis für einen Software-Download (Messung des tatsächlichen Klickverhaltens). Im Anschluss daran wurden Kontrollfragen zum erlebten Zeitdruck gestellt.

Das zweite Experiment fand während der objektiven Messung der „Online-Offenlegung persönlicher Daten" statt, bei der die Befragten aufgefordert wurden, persönliche Daten wie ihre Adresse und die letzten drei Ziffern ihrer Kontonummer einzugeben. Es wurden verschiedene Überzeugungstechniken eingesetzt, um die Bereitschaft der Befragten zur Weitergabe persönlicher Daten zu manipulieren (⅓ die Überzeugungstechnik „Autorität", ⅓ die Überzeugungstechnik „Gegenseitigkeit", ⅓ keine Überzeugungstechnik). Allen Befragten wurde gesagt: „Wir würden Ihnen gerne einige abschliessende Fragen stellen". Ein Drittel der Befragten ging zu den Fragen nach persönlichen Informationen über, ohne eine Überzeugungstechnik anzuwenden. In der Kategorie Reziprozität (ein Drittel der Befragten) wurde den Befragten die Chance auf einen Gutschein versprochen, wenn sie alle Fragen zu persönlichen Informationen vollständig beantworten. In der Kategorie Autorität (ein Drittel der Befragten) drängten die Forscher die Befragten aufgrund der Bedeutung der wissenschaftlichen Studie dazu, alle persönlichen Angaben vollständig zu machen.

V. Diskussion

In diesem Beitrag wurde die Entwicklung eines Forschungsinstruments für die Studie *Online Behaviour and Victimization Study* beschrieben. Die zu Beginn dieser Studie durchgeführte Literaturrecherche zeigt deutlich, dass es an Studien mangelt, die das tatsächliche Online-Verhalten messen. Eine Erklärung dafür ist, dass dieser Forschungsbereich noch relativ jung ist. Die meisten Studien, die durchgeführt wurden, können als explorativ angesehen werden oder testen hauptsächlich, ob bestehende kriminologische oder psychologische Modelle zur Erklärung des selbstberichteten unsicheren Online-Verhaltens oder der Viktimisierung von Internetkriminalität verwendet werden

können.[76] Die verfügbaren Studien, in denen das tatsächliche Online-Verhalten gemessen wurde, hatten mit Einschränkungen zu kämpfen, da beispielsweise eine nicht repräsentative Stichprobe verwendet wurde. Darüber hinaus haben diese Studien zwar wertvolle Ergebnisse zur Prävalenz unsicheren Online-Verhaltens geliefert, sich aber nur selten auf ein breites Spektrum an erklärenden Faktoren ausgerichtet. Ein möglicher Zusammenhang zwischen Faktoren wie Wissen und Motivation und der Prävalenz des tatsächlichen (objektiv gemessenen) Online-Verhaltens ist bisher kaum untersucht worden. Auch der Zusammenhang zwischen unsicherem tatsächlichen Online-Verhalten und Online-Viktimisierung wurde bisher kaum untersucht. In einigen Studien wurde zwar beschrieben, dass Online-Viktimisierung auf unsicheres Online-Verhalten zurückgeführt werden kann, wie z. B. die Weitergabe persönlicher Informationen im Internet, doch bleibt unklar, wie unsicheres Online-Verhalten das Risiko der Online-Viktimisierung beeinflusst oder wie dies mit individuellen oder kontextuellen Faktoren zusammenhängen könnte.

Mit der *Online Behaviour and Victimization Study* wurde daher ein Forschungsinstrument entwickelt, das in verschiedener Hinsicht neue Möglichkeiten für das Forschungsfeld bietet. Es wurde bewusst entschieden, sowohl das selbstberichtete als auch das tatsächliche Online-Verhalten zu messen. Schliesslich wissen wir, dass, obwohl die meisten Menschen angeben, Cybersicherheit sei wichtig, das tatsächliche Verhalten der Menschen nicht immer mit ihren Einstellungen oder ihrem wahrgenommenen Verhalten übereinstimmt. Durch die Verwendung eines bevölkerungsbasierten Umfrageexperiments – eine Methode, die die Vorteile der Fragebogenforschung mit den Vorteilen von Experimenten verbindet – ist der Mehrwert dieses Forschungsinstruments offensichtlich: Dieses Instrument ermöglicht es, über bestehende Studien hinauszugehen, indem es das tatsächliche Online-Verhalten in einer grossen repräsentativen Stichprobe misst. Darüber hinaus ist dieses Instrument auch in anderer Hinsicht innovativ: Wir zielen nicht nur darauf ab, die Viktimisierung bestimmter Formen von Cyberkriminalität zu erklären, sondern auch mehrere Cluster von Online-Verhalten. Schließlich sind es Verhaltensweisen, die das Risiko für alle Arten von Online-Kriminalität erhöhen.

Bei der Konzeption der experimentellen Umfrage ergaben sich mehrere ethische Fragen, die im Einzelnen erörtert werden sollten. Während der experimentellen Umfrage werden den Befragten verschiedene fiktive Cyber-Risikosituationen präsentiert. Die Befragten werden auch aufgefordert, ein Passwort zu erstellen und persönliche Daten einzugeben. Darüber hinaus wurde befürchtet, dass (im Vergleich zu anderen Studien) auffällige Fragen und

[76] Für einen Überblick siehe Leukfeldt, Research.

Situationen die Befragten abschrecken würden, was zu einer hohen Zahl von Abbrüchen oder Kontakten mit dem Helpdesk führen könnte.[77] Eine Ethikkommission der Universität hat daher das Instrument genehmigt. Die Abfrage eines Passworts und persönlicher Daten ist ethisch zulässig, wenn die Antworten nicht registriert werden. So bleibt den Forschern beispielsweise unbekannt, welches Passwort die Befragten wählen, nur wie stark dieses Passwort ist. Darüber hinaus werden die persönlichen Daten, die die Befragten ausfüllen, nicht an die Forscher weitergegeben, sondern nur, ob die Befragten eine bestimmte Frage zu persönlichen Informationen beantworteten oder nicht. Schliesslich wurden alle Befragten (so weit wie möglich) im Voraus durch eine „informierte Zustimmung" informiert und anschliessend durch eine „Nachbesprechung" über die Cyber-Risikosituationen und Manipulationen informiert, denen sie „ausgesetzt" waren (unabhängig davon, ob die Befragten die Umfrage abgeschlossen haben oder nicht).

Wie jedes Messinstrument hat auch dieses Forschungsinstrument seine Grenzen. Erstens misst das Forschungsinstrument sowohl abhängige als auch erklärende Faktoren zum gleichen Zeitpunkt. Um kausale Zusammenhänge zwischen Verhalten und Viktimisierung zu untersuchen, ist eine zweite Welle der Datenerhebung erforderlich, bei der insbesondere die Viktimisierung durch Internetkriminalität im Zeitverlauf gemessen wird.

Zweitens haben die objektiven Messungen und Experimente auch jeweils ihre eigenen Grenzen. Aufgrund der Länge des Fragebogens war es nicht möglich, objektive Messungen und Experimente für alle sieben Verhaltenscluster aufzunehmen. Darüber hinaus wird zwar die Passwortstärke ermittelt, aber es bleibt unbekannt, ob das Passwort einmalig ist und vom Befragten nie in anderen Anwendungen verwendet wird, was eine zweite Voraussetzung für eine sichere Passwortverwaltung ist. Darüber hinaus werden die Informationen, die die Befragten weitergeben, gemäß der Datenschutz-Grundverordnung[78] nicht aufgezeichnet, so dass nicht überprüft werden kann, ob es sich um tatsächliche/richtige Daten handelt. Bei der Messung, ob die Befragten unsichere Software heruntergeladen haben oder nicht (d. h. beim Klickverhalten), verwendet das Instrument ein Popup-Fenster im Stil des Windows-Betriebssystems. Nicht-Windows-Benutzer sind mit dem Pop-up weniger vertraut, was sie möglicherweise misstrauischer macht und die Wahrscheinlichkeit verringert, dass sie

---

77 Bei einem Pilotversuch mit dem Forschungsinstrument trat dieser Effekt jedoch nur selten auf.

78 Allgemeine Datenschutz-Verordnung (General Data Protection Regulation GDPR), <https://gdpr-info.eu/>.

die Frage bejahen. Diese objektive Messung muss weiterentwickelt werden, und zwar mit verschiedenen Pop-ups, die technisch gesehen echte Pop-ups sind und an verschiedene Geräte und Betriebssysteme angepasst werden.

Drittens: Obwohl die Methode – eine Umfrage mit Experimenten – für diese Art von Forschung sehr gut geeignet ist, ist es möglich, dass sich die Befragten in der Online-Umgebung der Umfrage sicher fühlen. Infolgedessen treffen sie möglicherweise schneller unsichere Entscheidungen als in tatsächlichen Cyber-Risikosituationen im wirklichen Leben. Dies kann bedeuten, dass der Prozentsatz des unsicheren Verhaltens in der häuslichen Umgebung geringer ist als durch das Forschungsinstrument ermittelt. Es ist jedoch wichtig zu erwähnen, dass der Zweck des Forschungsinstruments darin besteht, das Online-Verhalten in einer scheinbar sicheren Umgebung zu messen – Kriminelle imitieren oft auch eine sichere Umgebung (z. B. eine Online-Bank oder einen Webshop) und verleiten Menschen dazu, auf einen Hyperlink zu klicken oder persönliche Informationen preiszugeben.

Schließlich ist es möglich, dass sich Teilnehmer von Nicht-Teilnehmern in Bezug auf nicht registrierte Eigenschaften unterscheiden. Angesichts des Ziels der Studie werden die Befragten im Voraus nicht vollständig über den Inhalt der Studie informiert. Die Befragten erwarten, dass sie nur Fragen darüber beantworten, was sie online tun. Bestimmte Fragen könnten Teilnehmer, die misstrauisch sind, abschrecken. Daher könnten Befragte, die misstrauischer/aufmerksamer sind, die Studie schneller abbrechen.

Trotz der hier erwähnten Einschränkungen ermöglicht dieses Forschungsinstrument die Untersuchung des selbstberichteten Online-Verhaltens und des tatsächlichen Online-Verhaltens sowie der Unterschiede zwischen beiden und die Erklärung des Auftretens von unsicherem Online-Verhalten und der Viktimisierung durch Internetkriminalität. Dies ist relevant für künftige Interventionen, die darauf abzielen, das Online-Verhalten sicherer zu machen…

Literaturverzeichnis

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior. *Information and Computer Security*. https://doi.org/10.1108/ICS-03-2018-0037

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *Mis Quarterly*, 39(4).

Bossler, A. M., & Holt, T. J. (2009). On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 3(1), 400–420.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227–236.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45.

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior. *Journal of Adolescent Research*, 27(6), 714–731.

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice*, (518).

Crossler, R. E., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database*, 45(4), 51–71.

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1–15.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, 32, 90–101.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups – 2nd annual eCrime researchers summit* (pp. 37–44). New York, New York, USA: ACM Press.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30,(2,), 407–429.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford: Stanford University Press.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125.

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, 29(4), 420–436.

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Doctoral thesis. Gildeprint.

Jansen, J., & Leukfeldt, R. (2015). How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases. In *Proceedings – 5th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2015* (pp. 24–31).

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91.

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology*, 6(2), 205–228.

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, 25(2), 165–180.

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, 53(2), 22–30.

Jong, L., Leukfeldt, R., & van de Weijer, S. (2018). Determinanten en motivaties voor intentie tot aangifte na slachtofferschap van cybercrime. *Tijdschrift Voor Veiligheid*, 17(1–2), 66–78.

Junger, M., Montoya Morales, A. L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66.

Kaptein, M., Markopoulos, P., De Ruyter, B., & Aarts, E. (2009). Can you be persuaded? Individual differences in suceptibility to persuasion. In *IFIP Conference on Human-Computer Interaction. Springer, Berlin, Heidelberg.* (pp. 115–118).

Kaye, J. (2011). Self-reported password sharing strategies. *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems – CHI '11*, 2619.

Leukfeldt, E.R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, 17(8), 551–555.

Leukfeldt, E.R. (Ed.). (2017). *Research Agenda the Human Factor in Cybercrime and Cybersecurity*. Den Haag: Eleven International Publishing.

Leukfeldt, E.R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks. *British Journal of Criminology*, 57(3), 704–722.

Leukfeldt, E.R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263–280.

Leukfeldt, Eric Rutger, Notté, R. J., & Malsch, M. (2019). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims and Offenders*, 15(1), 60–77.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1), 79–100.

Lusthaus, J. (2018). Honour Among (Cyber)thieves? *European Journal of Sociology*, 59(2), 191–223.

Madden, M., & Rainie, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*(1).

Michie, S., Stralen, M. M. Van, & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions, *42*(6).

Mullinix, K. J., Leeper, T. J., Druckman, J. N., & Freese, J. (2015). The Generalizability of Survey Experiments. *Journal of Experimental Political Science*, *2*(2), 109–138.

Mutz, D. C. (2011). *Population-based survey experiments*. Princeton: Princeton University Press.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection Motivation Theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour* (pp. 81–127). Open University Press.

Ovelgönne, M., Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks. *ACM Transactions on Intelligent Systems and Technology*, *8*(4), 1–25.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, *80*(1).

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382.

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*.

Smith, J. R., & Louis, W. R. (2008). Do as we say and as we do: The interplay of descriptive and injunctive group norms in the attitude-behaviour relationship. *British Journal of Social Psychology*, *47*(4), 647–666.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd Generation E-Commerce : Privacy Preferences versus actual Behavior. *ACM Conference on Electronic Commerce*, 1–10.

Symantec. (2018). *Security Center White Papers*. Retrieved from https://www.symantec.com/security-center/white-papers

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *ARES 2010 – 5th International Conference on Availability, Reliability, and Security*, 196–203.

Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of Bluetooth security. *Information Management and Computer Security*, *20*(5), 364–381.

Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559.

Van Wilsem, J. (2013). „Bought it, but never got it" assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178.]

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4).

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816.

Appendix

R = Umgekehrt formulierte Frage-Items

Fragen
Passwort-Verwaltung
Ich teile meine persönlichen Passwörter mit anderen (R)
Ich verwende einfache, kurze Passwörter, z. B. mit nur 1 Zahl oder einem Großbuchstaben (R)
Ich verwende dasselbe Passwort für verschiedene Anwendungen, zum Beispiel für soziale Medien, Online-Banking und Webshops (R)
Sichern von wichtigen Dateien
Ich erstelle Sicherheitskopien von wichtigen Dateien
Ich speichere persönliche Informationen verschlüsselt, so dass andere sie nicht ohne weiteres lesen können
Installation von Updates
Ich installiere Betriebssystem-Updates auf meinen Geräten, sobald ein neues Update verfügbar ist
Ich installiere Updates für die von mir verwendeten Anwendungen oder Software, sobald ein neues Update verfügbar ist
Ich aktualisiere meine Sicherheitssoftware, sobald ein neues Update verfügbar ist

Fragen
Verwendung von Sicherheitssoftware
Auf meinen Geräten ist eine Sicherheitssoftware installiert, die nach Viren und anderer schädlicher Software sucht
Ich verwende Browsererweiterungen,[79] die mir helfen, sicher zu surfen, z. B. Software zum Blockieren von Werbung oder Pop-ups
Online-Wachsamkeit
Ich lade Software, Filme, Spiele oder Musik aus illegalen Quellen herunter (R)
Ich nutze öffentliches Wi-Fi (z. B. in Hotels, Restaurants, Bars oder öffentlichen Verkehrsmitteln) ohne VPN-Verbindung[80] (R)
Ich überprüfe die Datenschutzeinstellungen meiner Geräte, Apps oder sozialen Medien
Online-Weitergabe von persönlichen Informationen
Ich gebe persönliche Informationen wie meine Wohnadresse, E-Mail-Adresse oder Telefonnummer über soziale Medien weiter (R)
Ich bin wählerisch bei der Annahme von Verbindungsanfragen in sozialen Medien von anderen
Umgang mit Anhängen und Hyperlinks in E-Mails
Ich lösche E-Mails, denen ich nicht traue, sofort
Wenn ich Zweifel an der Echtheit einer E-Mail habe, kontaktiere ich den Absender, um zu fragen, ob eine E-Mail tatsächlich an mich gesendet wurde
Ich öffne Anhänge in E-Mails, auch wenn die E-Mail von einem unbekannten Absender stammt (R)

79 Für einen Überblick siehe z.B. Leukfeldt, Research.

80 Crossler et al.; Debatin et al.

Kartenbetrug – Herausforderungen für die Prävention

Stefan Giger

Inhalt

I. Kartenbetrug

1. Betrugsarten und Schäden

Kartenbetrug hat viele Facetten. Dabei lassen sich die Täter ständig neue Vorgehensweisen einfallen. Generell wird zwischen Kredit- und Debitkartenbetrug unterschieden. Kreditkartenbetrug findet in erster Linie im Onlinebereich statt. Debitkartenbetrug hingegen ist vielfältiger. Meistens profitieren die Betrüger von der fehlenden Aufmerksamkeit ihrer Opfer. Deshalb kommt der Präventionsarbeit hier eine besondere Bedeutung zu. Die nachfolgenden Ausführungen konzentrieren sich allein auf den Debitkartenbetrug.

a) Art der Debitkartendelikte

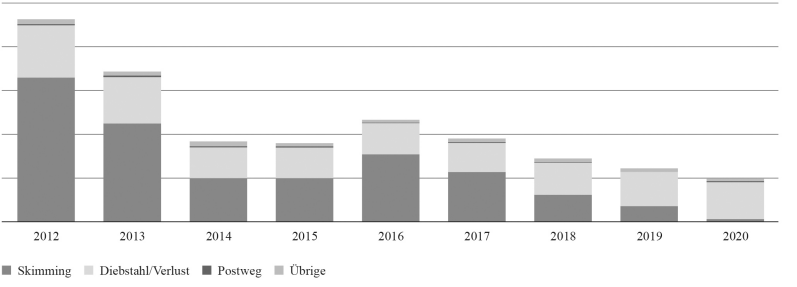
Im Gegensatz zum Ausland kennt die Schweiz keine Meldepflicht für Debitkartendelikte. Das bedeutet, dass wir hierzulande keine offiziellen Daten über die Art und Häufigkeit von Debitkartenbetrug erfassen.

Die UBS erfasst diese Daten jedoch seit vielen Jahren. Damit kann die Bank frühzeitig erkennen, wo die Täter aktiv sind und entsprechend reagieren.

Die Zahlen dazu publiziert die UBS nicht. Aus nachfolgender Grafik lässt sich dennoch eine klare Tendenz feststellen: Skimming-Fälle, also das Kopieren der Magnetstreifendaten, spielen heute kaum noch eine Rolle. Ein entscheidender Grund dafür ist, dass praktisch alle Banken weltweit in diesem Bereich massiv investiert haben. Debitkartentransaktionen erfolgen heute nicht mehr über den Magnetstreifen, sondern praktisch ausschliesslich über den Chip auf der Karte.

Unverändert gleich geblieben sind Kartendelikte durch Diebstähle oder den Verlust der Debitkarte. Die vermisste Karte wird in der Folge von den Tätern genutzt, um Geld abzuheben.

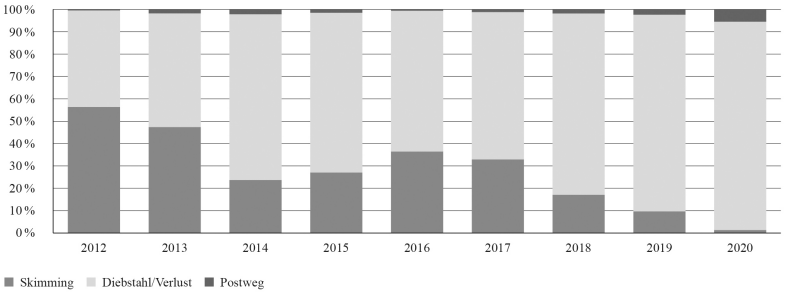
Alle weitere Kartendelikte sind vernachlässigbar.



Anzahl Schadenfälle mit UBS-Debitkarten nach Deliktart

b) Verursachte Schäden durch Debitkartdelikte

Interessant ist zu sehen, welche Schäden die einzelnen Delikte verursachen. Der grösste Schaden entsteht bei Kartendiebstählen und -verlusten – sowohl für die Kundinnen und Kunden als auch für die UBS als Bank.



Schadensumme nach Deliktart bei Schadenfällen mit UBS-Debitkarten

Hohe Schadensummen entstehen jeweils dann, wenn der Kartendiebstahl mit einem PIN-Verlust verbunden ist. Nur im Besitz der PIN (Personal Identification Number) können Täter grosse Geldsummen abheben. Vergleicht man dazu die Schäden aus kontaktlosen Abbuchungen – also Abbuchungen ohne PIN-Abfrage – sind diese vernachlässigbar. Sie machen nur gerade vier Prozent der Gesamtschadensumme aus.

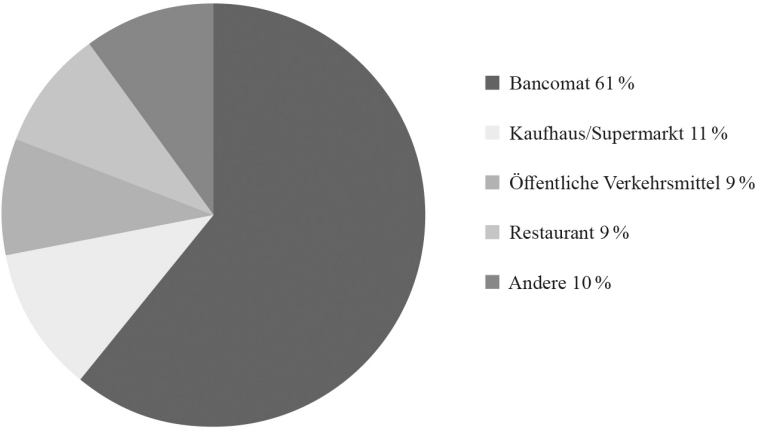
2. Tatort und Opferprofil

Die Wahrscheinlichkeit, Opfer eines Kartendelikts zu werden ist relativ gering. Wir können sowohl das Opferprofil als auch den Ort des Kartendelikts sehr klar eingrenzen.

In der Regel sind die Opfer über 65 Jahre alt, wohnen oft in der Westschweiz und das Delikt geschieht weitaus am häufigsten direkt am Bankomaten, währenddem sie ihre PIN eingeben.

a) Ort des Kartendiebstahls

Das nachfolgende Kreisdiagramm schlüsselt auf, wo von 2012 bis 2020 die Kartendelikte bei UBS-Kunden stattfanden.



Ort des Kartendiebstahls von UBS-Debitkarten

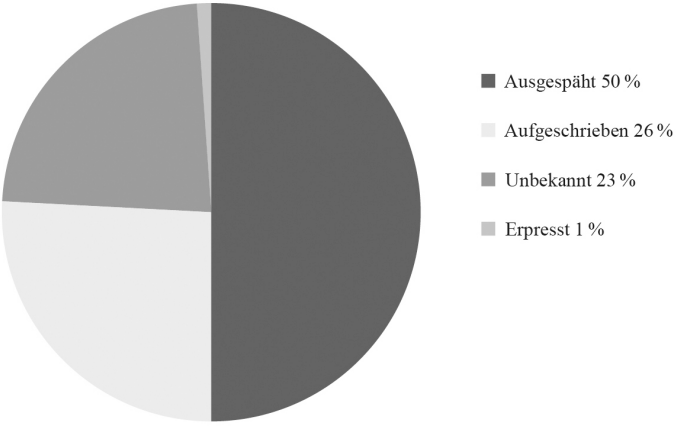
Neben Bankomaten sind auch Kaufhäuser und Supermärkte beliebte Tatorte. In der Regel läuft das so ab, dass die Opfer vor dem Einkauf noch Geld abheben. Dabei wird ihre PIN von den Tätern ausspioniert. Die Karte beziehungsweise das Portemonnaie wird dann im Supermarkt gestohlen. Die Opfer bemerken es erst an der Kasse und die Täter haben zwischenzeitlich schon das Konto geplündert.

Ähnlich ist das Vorgehen bei den öffentlichen Verkehrsmitteln. Die PIN wird am Billettautomaten eingegeben, die Brieftasche wird auf dem Weg zum Perron gestohlen. Das Opfer bemerkt es erst, wenn es das Billett im Zug vorweisen muss, und die Täter haben zwischenzeitlich bereits Geld vom Konto gestohlen.

Bei den Restaurationsbetrieben finden die Taten häufig in Selbstbedienungsrestaurants statt. Die PIN-Eingabe erfolgt an der Kasse, danach wird das Portemonnaie in der Jacke verstaut und diese über den Stuhl gehängt. Ein leichtes Spiel für die Täter.

b) Ort der PIN-Ausspähung

Wie die Täter zur PIN kommen, ist nicht immer ganz klar. Bei der UBS haben wir diese Daten anhand des Tatvorgehens und der Angaben von Opfern erhoben.



Erlangung der PIN bei Kartendelikten mit UBS-Debitkarten

Weitaus am häufigsten (50 Prozent) wird die PIN direkt bei der Transaktion – am Bankomaten oder Zahlautomaten ausgespäht. Auffallend ist aber auch, dass in 26 Prozent der Fälle die PIN vom Opfer irgendwo aufgeschrieben wurde.

c) Herkunft der Opfer

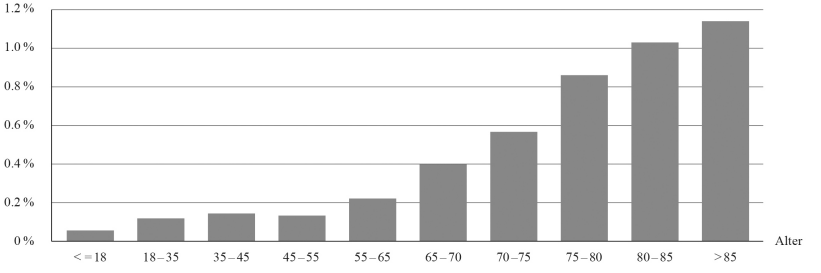
Betrachtet man den Wohnort der Opfer, so fällt auf, dass das Risiko, Opfer von Kartendelikten zu werden, steigt, je weiter westlich man in der Schweiz wohnt. Ein Grossteil der Opfer lebt in der Romandie. Das hat damit zu tun, dass die Täter mehrheitlich aus Frankreich über die Grenze kommen. Meist stammen sie ursprünglich aus dem Maghreb und sprechen Französisch. Das Risiko, Opfer eines Kartendelikts zu werden, ist im Kanton Genf 21-mal höher als im Kanton Appenzell Ausserrhoden. Ein Ausreisser bildet einzig der Kanton Glarus. Die erhöhten Opferzahlen im Glarnerland lassen sich damit erklären, dass die Taten nicht unbedingt in Glarus selbst, sondern oft in Zürich stattfinden.

Wohnort der Opfer von Lost/Stolen Fraud im Verhältnis zur Grundgesamtheit aller UBS-Kartenkunden
Lesebeispiel: Je dunkler, desto grösser ist das Risiko, Opfer eines Kartendeliktes zu werden.

Wohnort der Opfer von Debitkartendelikten bei der UBS

d) Alter der Opfer

Die UBS hat auch das Alter der Kartenbesitzer erfasst und dieses ins Verhältnis zu sämtlichen Kartenbesitzern gesetzt. Besonders augenfällig wird dabei, dass es die Täter vor allem auf ältere Opfer abgesehen haben. Kartenbesitzerinnen und Kartenbesitzer über 65 Jahre haben ein achtmal höheres Risiko, Opfer eines Kartendelikts zu werden, als Personen unter 65 Jahren.

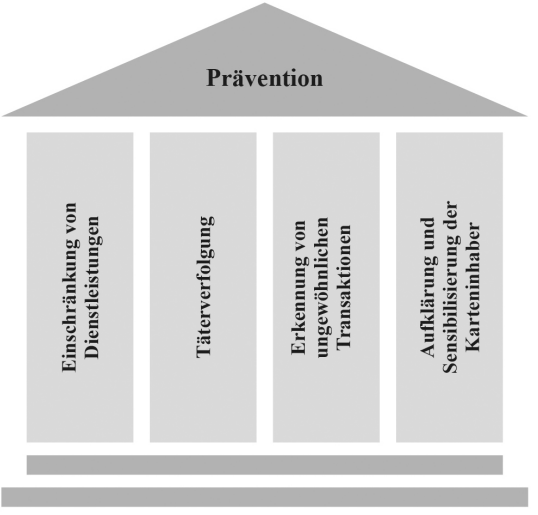


Alter der Opfer von Debitkartendelikten bei der UBS

II. Präventionsarbeit

1. Die vier Säulen der Präventionsarbeit

Bei der Präventionsarbeit von Kartendelikten bauen wir auf vier Säulen auf.



Die vier Säulen der Prävention

a) Aufklärung und Sensibilisierung der Karteninhaber

Die Aufklärung von Kartenbesitzerinnen und -besitzer beginnt bereits mit dem Erhalt der Karte. Die Banken und Kartenherausgeber informieren von Anfang an darüber, dass die Kundinnen und Kunden Sorge zur Karte tragen und ihre PIN verdeckt eingeben müssen. Ebenso sind sie verpflichtet, ihre Karten sperren zu lassen, wenn diese gestohlen oder verloren wurde.

b) Erkennung von aussergewöhnlichen Transaktionen

Jeder Kartenherausgeber verfügt über ein Präventionssystem, das aussergewöhnliche Transaktionen erkennt. Problematisch wird es dann, wenn sich das Verhalten der Täter nicht vom Verhalten ihrer Opfer unterscheidet. Das ist beispielsweise dann der Fall, wenn ein Kunde immer bei der gleichen Bankniederlassung Geld bezieht. Und der Täter ebenfalls dort Geld abhebt. Dann können Präventionssysteme nichts Aussergewöhnliches feststellen. Es gibt aber

auch Fälle, bei denen sich die Kartenbesitzerinnen und -besitzer selbst verhalten wie Betrüger. Zum Beispiel, wenn sie innert kürzester Zeit mehrere Transaktionen tätigen. Wenn Banken und Kartenherausgeber solche Transaktionen jedes Mal stoppen würden, weil sie von einem Betrugsfall ausgehen, dann würden sie mehr Kundinnen und Kunden verärgern, als Delikte aufdecken. Die meisten solcher Transaktionen werden nämlich nicht von Tätern, sondern von den Kartenbesitzerinnen und -besitzer selbst getätigt.

c) Einschränkung von Dienstleistungen

Die wichtigste Einschränkung bei Debitkarten ist die Kartenlimite. Dabei muss diese so tief wie möglich sein. Das bedeutet nur so hoch, wie sie der Kunde auch tatsächlich braucht. Weitere Einschränkungsmöglichkeiten sind geografische Einschränkungen (Geoblocking) oder die Möglichkeit, gewisse Dienstleistungen wie beispielsweise die Kontaktlosfunktion auszuschalten. Mit solchen Massnahmen kann der Kunde sein Risiko und vor allem die Schadensumme begrenzen.

d) Täterverfolgung

Die Täterverfolgung ist primär Sache der Strafverfolgung. Selbstverständlich tragen aber auch die Finanzinstitute viel dazu bei, dass Täter gefasst werden können. – beispielsweise durch die Überwachung der Bancomaten. Zudem arbeiten die Banken eng mit der Polizei zusammen. Die UBS beispielsweise besteht darauf, dass sämtliche Kartendelikte den Strafverfolgungsbehörden angezeigt werden. Und sie trägt durch ihre Kooperation mit der Polizei dazu bei, dass Täter gefasst werden.

2. Kundinnen und Kunden im Zentrum der Prävention

Ein Missbrauch von Debitkarten ist grundsätzlich nur dann möglich, wenn die Täterschaft im Besitz von Karte und PIN ist. In einem solchen Fall geht es sehr rasch. In der Regel heben die Täter sofort Geld ab. Die Präventionssysteme hingegen greifen immer erst dann, wenn ein Missbrauch schon stattgefunden hat und ungewöhnliche Transaktionen festgestellt wurden.

Deshalb tragen Kartenbesitzerinnen und -besitzer eine sehr grosse Eigenverantwortung. Während sie den Diebstahl der Karte kaum verhindern können, tragen sie entscheidend dazu bei, dass die PIN geheim bleibt. Schliesslich können die Täter nur dann in den Besitz der PIN kommen, wenn die Karteninhaber diese gegenüber ihnen offenlegen.

Wer also seine PIN am Automaten abdeckt, sich beim Geldabheben nicht ablenken lässt und die PIN nirgends aufschreibt sowie den Verlust der Debitkarte umgehend meldet, kommt der Sorgfaltspflicht nach und verhindert Kartendelikte.

Bei der Präventionsarbeit muss also die Frage gestellt werden: Sind sich die Kartenbesitzerinnen und -besitzer überhaupt darüber im Klaren, wie wichtig ihr eigenes Verhalten ist?

Zur Stärkung der Präventionsarbeit im Bereich Kartendelikte arbeiten in der Schweiz die Banken und die Polizei sehr eng zusammen. 2011 haben wir gemeinsam die Initiative stop-skimming.ch lanciert. Damals lag der Fokus allein auf Skimming-Delikten. Daraus weiterentwickelt wurde das Präventionsprojekt card-security.ch. Unter diesem lief 2020 eine Kampagne zu den Themen Trickdiebstähle von Debitkarten und Ausspionieren von PIN-Codes. Die Kampagne richtete sich gezielt an Personen im Alter über 65 Jahre. Für 2020/2021 ist eine Kampagne zum Thema Onlinebetrug geplant. Hintergrund dafür ist, dass zunehmend auch Debitkarten für Onlineeinkäufe eingesetzt werden können. Kartendelikte im Internet betreffen damit künftig sowohl Kredit- als auch Debitkarten.

Starke Opfer – Schwache Täter

Schwachstelle Mensch und Opfermitverantwortung im Strafrecht

Marc Jean-Richard-dit-Bressel

Inhalt

I. Menschliche Schwäche als roter Faden des Strafrechtsbetriebs

Die menschliche Schwäche ist im Strafrecht nicht lediglich ein Aspekt der Prävention, sondern der Kern der Sache, um den sich alles dreht. Auch wenn entsprechend dem Tagungsthema vor allem das Opferverhalten zur Diskussion steht, ist dieser Teilaspekt in einem ersten Schritt in eine Gesamtschau von Problemstellungen im Strafrechtsbetrieb einzuordnen, um den Blick für das Mass der Aufmerksamkeit zu öffnen, das dem Verhalten und der Schwäche des Opfers im materiellen Strafrecht angemessen ist.

1. Täter

a) Schwäche beim strafbaren Verhalten

Im Zentrum des Strafrechts steht ein gesetzlich definiertes unerwünschtes Verhalten eines Menschen, für den bei materieller Betrachtung die Bezeichnung „Täter" gebräuchlich ist. In prozessualer Hinsicht ist erst nach der rechtskräftigen Verurteilung von der Täterschaft einer Person auszugehen. Lehre und Rechtsprechung legen grossen Wert auf den das Bundesstrafrecht beherrschenden Grundsatz, dass ein Täter nur zu bestrafen ist, wenn er *schuldhaft* gehandelt hat.[1] In diesem Zusammenhang bedeutet Schuld über Vorsatz oder Fahrlässigkeit hinaus die Einsichts- und Steuerungsfähigkeit.[2] Art. 19 Abs. 1 StGB[3] verleiht diesem Gedanken folgendermassen Ausdruck:

> „War der Täter zur Zeit der Tat nicht fähig, das Unrecht seiner Tat einzusehen oder gemäss dieser Einsicht zu handeln, so ist er nicht strafbar."

Das Fehlen dieser Fähigkeit ist eine Schwäche, die den Täter „entschuldigt", d.h. von Schuld befreit.

Es entspricht indessen nicht der Realität des Strafrechtsalltags und auch nicht der herrschenden Lehre, dass Unvermögen der Strafbarkeit grundsätzlich entgegenstünde. Diese Folge haben in der Regel nur Formen des Unvermögens, die sich medizinisch als Krankheit oder als krankheitsähnlicher Ausnahmezustand fassen lassen.[4] *Labilität*, *Gier*, *Egoismus*, *Rücksichtslosigkeit*, *Triebhaftigkeit*, *Bösartigkeit* und vergleichbare kriminogene Eigenschaften sind ebenso Ausdruck menschlicher Schwäche, die offensichtlich das Vermögen, sich rechtmässig zu verhalten, beeinträchtigen, ohne dass solcherlei die Tat zu entschuldigen vermöchte.

---

1 BGE 135 IV 6 E. 4.2 S. 11; 134 IV 132 E. 6.1 S. 135; 123 IV 1 S. 4; 120 IV 313 S. 316 f.; 118 IV 1 E. 2 S. 4; 117 IV 292 S. 294; 104 IV 249 S. 254; BSK StGB I-Bommer, Vor Art. 19, N 32; PK StGB-Trechsel/Fateh, Art. 19, N 0.

2 BSK StGB I-Bommer, Vor Art. 19, N 26.

3 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB, SR 311.0).

4 Stratenwerth, AT I, § 8 N 26. Zwar will die Neufassung von Art. 10 aStGB als Art. 19 Abs. 1 StGB gemäss der am 1. Januar 2007 in Kraft getretenen Revision des AT StGB die Beschränkung der Schuldunfähigkeit auf die Ursachen „Geisteskrankheit, Schwachsinn oder schwerer Störung des Bewusstseins" beseitigen, doch ist es schwer vorstellbar, dass die Praxis aus anderen Gründen von Schuldunfähigkeit ausgehen könnte. Vgl. dazu BSK StGB I-Bommer/Dittmann, Art. 19, N 14; PK StGB-Trechsel/Fateh, Art. 19, N 6; Stratenwerth, AT I, § 11 N 15.

Hier ist nicht der Ort, nach Gründen zu suchen, weshalb das Strafrecht einige Schwächen als entlastend oder gar entschuldigend ansieht und andere als belastend beurteilt. Es lässt sich indessen festhalten, dass eine *Straftat grundsätzlich Ausdruck einer Schwäche des Täters* ist, wobei diese nicht zwingend eine dauernde charakterliche Disposition zu sein braucht, sondern auch durch eine bestimmte Situation hervorgerufen werden kann.

b) Schwäche im Strafverfahren

Von ganz anderer Natur ist die Schwäche der beschuldigten Person im Strafverfahren. Sie sieht sich der *Übermacht der Strafbehörden*[5] gegenüber, die geltend machen, es bestünden gegen sie Verdachtsgründe. Das Strafprozessrecht bezweckt, hier einen Ausgleich zu schaffen und der beschuldigten Person Verteidigungsrechte und überhaupt eine faire Behandlung zu gewährleisten. Gleichwohl fühlt sie sich mitunter so in die Enge getrieben, dass sie aus einem Gefühl der Schwäche heraus ein unzweckmässiges Verteidigungsverhalten an den Tag legt, was die Verdachtsgründe auch zu Unrecht verstärken kann.

2. Gesetzgebung

Ob ein unerwünschtes Verhalten eine Straftat ist, wird durch das Gesetz bestimmt. Art. 1 StGB lautet:

> „Eine Strafe oder Massnahme darf nur wegen einer Tat verhängt werden, die das Gesetz ausdrücklich unter Strafe stellt."

Bei der gesetzlichen *Grundlage der Strafbarkeit* handelt es sich um die sprachliche Definition eines Unrechtstatbestandes und dessen Verknüpfung mit einer Sanktionsfolge. Diese Beschreibung ist das Ergebnis des Zusammenwirkens von Menschen, die in politischen und dienstrechtlichen Verfahren dafür ausgewählt worden sind. Sie haben die Herausforderung zu meistern, zunächst zu entscheiden, welches Verhalten strafwürdig ist, und dieses Verhalten in allgemeiner Form, aber gleichwohl genügend bestimmt zu beschreiben.

Der Gesetzestext soll sämtliche Erscheinungsformen des anvisierten strafwürdigen Verhaltens erfassen, jedoch keinerlei harmlose und unschädliche Lebensäusserungen. Diese Herausforderung übersteigt das menschliche Ver-

---

[5] Boll, 100 (Einvernahme); Kaufmann, 69, 80; Urwyler, § 1 N 26; Zehnder, N 411. Allerdings ist zu beachten, dass die beschuldigte Person zumindest bei Vorsatzdelikten in der Regel weiss, ob die Verdachtsgründe zu recht bestehen oder nicht, und diesbezüglich gegenüber den Strafbehörden die stärkere Position innehat, vgl. Jean-Richard-dit-Bressel, Informationsgefälle, 141, 171 ff.

mögen. Denn es fehlt an einem absoluten Massstab für die Schädlichkeit. Und selbst dort, wo ein breiter Konsens darüber besteht, führt der Versuch, diesen in Sprache zu fassen, regelmässig zu Formeln, die viele Zweifelsfälle offenlassen. Deshalb kranken die Strafnormen – wie die Gesetzgebung überhaupt – praktisch durchwegs in kleinerem oder grösserem Mass an der „Schwachstelle Mensch". Unsicherheiten und Meinungsverschiedenheiten darüber, ob ein konkretes Verhalten schädlich sei und ob es unter eine bestimmte Strafnorm falle, sind ein fester Bestandteil des Strafrechtsbetriebs.[6]

3. Strafbehörden

Die Menschen, die zur Anwendung der Strafnormen auf bestimmte Sachverhalte berufen sind, kämpfen nicht nur mit der Rechtsunsicherheit, sondern auch mit der *Wahrheitsfindung*, die einerseits durch das unvollkommene Erkenntnisvermögen des Justizpersonals und andererseits durch die menschlichen Schwächen unterliegenden Beweismittel erschwert wird, namentlich durch die beschränkten Wahrnehmungs-, Erinnerungs- und Ausdrucksmöglichkeiten von Menschen, die in den Zeugenstand gerufen werden.

4. Medien und Wissenschaft

Das *Öffentlichkeitsprinzip* bezweckt, Schwächen der Gesetzgebung und Rechtsanwendung aufzudecken. Medien und Wissenschaft haben deshalb eine wichtige Funktion in der Welt des Strafrechts. Doch auch die in diesem Bereich tätigen Leute unterliegen menschlichen Schwächen und haben kein unfehlbares Urteil über die Wahrheit und Schädlichkeit des Verhaltens, das Gegenstand der Entscheidungen der Strafbehörden ist.

5. Prävention

Noch schwächer ist die Position der Menschen, die sich mit der Prävention befassen, der Verhinderung künftiger Straftaten. Die Wahrheitsfindung über Vergangenes ist zwar schwierig, aber grundsätzlich möglich. Darüber, was in der Zukunft unter welchen Voraussetzungen geschehen wird, gibt es in der Gegenwart keine Wahrheit. Tritt ein prognostiziertes Ereignis nach Präventionsmassnahmen nicht ein, besteht oft eine grosse Unsicherheit darüber, wie es ohne Präventionsmassnahmen abgelaufen wäre. Dem Menschen fehlt das Vermögen, einen *hypothetischen Kausalverlauf* zweifelsfrei festzustellen und damit die Erforderlichkeit von unter Umständen teuren und einschneidenden Präventionsmassnahmen sicher zu erkennen.

---

[6] Arzt, Rechtsunsicherheit, passim.

6. Opfer

Nach diesem Reigen menschlicher Schwächen widmen wir uns nun der geschädigten Person, die auch als *Opfer* bezeichnet wird, was im vorliegenden Zusammenhang keine Beschränkung auf den Anwendungsbereich des Opferhilfegesetzes anzeigen soll.[7]

Aus einer Straftat muss nicht zwingend ein Opfer hervorgehen. Wo dies aber der Fall ist, entspricht der Schutz von dessen Interessen einer wesentlichen Aufgabe des Strafrechts.[8] Durch die Straftat sind schützenswerte Interessen des Opfers verletzt worden, was Ausdruck davon ist, dass dieses in der Tatsituation in Bezug auf das verletzte Rechtsgut gegenüber dem Täter in der schwächeren Position war. Es ist eine wichtige Aufgabe des Strafrechts, einen *Ausgleich für die situationsbezogene Schwäche des Opfers* zu schaffen. Das Strafrecht soll einerseits potenzielle Opfer schützen, indem es Tatgeneigte davon abhält, deren Verletzlichkeit auszunützen. Andererseits soll die Bestrafung des Täters dem Opfer dabei helfen, den Eingriff in seine Rechtsgüter zu verarbeiten. Soweit Vermögensinteressen des Opfers betroffen sind, kommt zudem die Wiederherstellung des rechtmässigen Zustandes in Frage.[9]

Hingegen ist es grundsätzlich nicht Aufgabe des Strafrechts, erziehend auf das potenzielle Opfer einzuwirken, damit es Massnahmen ergreift, um seine Verletzlichkeit zu vermindern. Gleichwohl hat vor allem im Zusammenhang mit Betrug der Gedanke Fuss gefasst, dass das Opfer eine gewisse Verantwortung trägt, sich selbst zu schützen, und dass es den Täter bis hin zur Straflosigkeit entlasten kann, wenn es diese Verantwortung nicht wahrnimmt. Mit dem Ziel, die *Opfermitverantwortung im System des Strafrechts* einzuordnen und

---

7 Im vorliegenden Aufsatz ist „Opfer" ein Synonym für „geschädigte Person" gemäss Art. 115 Abs. 1 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0), d.h. „die Person, die durch die Straftat in ihren Rechten unmittelbar verletzt worden ist". Das Opfer gemäss Art. 1 des Bundesgesetzes über die Hilfe an Opfer von Straftaten vom 23. März 2007 (Opferhilfegesetz, OHG, SR 312.5) ist eine Person, „die durch eine Straftat in ihrer körperlichen, psychischen oder sexuellen Integrität unmittelbar beeinträchtigt worden ist". Im Übrigen beeinträchtigen gewisse Formen des Betrugs das Opfer durchaus unmittelbar in der psychischen Integrität, namentlich, wenn der Täter ihm in Betrugsabsicht eine Liebesbeziehung vorgespielt hat.

8 Das zeigt sich z.B. daran, dass bei der Strafbefreiung wegen Wiedergutmachung gemäss Art. 53 Bst. b StGB und beim Verzicht auf Strafverfolgung bei Konkurrenz mit unerheblichem Einfluss auf das Strafmass gemäss Art. 8 Abs. 2 und 3 StPO die Interessen des Geschädigten bzw. der Privatklägerschaft vorbehalten werden und die Privatklägerschaft ferner gemäss Art. 360 Abs. 3 StPO eine Anklage mit Urteilsvorschlag im abgekürzten Verfahren ablehnen kann.

9 Sog. Restitution gemäss Art. 70 Abs. 1 in fine StGB.

dadurch besser zu verstehen, werden im Folgenden verschiedene Strafnormen betrachtet, bei denen das Verhalten des Opfers einen Einfluss auf die Strafbarkeit des Täters haben kann.

II. Skizze eines Systems potenzieller Opfermitverantwortung

Die Opfermitverantwortung wird in der Literatur und Judikatur zum schweizerischen Strafrecht praktisch ausschliesslich im Zusammenhang mit dem *Betrug gemäss* Art. 146 StGB erwähnt und dort mit dem Tatbestandsmerkmal der *Arglist* in Verbindung gebracht. Doch auch bei anderen Strafnormen kann das Verhalten des Opfers einen erheblichen Einfluss auf die Strafbarkeit oder den Strafrahmen haben. Die Suche nach Beispielen dafür zeigt allerdings, dass es sich dabei keinesfalls um ein Grundprinzip des Strafrechts handelt, sondern um eine *Randerscheinung*.

1. Täterorientiert: Einfluss des Opfers auf das Täterverhalten

Bei den nachfolgenden Beispielen für Opfermitverantwortung geht es darum, dass das Opfer seine Möglichkeiten, *Einfluss auf das Verhalten des potenziellen Täters* zu nehmen, so nutzt, dass sich die Wahrscheinlichkeit vermindert, dass dieser dessen Rechtsgüter verletzt.

a) Kenntlichmachung des Opferwillens

Die *Einwilligung des Opfers* beseitigt die Tatbestandsmässigkeit oder die Rechtswidrigkeit eines an sich strafrechtlich relevanten Eingriffs in seine disponiblen Rechtsgüter.[10] Geht der Täter irrtümlich von einer Einwilligung des Opfers aus, so ist seine Tat gestützt auf Art. 13 Abs. 1 StGB so zu beurteilen, wie wenn die Einwilligung vorgelegen hätte. Daraus lässt sich die Regel ableiten, dass das Opfer seinen Willen soweit kenntlich machen muss, dass dessen Verkennung durch den Täter ausgeschlossen erscheint. In der Regel ist dafür keine besondere Vorkehr des Opfers nötig, wenn der Wille, nicht verletzt zu werden, selbstverständlich aus den Umständen hervorgeht. Geht es jedoch um Handlungen, die ihrem Wesen entsprechend auch einvernehmlich erfolgen können und dann nicht den Charakter von Verletzungen haben, hat das Opfer dem Täter die Grenze deutlicher aufzuzeigen, will es den Schutz des

[10] Der Grundsatz ist unbestritten. Zur Diskussion steht jedoch, ob er die Erfüllung des Tatbestands verhindert oder rechtfertigt: BSK StGB I-Niggli/Görlich, Vor Art. 14, N 8; Donatsch/Tag, Strafrecht I, 257 ff.; PK StGB-Trechsel/Geth, Art. 14 N 11; Stratenwerth, AT I, § 10 N 3.

Strafrechts in Anspruch nehmen. Dies gilt in besonderem Mass dann, wenn der Täter Handlungen der fraglichen Art zu einem früheren Zeitpunkt tatsächlich schon im Einverständnis des Opfers ausgeführt hat.

aa) Körperverletzung, v.a. durch Mitwirkung bei fremder Selbstgefährdung

Von Bedeutung ist der Opferwille bei der Mitwirkung an der „eigenverantwortlich gewollten Selbstgefährdung". Das Bundesgericht hatte eine solche im Zusammenhang mit schweren Verbrennungen zu beurteilen, die sich die Beschwerdeführerin bei einer Veranstaltung zuzog, bei der die Teilnehmerinnen nach entsprechender Vorbereitung über glühende Kohlen liefen. Aus naturwissenschaftlich nicht geklärten Gründen scheint es mit entsprechender Instruktion auch dem Durchschnittsmenschen möglich zu sein, einen solchen „Feuerlauf" zu unternehmen, ohne sich zu verletzen. Für die Rechtfertigung der Organisatorin vom Vorwurf der Körperverletzung genügte es nicht, dass die Teilnehmerinnen vorgängig schriftlich bestätigt hatten, die Risiken zu kennen und eigenverantwortlich auf sich zu nehmen. Denn die Einwilligung des Verletzten rechtfertigt eine schwere Körperverletzung nur, wenn diese einem „sittlichen oder ethischen Zweck" dient.[11] Die körperliche Unversehrtheit ist insofern kein frei disponierbares Rechtsgut.[12] Entscheidend für die Rechtfertigung der Organisatorin war, dass sie keine „einvernehmliche Fremdgefährdung" vornahm, sondern lediglich an „fremder Selbstgefährdung" mitwirkte, was dann der Fall ist, wenn der *Rechtsgutträger jederzeit die alleinige Tatherrschaft* in Bezug auf seine Selbstgefährdung innehat.[13] Nicht straflos ist, wer eine fremde Selbstgefährdung veranlasst oder fördert und dabei „das Risiko kraft überlegenen Sachwissens besser erfasst oder erkennt, dass das Opfer die Tragweite seines Entschlusses nicht überblickt".[14]

Der Leitentscheid zeigt auf, dass die Einwilligung des Opfers in die Gefährdung oder Verletzung des Rechtsgutes „Leib und Leben" nur begrenzt rechtfertigend wirken kann. Soweit die Selbstgefährdung an sich keine Straftat ist und die Mitwirkung daran im Rahmen einer blossen *Teilnahme*[15] *an straflosem Verhalten* bleibt, besteht kein Raum für die Strafbarkeit des Teilnehmers. Es handelt sich somit nicht um eine blosse Opfermitverantwortung, sondern um die Eigenverantwortung des Opfers, die entlastend wirkt.

---

11 BGE 134 IV 139 E. 3.2 u. 4.1 S. 152, Meinung der Vorinstanz.

12 Kritisch: BSK StGB I-Niggli/Görlich, Vor Art. 14, N 28 ff.

13 BGE 134 IV 139 E. 4.4-5 S. 153.

14 BGE 134 IV 139 E. 4.5 S. 153 f., mit Hinweis auf BGE 125 IV 189 E. 3a S. 194.

15 Die Beiträge zur Selbstgefährdung gehen ihrem Wesen nach nicht über eine Anstiftung gemäss Art. 24 StGB oder eine Gehilfenschaft gemäss Art. 25 StGB hinaus.

Im vorliegenden Fall geht es nicht darum, dass das Opfer seinen Willen ungenügend zum Ausdruck gebracht hätte. Denkbar ist, dass die an einer fremden Selbstgefährdung mitwirkende Person den *ungenügenden Informationsstand des Opfers* und damit die Mangelhaftigkeit von dessen Willen, die dessen Tatherrschaft beseitigt, verkennt und deshalb einem entlastenden Sachverhaltsirrtum unterliegt. Doch gerade in diesem Punkt besteht kein Raum für eine Opfermitverantwortung, denn es gehört zu den Sorgfaltspflichten der Veranstalter, die Teilnehmer hinreichend aufzuklären. Ist die Mangelhaftigkeit des Opferwillens auf die Verletzung dieser Pflicht zurückzuführen, ist der Veranstalter gemäss Art. 13 Abs. 2 StGB wegen fahrlässiger Körperverletzung strafbar.

Auch bei Eingriffen in die körperliche Integrität, die einem Heilungs-, Schutz- oder Lebenserhaltungszweck dienen, besteht die Gefahr des Irrtums über den Willen des Opfers. Dabei ist typischerweise eine *medizinische Fachperson* mit einem erheblichen Informationsvorsprung beteiligt, die eine hohe Verantwortung dafür trägt, dass der Patient oder die Patientin sich auf einer adäquaten Informationsgrundlage für oder gegen einen Eingriff entscheidet. Entsprechend klein ist der Raum, der bei Missverständnissen der Opfermitverantwortung zukommt.

bb) Hausfriedensbruch

Bei Hausfriedensbruch gemäss Art. 186 StGB gehört es zum gesetzlichen Tatbestand, „*gegen den Willen des Berechtigten*" in den geschützten Bereich einzudringen. Dieser Wille kann sich selbstverständlich aus den Umständen ergeben. So besteht kein Zweifel, dass ein Kaufhaus zum Zwecke des Kaufs oder der Besichtigung des Angebots während der Öffnungszeiten betreten werden darf. Wer dasselbe Lokal zum Zweck des Diebstahls betritt, tut dies offensichtlich gegen den Willen des Berechtigten. Dies erkennt der Täter auch ohne Warntafeln und dergleichen.

Wenn die berechtigte Person an ihrem Wohnhaus im umfriedeten Bereich einen *Briefkasten* und einen *Klingelknopf* anbringt, bringt sie dadurch zum Ausdruck, dass sie das Betreten des Grundstücks zur Betätigung der Klingel oder zum Einwerfen von Schriftstücken erlaube. Ausnahmen von dieser Erlaubnis – z.B. betreffend Hausieren oder Werbung – sind nicht selbstverständlich und deshalb deutlich zum Ausdruck zu bringen.

Das Gesetz auferlegt dem Opfer ferner die Verantwortung, den geschützten Bereich kenntlich zu machen. Dieser ist hinreichend sichtbar, wenn es sich um

ein Haus, eine Wohnung oder einen *abgeschlossenen Raum*[16] eines Hauses handelt. Soll hingegen auch ein zu einem Haus gehörender Hof, Platz oder Garten geschützt werden, so ist der nicht frei betretbare Bereich zu „umfrieden". Die *Umfriedung* genügt den Anforderungen, wenn sie die Grenze des geschützten Bereichs kenntlich macht, wofür ein leicht überwindbarer Zaun genügt. Es ist nicht nötig, dass die Umfriedung das Eindringen erschwert und dem Täter Widerstand bietet.[17]

Der Tatbestand des Hausfriedensbruchs enthält somit keine Vorgaben, wonach das Opfer die Verantwortung hätte, das *Eindringen des Täters* zu *erschweren*. Es genügt, kenntlich zu machen, dass es sich um einen geschützten Bereich handelt.

cc) Sexuelle Nötigung und Vergewaltigung

Bei der sexuellen Nötigung gemäss Art. 189 Abs. 1 StGB und der Vergewaltigung gemäss Art. 190 Abs. 1 StGB nötigt der Täter das Opfer zur Duldung der sexuellen Handlung bzw. des Beischlafs, wobei als Nötigungsmittel auch „psychischer Druck" in Frage kommt. Die Nötigung, die hier durch ihr sexuelles Ziel qualifiziert wird, ist im Grundtatbestand gemäss Art. 181 StGB ein Vergehen gegen die Freiheit, wobei zur Hauptsache die Freiheit des Willens tangiert ist. Bei der Nötigung geht es dem Täter darum, den *Willen des Opfers* zu *brechen*, was bedingt, dass er diesen erkennt. Wenn der Täter sein Opfer durch plötzliche Gewaltanwendung überrascht, wenn er es in Todesangst versetzt oder es durch heimliche Verabreichung von Substanzen betäubt, bedarf es keiner Äusserung des Opfers, damit der Täter erkennen kann, dass er gegen den Willen des Opfers handelt. Verwendet der Täter als Nötigungsmittel gegen ein Opfer ausschliesslich *psychischen Druck*, setzt dies in der Regel eine vorbestehende Beziehung zwischen Täter und Opfer voraus.[18] Dabei ist zu verlangen, dass der Druckausübung ein deutlicher Widerstand, ein klares Nein des Opfers vorausgeht. Kaum nachweisbar ist der Nötigungsvorsatz hin-

---

16 Der Raum braucht nicht mit einem Schlüssel verriegelt zu sein, sondern es genügt, dass er baulich abgetrennt ist, BGE 90 IV 74 E. 2 S. 77, BSK StGB II-Delnon/Rüdy, Art. 186, N 15, Stratenwerth/Jenny/Bommer, BT I, § 7 N 4, wobei die Tür sogar offenstehen kann, PK StGB-Trechsel/Mona, Art. 186, N 3.

17 BGE 141 IV 132 E. 3.2.4 S. 142; Urteil des Bundesgerichts 6B_1056/2013 vom 20. August 2014 E. 2.1; BSK StGB II-Delnon/Rüdy, Art. 186, N 16; Donatsch, Strafrecht III, 501; PK StGB-Trechsel/Mona, Art. 186, N 3.

18 Kasuistik in BSK StGB II-Maier, Art. 189, N 36 ff.

gegen, wenn das Opfer beispielsweise aus der von Täter geförderten Angst, es zu verlassen oder fremdzugehen, widerstandslos ihm widerstrebende sexuelle Handlungen duldet.[19]

Äusserst problematisch ist es, dass die – wenn auch grobfahrlässige – Annahme des Täters, der *Widerstand des Opfers* sei *nicht ernst gemeint*, mangels einer fahrlässigen Tatvariante einen Freispruch zur Folge hat.[20] Das führt besonders dann, wenn der Täter mit psychischem Druck vorgeht, zu dem Erfordernis, dass das Opfer seinen Willen unmissverständlich bekunden muss, wobei auch die Gepflogenheiten in der Beziehung zwischen Täter und Opfer zu berücksichtigen sind.

b) Erschwerung der Tatbegehung

Eine Auswahl von Straftaten erfordert Beiträge des Opfers, in Bezug auf die sich die Frage stellt, ob es hier darum geht, der Tatbegehung über die Kenntlichmachung des Opferwillens hinaus Widerstände entgegenzusetzen, deren Fehlen die Strafbarkeit an sich oder den Strafrahmen beeinflussen kann. Auch dies sollen Beispiele veranschaulichen.

aa) Diebstahl

Die unrechtmässige Aneignung gemäss Art. 137 Ziff. 1 StGB ist ein Vergehen, das als Auffangtatbestand sämtliche nicht durch eine andere Strafnorm erfassten Formen der Anmassung einer eigentümerähnlichen Stellung in Bezug auf fremde bewegliche Sachen unter Strafe stellt. Diebstahl gemäss Art. 139 Ziff. 1 StGB droht als Verbrechen eine schwerere Strafe an als der Auffangtatbestand und findet Anwendung, wenn der Täter dem Opfer die fremde bewegliche Sa-

---

19 Anders war das in der Schweizerische Juristen-Zeitung (SJZ) 61 (1965) Nr. 44, wo der Täter den Widerstand des Opfers gegen Geschlechtsverkehr mit der Androhung des Abbruchs der Beziehung beseitigte. Ein anfänglicher Widerstand im Sinne eines „Nein" genügt, auch wenn dieser aufgrund der Nötigung einer vordergründig einvernehmlichen Duldung weicht. Ungenügend wäre es hingegen, aus Angst vor dem Beziehungsabbruch dem Ansinnen des Täters von Anfang an keinerlei Widerstand entgegenzusetzen.

20 BSK StGB II-Maier, Art. 189, N 54b; Donatsch, Strafrecht III, 539; PK StGB-Trechsel/Bertossa, Art. 189, N 12 (einschränkend); Stratenwerth/Jenny/Bommer, BT I, § 8 N 15.

che zur Aneignung „wegnimmt". Lehre und Rechtsprechung beschreiben den Vorgang der Wegnahme als Bruch fremden und Begründung eigenen *Gewahrsams*.[21]

Wenn das Opfer Gewahrsam ausübt, hat der Täter einen *zusätzlichen Widerstand* zu überwinden, was eine grössere kriminelle Energie erfordert und deshalb zur Erhöhung des Strafrahmens führt. Das lässt sich so auslegen, dass das Opfer mit einem besseren Schutz belohnt wird, wenn es die Verantwortung wahrnimmt, auf seine Sachen zu achten.

Allerdings stellt die Rechtsprechung *sehr geringe Anforderungen an den Gewahrsam*. Dieser wurde etwa bejaht bei einer in einer Telefonkabine vergessenen Brieftasche[22] oder bei zur Abholung am Strassenrand deponiertem Altpapier.[23] Diese Beispiele sprechen gegen die These, dass der Gewahrsam Ausdruck einer Opfermitverantwortung sei. Umgekehrt sind diese Entscheide, die die Anforderungen an den Gewahrsam derart weit herabgesetzt haben, vor der Einführung des generellen Auffangtatbestandes von Art. 137 StGB ergangen.[24] Vor dessen Inkrafttreten im Jahr 1995 konnte es zu unangebrachten Strafbarkeitslücken kommen, wenn sich der Täter eine fremde Sache aneignen konnte, die ihm weder „gegen seinen Willen"[25] noch durch Bruch fremden Gewahrsams noch infolge eines Treuhandverhältnisses zugekommen ist.[26] Die Neuerungen gemäss der im Jahr 1995 in Kraft getretenen Revision des Vermögensstrafrechts hätten Anlass für eine Rückbesinnung darauf sein können, dass kein Diebstahl vorliegt, wenn das Opfer die Sache im Zeitpunkt der Weg-

---

21 BGE 132 IV 108 E. 2.1 S. 110 (nicht an vom Bankautomaten ausgegebenen, von der Kundin versehentlich nicht behändigten Noten); 115 IV 104 E. 1.c.aa S. 106 (an Altpapier am Strassenrand); 112 IV 9 E. 2.a S. 11 (an in Telefonkabine vergessenem Portemonnaie); 110 IV 80 E. 1.b S. 84 (an im Postomat enthaltenen Bargeld); Urteil des Bundesgerichts 6B_943/2020 vom 19. Januar 2021 E. 2.4.1 (übergeordneter Mitgewahrsam des Unternehmens gegenüber den Angestellten); 6B_1360/2019 vom 20. November 2020 E. 2.3.1 (dito); BSK StGB II-Niggli/Riedo, Art. 139, N 15; Corboz, Vol. 1, Art. 139 N 2; CR CP II-Papaux, Art. 139, N 15 ff.; Hurtado Pozo, Partie spéciale, N 900 ff.; PK StGB-Trechsel/Crameri, Art. 139, N 3; Stratenwerth/Jenny/Bommer, BT I, § 13 N 69.

22 BGE 112 IV 9.

23 BGE 115 IV 104.

24 Von den üblicherweise zitierten Entscheiden ist einzig BGE 132 IV 108 unter neuem Recht ergangen. Dieser verneint den Gewahrsam der Bank an Geld, das der Bankautomat ausgegeben, aber die Kundin versehentlich nicht behändigt hat.

25 Art. 141 aStGB, Unterschlagung und Fundunterschlagung.

26 Botschaft des Bundesrates über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) vom 24. April 1991, BBl 1991 II, 696 ff., 999.

nahme nicht wenigstens einigermassen unter Kontrolle hatte, was bei dem vorübergehend gelockerten Gewahrsam gemäss der Rechtsprechung noch zu bejahen ist.[27]

bb) Unbefugte Datenbeschaffung

In derselben Revision, in der der Gesetzgeber den Auffangtatbestand der unrechtmässigen Aneignung einführte, stellte er auch die unbefugte Datenbeschaffung gemäss Art. 143 StGB unter Strafe. In der Botschaft gab der Bundesrat diesem Phänomen den Übernamen „*Datendiebstahl*". Dabei war es sich sehr wohl bewusst, dass die Daten der berechtigten Person nicht entzogen werden und deshalb in einem wesentlichen Punkt keine Analogie zum Diebstahl besteht.[28]

Gemäss Art. 143 Abs. 1 StGB müssen Daten *gegen den „unbefugten Zugriff besonders gesichert*" sein, damit der strafrechtliche Schutz besteht. Damit geht die Opfermitverantwortung einher, für eine solche Sicherung zu sorgen. Es ist zu prüfen, ob diese Vorschrift nur der Kenntlichmachung des Opferwillens dient oder eine Erschwerung der Tatbegehung bezweckt.

Das Obergericht des Kantons Bern hielt in einem Urteil fest:

> „Handelt es sich um private Laptops oder PCs, so darf von den Datenberechtigten keine übermässige Sicherung verlangt werden."[29]

E contrario geht daraus hervor, dass *bei nicht privater Nutzung des Computers* die Daten nur dann strafrechtlich geschützt sind, wenn eine sehr effiziente technische Sicherung gegen unbefugten Zugriff vorhanden ist. Dies würde bedeuten, dass das Opfer dafür verantwortlich ist, Hacking durch technische Massnahmen erheblich zu erschweren, wenn es den Computer gewerblich, behördlich, wissenschaftlich, schulisch, publizistisch, kulturell oder sonst wie ausserhalb des in der Alltagssprache als „privat" bezeichneten Bereichs nutzt.

---

27 BGer 6B_1360/2019 E. 2.3.1; BSK StGB II-Niggli/Riedo, Art. 139, N 24 f.

28 BBl 1991 II, 983 und 1009.

29 Urteil des Obergerichts des Kantons Bern vom 13. November 2007 [SK 2007/187] E. IV.2b S. 5, zitiert in BSK StGB II–Weissenberger, Art. 143 N 19.

Diese These entspricht zwar dem Tenor der herrschenden Lehre,[30] ist jedoch angesichts eines neueren Bundesgerichtsentscheides zu Art. 143 StGB nicht haltbar. Dort heisst es:

> „Als Angriff genügt, gleichsam analog zum Tatbestand des Hausfriedensbruchs gemäss Art. 186 StGB,[31] jede Handlung, die geeignet ist, die jeweilige Sicherung auszuschalten, ohne dass ein besonderer zeitlicher oder technischer Aufwand erforderlich wäre."[32]

Aus diesem Bundesgerichtsentscheid geht hervor, dass die besondere Sicherung in keinem Fall die Erschwerung der Tatbegehung bezweckt. Vielmehr soll lediglich der Opferwille kenntlich gemacht werden, wie die vom Bundesgericht hervorgehobene *Analogie zum Hausfriedensbruch* aufzeigt, auf die bereits die Botschaft mit Nachdruck hingewiesen hat:

> „Ein Straftatbestand, der unterschiedslos alle *fremden* Daten unter Schutz stellt, überdehnt den Strafrechtsschutz. Wenn man bedenkt, dass z.B. in Schulen, Forschungs- und Universitätsinstituten oder Bibliotheken oft eine Grosszahl von Computeranschlüssen, d.h. Terminals, vorhanden und ohne weiteres zugänglich [ist], und dass auf diese Weise eine grosse Menge von Daten sowie Programmen verfügbar und benutzbar ist, wird deutlich, dass nicht jede an sich unkorrekte Datenbeschaffung a priori strafwürdig ist. Es kann nicht richtig sein – wie dies das Ergebnis von Artikel 143 des Expertenentwurfs wäre –, dass die in einem Büro oder einem Universitätsinstitut ohne weiteres von einer Datenverarbeitungsanlage, insbesondere einem Personal-Computer, abrufbaren Daten oder Programme, für die vielleicht gar kein Schutzbedürfnis besteht, zur Anwendung von Artikel 143 StGB-E und zur Verhängung einer Sanktion wie bei Diebstahl führen. Vor allem wäre es stossend, gewisse Informationen nur deshalb strafrechtlich zu schützen, weil sie elektronisch oder in vergleichbarer Weise gespeichert sind, während die traditionelle Art (also in Schriftstücken) erfolgte Niederlegung nicht geschützt wäre. In diesem Zusammenhang sei erwähnt, dass nach Artikel 179 Absatz l StGB (Verletzung des Schriftgeheimnisses) die Kenntnisnahme vom Inhalt einer Schrift nur dann strafbar ist, wenn der Täter die entsprechende verschlossene Sendung öffnet, während Hausfriedensbruch (Art. 186 StGB) voraussetzt, dass in abgeschlossene Räume eingedrungen wird. Übernimmt man diese Grundideen von Artikel 179 Absatz l und 186 StGB, so ergibt sich, dass

---

30 AK StGB-Simmler/Selman, Art. 143, N 4; BSK StGB II-Weissenberger, Art. 143, N 19 f.; Corboz, Vol. I, Art. 143, N 7; Graf, 87 in Anm. 187; HK StGB-Schlegel, Art. 143, N 3; PK StGB-Trechsel/Crameri, Art. 143, N 6; relativierend: Ackermann, Individualinteressen, 159; Donatsch, Strafrecht III, 201; Stratenwerth/Jenny/Bommer, BT I, § 14 N 29 (krit.); anderer Meinung: CR CP II-Monnier, Art. 143, N 9, gestützt auf BGE 130 III 28 E. 4.2 S. 32 f.

31 Hinweise im Zitat: BGE 130 III 28 E. 4.2; BBl 1991 II, 1011.

32 BGE 145 IV 185 E. 2.2.2 S. 189.

> – in Anlehnung an § 202a des deutschen Strafgesetzbuches – nur die gegen unbefugten Zugriff besonders geschützten Daten den Schutz der Strafnorm geniessen sollen. Es ist also notwendig, dass der Zugang zu den betreffenden Daten durch Verschliessen des Computerraumes, Einschliessen der Datenträger, Verwendung von Passwörtern, Chiffrierung von übermittelten Daten oder ähnlichen Massnahmen gesperrt wird und der Täter bei der Datenbeschaffung diese für ihn erkenntliche Schranke übersteigen muss."[33]

Es ging dem Gesetzgeber somit ausschliesslich darum sicherzustellen, dass der *Wille des Opfers für den Täter klar erkennbar* sein muss. Dieses Kriterium war in keiner Weise darauf ausgerichtet, im Bestreben, eine an den Tatbestand des Diebstahls angelehnte Bestimmung zu schaffen, ein Pendant zum Gewahrsam zu verlangen. Es wird jedoch von der Lehre so ausgelegt.[34] Vielmehr liess sich der Gesetzgeber von der sachgerechten Analogie der unbefugten Datenbeschaffung zum Hausfriedensbruch und zur Verletzung des Schriftgeheimnisses leiten.

c) Unterlassung der Provokation des Täters

Von einer grundlegenden Mitverantwortung des Opfers ist auszugehen, wenn dieses einen erheblichen Einfluss darauf genommen hat, dass sich der Täter zur Tat entschieden hat.

aa) Genereller Strafmilderungsgrund der Provokation durch das Opfer

Gemäss Art. 48 Bst. b StGB mildert das Gericht die Strafe, „wenn der Täter durch das Verhalten der verletzten Person ernsthaft in Versuchung geführt worden ist". Aus dieser Bestimmung ergibt sich e contrario, dass selbst eine ernsthafte *Versuchung durch das Opfer* kein genereller Grund für eine Strafbefreiung ist.

Der *Wunsch oder die Einwilligung* des adäquat informierten Opfers, der Täter möge in seine disponiblen Rechtsgüter eingreifen, ist eine Form der Provokation, die zur Straflosigkeit des Täters führt, soweit es dabei nicht um den Eingriff in die Rechtsgüter Dritter geht, z.B. um Versicherungsbetrug.[35]

Kein disponibles Rechtsgut ist die sexuelle Integrität von Kindern, Abhängigen und dergleichen. Die Verletzung dieses Rechtsguts ist deshalb strafbar, auch wenn es das Opfer so wollte. *Sexualdelikte* stellen denn auch in der Praxis den

---

33 BBl 1991 II, 1010 f.

34 AK StGB-Simmler/Selman, Art. 143, N 4; BSK StGB II-Weissenberger, Art. 143, N 18; PK StGB-Trechsel/Crameri, Art. 143, N 6.

35 Oben, II.1.a)aa).

weitgehend einzigen Anwendungsfall des Strafmilderungsgrundes von Art. 48 Bst. b StGB dar.[36] Zu Recht wird dabei die Zustimmung zu sexuell motivierter körperlicher Nähe nicht als ernsthafte Provokation zur Erzwingung von Geschlechtsverkehr oder diesem ähnlichen Handlungen anerkannt.[37]

Allerdings ist Provokation nicht auf Handlungen mit Einwilligungscharakter beschränkt. So kann das Opfer den Täter durch „Protzen mit Geldbesitz an einer Bar"[38] zu einem *Vermögensdelikt* veranlassen, ohne auch nur den Anschein einer Zustimmung zu erwecken. Entsprechend liesse sich auch die These aufstellen, dass ein Opfer, das dem Täter durch seinen Leichtsinn oder seine mangelhaften Kontrollmechanismen auffällt, diesen ernstlich in Versuchung führt, es zu betrügen. Doch wäre es abwegig, in einem solchen Fall den Strafmilderungsgrund der Provokation anzuwenden.[39] Ganz im Gegenteil belastet die Kenntnis und gezielte Ausnützung einer solchen Schwäche des Opfers den Täter, namentlich im Zusammenhang mit dem Tatbestandsmerkmal der Arglist.[40]

bb) Strafantrag nach Provokation, v.a. bei Verleitung zu Misswirtschaft

Generell gilt ein Strafantrag als *rechtsmissbräuchlich* und damit ungültig, wenn die antragsberechtigte Person das potenziell strafbare Verhalten durch eine rechtswidrige Provokation veranlasst hat.[41] Dies hat das Bundesgericht in Bezug auf den Strafantrag des erziehungsberechtigten Vaters wegen Entziehung von Unmündigen gemäss Art. 220 StGB gegen die von ihm geschiedene Mutter bejaht, die das Besuchsrecht, das er zuvor über längere Zeit systematisch vereitelt hatte, geringfügig überschritten hatte.[42]

Eine spezielle Regelung über die Provokation durch den Gläubiger enthält die *Misswirtschafts-Strafnorm*, die zu einem Antragsdelikt heruntergestuft wird, wenn als objektive Strafbarkeitsbedingung keine Konkurseröffnung, sondern

---

36 PK StGB-Trechsel/Seelmann Art. 48 N 14–16.

37 BGE 97 IV 77; Urteil des Bundesgerichts 6S.378/2005 vom 20. Dezember 2005; SJZ 62 [1966] Nr. 3; BSK StGB II-Wiprächtiger/Keller, Art. 148 N 23; PK StGB-Trechsel/Seelmann, Art. 48, N 16.

38 PK StGB-Trechsel/Seelmann, Art. 48, N 14, unter Hinweis auf den Sachverhalt von BGE 101 IV 154.

39 Gleicher Meinung: Arzt, Leichtsinnige, 47.

40 Unten, II.2.c)bb), III.4.

41 AK StGB-Konopatsch/Uhrmeister, Art. 30, N 12; HK StGB-Wohler, Vor Art. 30, N 5; PK StGB-Trechsel/Geth Vor Art. 30, N 12.

42 BGE 105 IV 229 passim, 104 IV 90 E. 3 S. 94 ff.

nur ein Pfändungsverlustschein vorliegt. Der dem Pfändungsgläubiger zustehende Strafantrag unterliegt Regeln, die von Art. 30 ff. StGB abweichen. Dazu gehört die Bestimmung von Art. 165 Ziff. 2 Abs. 3 StGB:

> „Dem Gläubiger, der den Schuldner zu leichtsinnigem Schuldenmachen, unverhältnismässigem Aufwand oder zu gewagten Spekulationen verleitet oder ihn wucherisch ausgebeutet hat, steht kein Antragsrecht zu."

Anscheinend liegt *keinerlei Kasuistik* zu dieser Bestimmung vor.[43]

Bei den hier beschriebenen unzweckmässigen Geschäften, zu denen der Gläubiger den Schuldner verleitet hat, ist in erster Linie an die Grundlagen seiner in Betreibung gesetzten Forderung zu denken. Wenn der *Gläubiger* im Bestreben, seinen *eigenen Umsatz* zu *steigern*, den Schuldner zu unvernünftigen Geschäften verleitet hat und ihm namentlich leichtsinnig Kredit gewährt, unverhältnismässigen Aufwand verursachende Leistungen anbietet oder hochspekulative Titel verkauft oder entgeltlich vermittelt, soll in der *Spezialexekution* nicht den Schutz des Strafrechts in Anspruch nehmen können, wenn sein Schuldner die Pflichten, die er ihm solchermassen aufgebürdet hat, nicht erfüllen kann.

Kommt es aber zur *Generalexekution*, ist die Misswirtschaft ungeachtet der Provokation von Amtes wegen zu verfolgen. Vorbehalten bleibt eine Strafmilderung gemäss Art. 48 Bst. b StGB. Konsequent wäre es, dem vom Strafantrag ausgeschlossenen Gläubiger in einem von Amtes wegen durchzuführenden Strafverfahren gestützt auf die allgemeine Rechtsmissbrauchsklausel die dem Gläubiger zustehende Konstituierung als Privatkläger gemäss Art. 118 Abs. 1 StPO[44] zu verwehren. Allerdings bedarf es dazu einer hinreichenden Feststellung des Sachverhalts, während der dem potenziell auszuschliessenden Gläubiger die Parteirechte vorläufig zu gewähren sind.

2. Opferorientiert: Einfluss des Täters auf das Opferverhalten

Bei den hiervor diskutierten Beispielen ist durchwegs die Einflussnahme des Opfers auf das Verhalten des Täters der Gegenstand seiner potenziellen Verantwortung. Eine Reihe von Erfolgsdelikten ist jedoch so aufgebaut, dass der Täter das Opfer durch unrechtmässige Mittel zu einem Verhalten bestimmen will, durch das es in Vermögen, über das es verfügen kann, schädigend ein-

---

43 Negativ: BSK StGB II-Hagenstein; Art. 165, N 105; PK StGB-Trechsel/Ogg Art. 165, N 13; Swisslex-Suche nach Art. 165 Ziff. 2 StGB am 5. Juli 2021 führte zu nur 7 Treffern, wovon keiner einschlägig war.

44 BGE 140 IV 155 E. 3.3.2 S. 158.

greift. Dies bewirkt der Täter, indem er den *Willen des Opfers manipuliert*, namentlich indem er es irreführt, bedroht oder ausbeutet. In diesem Zusammenhang steht die Frage zur Diskussion, inwiefern das Opfer dafür verantwortlich sein kann, der Manipulation seines Willens durch den Täter zu widerstehen.

a) Sich nicht täuschen lassen

aa) Betrug gemäss Art. 146 StGB und absichtliche Täuschung gemäss Art. 28 OR

Beim Betrug gemäss Art. 146 StGB übt der Täter Einfluss auf das Verhalten des Opfers aus, um es irrezuführen und so zu einer selbstschädigenden Vermögensdisposition zu veranlassen. Die *Opfermitverantwortung* steht *in erster Linie im Zusammenhang mit dem Betrug* zur Diskussion, wo sie an das im Gesetzestext enthaltene Adverb „arglistig" geknüpft wird. Darauf ist hinten in Titel III näher einzugehen. An dieser Stelle geht es vorerst nur darum, den Betrug in dem skizzierten Gesamtsystem der potenziellen Opfermitverantwortung einzuordnen.

Das zivilrechtliche Pendant zum Betrug ist die *absichtliche Täuschung gemäss Art. 28 Abs. 1 OR*:[45]

> „Ist ein Vertragschliessender durch absichtliche Täuschung seitens des andern zu dem Vertragsabschlusse verleitet worden, so ist der Vertrag für ihn auch dann nicht verbindlich, wenn der erregte Irrtum kein wesentlicher war."

Die Rechtsfolge von Art. 28 Abs. 1 OR tritt auch bei Täuschungen ein, die *nicht arglistig* sind. Aus der Anwendbarkeit auch auf nicht wesentliche Irrtümer folgt, dass durch den Irrtum *kein Schaden* einzutreten braucht.[46]

Da *fahrlässiger Irrtum* dem Irrenden gemäss Art. 26 Abs. 1 OR nicht schadet, wenn „der andere den Irrtum gekannt" hat, entfällt bei der absichtlichen Täuschung gemäss Art. 28 Abs. 1 OR jede Opfermitverantwortung, da der absichtlich Täuschende den Irrtum ja zwangsläufig kennt.[47]

---

45 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (OR, SR 220).

46 BSK OR I-Schwenzer/Fountoulakis, Art. 28, N 1; Furrer/Müller-Chen, in Furrer, Kap. 7 N 2.

47 BSK OR I-Schwenzer/Fountoulakis, Art. 26, N 1a., Art. 28, N 14a, mit Hinweis auf Urteile des Bundesgerichts 4A_141/2017 vom 4. September 2017 E. 3.1.4 und 4A_533/2013 vom 27. März 2014 E. 4.3–4; kritisch: Vischer/Galli, 1398 ff.

bb) Betrugsähnliche Straftatbestände

Bei betrugsähnlichen Straftatbeständen, die auch das Schlüsselwort „arglistig" verwenden, steht diese Form der Opfermitverantwortung ebenfalls zu Diskussion, so bei der *arglistigen Vermögensschädigung* gemäss Art. 151 StGB und beim *Leistungs- und Abgabenbetrug* gemäss Art. 14 VStrR.[48]

Bei *Check- und Kreditkartenmissbrauch* gemäss Art. 148 StGB haben der Aussteller und „das Vertragsunternehmen die ihnen zumutbaren Massnahmen gegen den Missbrauch der Karte" zu ergreifen, was schon im Gesetzgebungsverfahren als *objektive Strafbarkeitsbedingung* gedacht war.[49] Dieses Kriterium wurde erst durch die Kommission des Ständerats als Zweitrat vorgeschlagen.[50] Lehre und Rechtsprechung erblicken darin ein Bestreben, ein Gleichgewicht mit dem Konzept der Arglist beim Betrug herzustellen,[51] was allerdings hinsichtlich der Ausgestaltung als objektive Strafbarkeitsbedingung aus den publizierten Materialien nicht hervorgeht.[52] Die Konzepte von Art. 146 und Art. 148 StGB unterscheiden sich grundlegend. Anders als die Wendung „arglistig irreführen" in Art. 146 StGB, die das Täterverhalten beschreibt, verlangt die Formulierung von Art. 148 StGB ausdrücklich, dass das Opfer Massnahmen zum Selbstschutz ergreift.

Eine Anzahl betrugsähnlicher Straftaten enthält weder das Stichwort „arglistig" noch eine vergleichbare Wendung. Es handelt sich teilweise um blosse Gefährdungsdelikte. Bei solchen Strafnormen bedarf es gemäss vorherrschender Meinung weder erhöhter Anforderungen an die Qualität der Lüge noch eines Ausschlusses der Opfermitverantwortung. Dies gilt etwa bei *betrügeri-*

---

48 Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (VStrR, SR 313.0).

49 AB 1993 S V 959 (Beerli, Berichterstatterin); BGE 125 IV 260 E. 2 S. 264; AK StGB-Mráz, Art. 148, N 12; BSK StGB II-Fiolka, Art. 148, N 35; Corboz, Vol. I, Art. 148, N 16; CR CP II-Grodecki, Art. 148, N 20 f.; Donatsch, Strafrecht III, Art. 265; HK StGB-Schlegel, Art. 148, N 7; PK StGB-Trechsel/Crameri, Art. 148, N 9; Stratenwerth/Jenny/Bommer, BT I, § 16 N 38.

50 AB 1993 S V 959 (Beerli, Berichterstatterin).

51 BGE 125 IV 260 E. 2 S. 264; BSK StGB II-Fiolka, Art. 148, N 35; CR CP II-Grodecki, Art. 148, N 20.

52 BBl 1991 II, 1027: „Der Straftatbestand des Check- und Kreditkartenmissbrauches ist ein Sonderfall des Betruges, zu welchem ein Mindestmass an täuschendem Verhalten des Täters gehört. Artikel 148 StGB-E nimmt diese Idee auf, indem er für die Strafbarkeit ausdrücklich einen *missbräuchlichen* Einsatz verlangt" (Hervorhebung gemäss Vorlage). AB 1993 S V 959 (Beerli, Berichterstatterin): Im Ständerat wurde das Wort „missbraucht" durch die objektive Strafbarkeitsbedingung ersetzt, wobei die Kommissionssprecherin Konkurrenz und Abgrenzung zum Betrug, nicht aber eine Analogie dazu thematisierte. AB 1994 N I 330 (Leuba, rapporteur), Zustimmung ohne Thematisierung des Betrugs.

schem Missbrauch einer Datenverarbeitungsanlage gemäss Art. 147 StGB,[53] bei *unrechtmässigem Bezug von Leistungen einer Sozialversicherung oder der Sozialhilfe* gemäss Art. 148a StGB,[54] bei *Zechprellerei* gemäss Art. 149 StGB,[55] bei *Erschleichen einer Leistung* gemäss Art. 150 StGB,[56] bei *unwahren Angaben über kaufmännische Gewerbe* gemäss Art. 152 StGB und bei verschiedenen betrugsähnlichen Straftaten des Nebenstrafrechts, so bei *unlauterem Wettbewerb* gemäss Art. 3 Abs. 1 Bst. b UWG[57] in Verbindung mit Art. 23 UWG[58] oder bei *Sozialversicherungsdelikten* des Typs von Art. 87 Alinea 1 und 2 AHVG[59].[60]

b) Sich nicht in Furcht versetzen lassen

aa) Erpressung gemäss Art. 156 StGB und Furchterregung gemäss Art. 29 f. OR

Bei einer anderen Gruppe von Straftaten macht der Täter das Opfer durch „*Gewalt oder Androhung ernstlicher Nachteile*" gefügig, so bei der Nötigung gemäss Art. 181 StGB und der Erpressung gemäss Art. 156 StGB, die bei der vorliegenden Betrachtung wegen ihrer Analogie zum Betrug[61] im Vordergrund steht. Erpressung ist ein qualifizierter Spezialtatbestand zur Nötigung.

Zivilrechtlich wird die Folge eines solchen Vorgehens unter dem Titel der *Furchterregung gemäss* Art. 29 OR geregelt, wobei die Unverbindlichkeit des dadurch herbeigeführten Vertragsschlusses nur eintritt, wenn die Furcht gegründet war. Dies ist gemäss Art. 30 Abs. 1 OR für die Person der Fall, die „nach den Umständen annehmen muss, dass er oder eine ihm nahe verbundene Per-

---

53 Urteil des Bundesgerichts 6B_936/2017 vom 9. Februar 2018 E. 2.4.2; Corboz, Vol. I, Art. 147, N 8; CR CP II-Grodecki, Art. 147 (keine Erwähnung); HK StGB-Schlegel, Art. 147, N 3; relativierend: Donatsch, Strafrecht III, 257; Stratenwerth/Jenny/Bommer, BT I, § 16 N 5; anderer Meinung: BSK StGB II-Fiolka, Art. 147, N 15 f., der aus dem Erfordernis der Unbefugtheit der Datenverwendung die Opfermitverantwortung zur Sicherung der Daten ableitet.

54 Urteile des Bundesgerichts 6B_46/2020 vom 22. April 2021 E. 2.1.; 6B_1015/2019 vom 4. Dezember 2019 E. 4.5.2; PK StGB-Burckhardt/Schulze, Art. 148a, N 8; anderer Meinung: HK StGB-Schlegel, Art. 148a, N 4.

55 BGE 125 IV 124 E. 2.c S. 126; AK StGB-Mráz, Art. 149, N 9; HK StGB-Schlegel, Art. 149, N 1; PK StGB-Trechsel/Crameri, Art. 149, N 9.

56 Donatsch, Strafrecht III, 278.

57 Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (UWG, SR 241).

58 BSK UWG-Killias/Guilléron, Art. 23, N 5 und 47; K UWG-Heimgartner, Art. 23, N 27.

59 Bundesgesetz über die Alters- und Hinterlassenenversicherung vom 20. Dezember 1946 (AHVG, SR 831.10).

60 Käser, N 27 und 145.

61 BSK StGB II-Weissenberger, Art. 156, N 2; CR CP II-Mazou, Art. 156, N 13; Donatsch, Strafrecht III, 302; PK StGB-Trechsel/Crameri, Art. 156, N 2 und 9.

son an Leib und Leben, Ehre oder Vermögen mit einer nahen und erheblichen Gefahr bedroht sei". Die aufgezählten Rechtsgüter sind nicht abschliessend. Das Zivilrecht macht damit die Folge der Furchterregung nicht von einem objektiven Massstab, den die Figur der verständigen Person setzt, abhängig, sondern stellt ganz auf die Wirkung ab, die bei der betroffenen Person eingetreten ist.[62]

bb) Anforderungen an die Furchterregung im Strafrecht

Wie im Zivilrecht genügt auch im Strafrecht nicht jede Furchterregung, sondern Art. 181 und Art. 156 StGB verlangen gleichermassen die „*Androhung ernstlicher Nachteile*". Nach der Praxis des Bundesgerichts ist dies nach einem objektiven Massstab zu beurteilen:

> „Ernstlich sind Nachteile, wenn ihre Androhung nach einem objektiven Massstab geeignet ist, auch eine besonnene Person in der Lage des Betroffenen gefügig zu machen und so seine Freiheit der Willensbildung oder -betätigung zu beschränken.[63] Die Drohung muss eine gewisse Intensität aufweisen, die sich nach objektiven Kriterien und den Umständen des Einzelfalls bestimmt."[64]

Bei der strafrechtlichen Furchterregung ist somit *ausschliesslich das Täterverhalten* der Massstab dafür, ob diese die für die Erfüllung des Tatbestands erforderliche Intensität erreicht hat. Die Formel geht zwar durchaus davon aus, dass angesichts von Drohungen eine gewisse Besonnenheit angebracht ist. Lehre und Rechtsprechung[65] knüpfen daran indessen keine Erwartung an das Opfer, es müsse wenigstens die grundlegenden Massnahmen ergreifen, um die

---

62 BSK OR I-Schwenzer/Fountoulakis, Art. 29/30, N 9f.

63 Hinweise im Zitat: Urteile des Bundesgerichts 6B_1105/2019 vom 12. Dezember 2019 E. 2.4; 6B_979/2018 vom 21. März 2019 E. 1.2.2; je mit Hinweisen.

64 Urteil des Bundesgerichts 6B_852/2019 vom 16. Juli 2020 E. 2.2.2 (versuchte Nötigung). Ähnlich: BGE 122 IV 322 E. 1a S. 324 f. (Nötigung); 120 IV 17 E. 2a/aa S. 19 (Nötigung); 105 IV 120 E. 2.a S. 122 (Nötigung); Urteile des Bundesgerichts 6B_458/2018 vom 9. April 2019 E. 1.2 (Nötigung); 6B_1139/2017 vom 23. Mai 2018 E. 2.2.2 (versuchte Erpressung); 6B_570/2017 vom 16. Oktober 2017 E. 2.1 (versuchte Nötigung); 6B_1074/2016 vom 20. Juli 2017 E. 2.1.2 (Nötigung); 6B_1193/2016 vom 30. März 2017 E. 2.2 (versuchte Nötigung); 6B_1082/2013 vom 14. Juli 2014 E. 2.2 (versuchte räuberische Erpressung); 6S.77/2003 vom 6. Januar 2004 E. 2 (Nötigung); Ackermann, Individualinteressen, 194; AK StGB-Mráz, Art. 156, N 3; BSK StGB II-Weissenberger, Art. 156, N 19; Corboz, Vol. II, Art. 156, N 16; CR CP II-Mazou, Art. 156, N 10; Donatsch, Strafrecht III, 448 f. (Art. 181 StGB); HK StGB-Schlegel, Art. 156, N 1; PK StGB-Trechsel/Crameri, Art. 156, N 4; Stratenwerth/Jenny/Bommer, BT I, § 5 N 9 in Verbindung mit § 17 N 4.

65 Belegstellen gemäss vorangehender Fussnote.

Bedrohung abzuwenden, ohne sich dem Täter zu fügen. Zwar weist eine Drohung, die das Opfer in seiner spezifischen Lage ohne weiteres entschärfen könnte, kaum die für eine Nötigung oder Erpressung erforderliche Intensität und Ernstlichkeit auf. Dies ist jedoch ausschliesslich ein Massstab zur Beurteilung der vom Täter gewählten Art der Furchterregung. Lehre und Praxis haben die Anforderungen an die Drohung nicht so ausgestaltet, dass es den Täter entlastet, wenn das Opfer grundlegende Selbstschutzmassnahmen unterlässt. Es bedarf für die Strafbarkeit keines Nachweises eines besonnenen Vorgehens des Opfers. Insofern kommt bei Nötigung und Erpressung keine Opfermitverantwortung zum Tragen. Das besonnene und das unbesonnene Opfer sind gleichermassen geschützt. Jedoch ist nach herrschender Lehre und Praxis ein Täterverhalten von der Strafbarkeit ausgenommen, das nur beim unbesonnenen, nicht aber auch beim besonnenen Opfer wirksam sein kann.[66]

c) Sich nicht übervorteilen lassen

aa) Wucher gemäss Art. 157 StGB und Übervorteilung gemäss Art. 21 OR

Der Wucher gemäss Art. 157 StGB ist der dritte Deliktstyp, bei dem der Täter das Opfer unter *Ausnützung eines Schwächezustandes* zu einer Selbstschädigung veranlasst. Das Opfer schädigt sich selbst, indem es dem Täter Vermögensvorteile gewährt oder verspricht, die bedeutend mehr wert sind als die dafür erbrachte Gegenleistung. Der Straftatbestand stimmt inhaltlich weitgehend mit dem vertragsrechtlichen Tatbestand der Übervorteilung gemäss Art. 21 OR überein, der der übervorteilten Person ein Rücktrittsrecht mit Wirkung ex tunc innerhalb eines Jahres nach Vertragsschluss verschafft.[67] Diese zivilrechtliche Folge tritt auch dann ein, wenn die ausgebeutete Schwächesituation selbstverschuldet ist.[68]

Während der Täter beim Betrug und bei der Erpressung das Opfer aktiv in den Zustand des Irrtums bzw. der Furcht versetzt, um es zur Selbstschädigung zu veranlassen, nutzt er beim Wucher einen *Schwächezustand* des Opfers aus, in dem es sich *ohne Zutun des Täters* befindet, nämlich „die Zwangslage, die Abhängigkeit, die Unerfahrenheit oder die Schwäche im Urteilsvermögen". Selbstverständlich entlastet es den Täter nicht, wenn er dazu beigetragen hat, dass das Opfer in einen solchen Zustand geraten ist, doch ist dies zur Erfüllung

---

66 Kritisch dazu BSK StGB II-Weissenberger, Art. 156, N 19, der die Ernstlichkeit nicht ausschliesslich nach objektiven Kriterien beurteilen, sondern auch die Eigenheiten des Opfers wie z.B. eine schwache Willenskraft belastend berücksichtigen will.

67 BSK OR I-Meise/Huguenin, Art. 21, N 15.

68 BSK OR I-Meise/Huguenin, Art. 21, N 10.

des Tatbestands nicht erforderlich. Es genügt, wenn der Täter erkennt, dass sich das Opfer in einem solchen Zustand befindet und deshalb für sein wucherisches Angebot empfänglich ist. Die Tathandlung besteht darin, einer aus diesen Gründen für Übervorteilung anfälligen Person ein wucherisches Angebot zu unterbreiten. Der tatbestandsmässige Erfolg tritt durch die Abgabe einer Verpflichtungserklärung oder Erbringung einer Leistung des Opfers ein.

Der Tatbestand des Wuchers ist *einer Opfermitverantwortung nicht zugänglich*. Er ist ausdrücklich darauf ausgerichtet, ein Opfer zu schützen, das sich in einem Zustand der Schwäche befindet, weil es dadurch in seinem Urteilsvermögen oder seiner Handlungsfreiheit beeinträchtigt ist. Der Tatbestand fragt nicht nach den Ursachen und der Verantwortung für diese Beeinträchtigungen. Selbstverschulden des Opfers führt zu keiner Privilegierung des Täters.[69] Der teilweise angebrachte Vorbehalt, wonach sich nicht in einer Zwangslage befinde, wer mit grossem Risiko auf hohe Gewinne spekuliere,[70] betrifft den Geldbedarf für die Spekulation und nicht die Notlage aufgrund der durch Spekulationsverluste eingetretenen Zahlungsschwierigkeiten.[71]

bb) Schnittstelle zur Opfermitverantwortung beim Betrug

Auch wenn die Opfermitverantwortung beim Wucher keinen Platz hat, ergeben sich teilweise ähnliche Fragen, wie sie beim Betrug unter diesem Titel diskutiert werden.[72] Nach der Rechtsprechung des Bundesgerichts verdient das *schwache Opfer höheren Schutz*, was eine Opfermitverantwortung ausschliesst oder vermindert:

> „Bei der Prüfung der Frage, ob Arglist gegeben sei, ist die Lage des Opfers im Einzelfall zu berücksichtigen. Ist das Opfer geistesschwach, unerfahren oder aufgrund des Alters oder einer (körperlichen oder geistigen) Krankheit beeinträchtigt, befindet es sich in einem Abhängigkeits- oder Unterordnungsverhältnis oder in einer Notlage, und nützt der Täter dies aus, ist Arglist zu

---

69 BGE 80 IV 15 E. 1 S. 20 (Ursachen unerheblich); BSK StGB II-Weissenberger, Art. 157, N 11; CR CP II-Mazou, Art. 157, N 9; Donatsch, Strafrecht III, 312 (Ursachen unerheblich); Hurtado Pozo, Partie spéciale, N 1462; PK StGB-Trechsel/Crameri, Art. 157, N 3.

70 Corboz, Vol. I, Art. 157, N 16; CR CP II-Mazou, Art. 157, N 9; Hurtado Pozo, Partie spéciale, N 1462; PK StGB-Trechsel/Crameri, Art. 157, N 3 in fine.

71 Das ergibt sich aus Rep. 1986 153, und ZR 43 (1944) Nr. 71, den einzigen Judikatur-Referenzen der in der vorangehenden Fussnote angeführten Lehrmeinungen, zitiert in PK StGB-Trechsel/Crameri, Art. 157, N 3 in fine.

72 Einen Zusammenhang bei der „Ausnützung der Inferiorität" sieht auch Cassani, 168.

> bejahen. Der Gesichtspunkt der Opfermitverantwortung kann nur dort zur Verneinung der Arglist führen, wo eine derartige Unterlegenheit des Opfers nicht besteht."[73]

Dies führt zur Frage, ob das Opfer an sich fähig gewesen wäre, die Unwahrheit der Erklärungen des Täters zu erkennen, von dieser Fähigkeit aber keinen Gebrauch gemacht habe. Beim Wucheropfer stellt sich im Grunde dieselbe Frage, nämlich, ob es an sich fähig gewesen wäre, dem übervorteilenden Angebot des Täters zu widerstehen. Denn wenn dies der Fall ist, erscheint es zumindest als zweifelhaft, ob sein Schwächezustand so stark war, dass er den tatbestandsmässigen Vorgaben von Art. 157 StGB genügt. Sollen beim Betrug entsprechend der Rechtsprechung *starke und schwache Opfer unterschieden* werden, bieten sich die Opfereigenschaften des Wuchers als Massstab oder wenigstens als Orientierungshilfe an.

III. Arglist und Opfermitverantwortung beim Betrug

Nach den allgemeinen Betrachtungen über menschliche Schwächen (Titel I) und Opfermitverantwortung (Titel II) im Strafrecht, ist nun – wie angekündigt – vertieft auf den Betrug einzugehen, der im Zentrum der Diskussion über die Opfermitverantwortung steht.

1. Grundstruktur des Betrugs

Der Betrug gemäss Art. 146 Abs. 1 StGB ist ein *Erfolgsdelikt*, der durch eine Kaskade von mehreren Erfolgsstufen gekennzeichnet ist, die Beweggrund (Motiv) bzw. Ursache (Causa) für die jeweils nächste Stufe sein müssen. Das tatbestandsmässige Verhalten, das diese auslöst, besteht in der als „Vorspiegelung oder Unterdrückung von Tatsachen" umschriebenen Lüge des Täters, die als *erste Erfolgsstufe* beim Opfer einen Irrtum hervorruft. Dieser Irrtum hat das Opfer ohne weiteres Zutun des Täters zu der *zweiten Erfolgsstufe* zu bewegen, nämlich dazu, eine Vermögensdisposition vorzunehmen, d.h., über eigenes oder gestützt auf eine Ermächtigung über fremdes Vermögen zu verfügen. Diese Vermögensverfügung muss als *dritte Erfolgsstufe* einen Schaden verursachen.[74]

---

[73] BGE 120 IV 186 Regeste; ähnlich: 147 IV 73 E. 3.2 S. 79; eingehend zu dieser Rechtsprechung Sägesser, N 200 ff.

[74] BSK StGB II-Maeder/Niggli, Art. 146, N 36 und 40; Donatsch, Strafrecht III, 226; PK StGB-Trechsel/Crameri, Art. 146, N 1; Stratenwerth/Jenny/Bommer, BT I, § 15 N 4.

Der *Schaden* hat unmittelbar durch die Vermögensdisposition einzutreten und besteht in der Differenz zwischen dem irrtümlich erwarteten und dem tatsächlich erlangten Gegenwert. Ist der Gegenwert eine Forderung, entspricht der Schaden der Differenz zwischen ihrer vermeintlichen und ihrer tatsächlichen Bonität.[75] Soll die Vermögensdisposition einen bestimmten Zweck fördern, der auch altruistisch sein kann, bestimmt sich der Schaden nach der Differenz zwischen dem vermeintlich und dem tatsächlich diesem Zweck zugeführten Anteil der Vermögenswerte, die Gegenstand der Disposition waren.[76]

Gemäss dem Stoffgleichheitsprinzip[77] muss der Schaden unmittelbar zu einer *unrechtmässigen Bereicherung* führen, die dem Täter oder der vom Täter als Empfängerin ausersehenen Person zukommt. Bei der Bereicherung handelt es sich eigentlich um die abschliessende *vierte Erfolgsstufe*. Die Lehre ordnet sie jedoch ausschliesslich dem subjektiven Tatbestand zu[78] und bringt damit zum Ausdruck, dass sie als überschiessende Innentendenz zur Vollendung der Straftat objektiv nicht einzutreten brauche. Diese Differenzierung entspricht einer sprachlogisch einwandfreien Analyse des Gesetzestextes, der verlangt, dass der Täter „in der Absicht, sich oder einen andern unrechtmässig zu bereichern", handeln müsse, jedoch nirgends hervorhebt, dass diese Bereicherung einzutreten habe. Eine praktische Bedeutung der Kupierung der vierten Erfolgsstufe ist nicht ersichtlich, zumal grundsätzlich jedes Erfolgsdelikt, bei dem nach Ausführung der Tathandlung der vom Täter angestrebte Erfolg nicht eintritt, als (vollendeter) Versuch gemäss Art. 22 Abs. 1 StGB strafbar ist und dadurch zum kupierten Erfolgsdelikt wird. Der Einfluss, den diese Erkenntnis auf die Auslegung des Wortes „Absicht" und die Figur der „Eventualabsicht"[79]

---

75 Das entspricht dem sog. Gefährdungsschaden; dazu: BGE 129 IV 124 E. 3.1 S. 125 f. (allg. Schadensdefinition); 102 IV 84 E. 4 S. 88 (Kreditbetrug); BSK StGB II-Maeder/Niggli, Art. 146, N 207; Corboz, Vol. I, Art. 146, N 37; Donatsch, Strafrecht III, 247; Hurtado Pozo, Partie spéciale, N 1201; PK StGB-Trechsel/Crameri, Art. 146, N 25; Stratenwerth/Jenny/Bommer, BT I, § 15 N 50.

76 Urteile des Bundesgerichts 6B_383/2013 vom 9. September 2013 E. 2.2; 6B_886/2013 vom 6. Februar 2014 E. 1.4. Das folgt aus dem objektiv-individuellen Vermögensbegriff; dazu: BSK StGB II-Maeder/Niggli, Art. 146, N 234 ff.; CR CP II-Garbarski/Borsodi, Art. 146, N 116; Donatsch, Strafrecht III, 248 f.; Hurtado Pozo, Partie spéciale, N 1203 ff.; PK StGB-Trechsel/Crameri, Art. 146, N 28; Stratenwerth/ Jenny/Bommer, BT I, § 15 N 53 f.

77 BGE 134 IV 210.

78 Corboz, Vol. I, Art. 146, N 43; CR CP II-Garbarski/Borsodi, Art. 146, N 126; Donatsch, Strafrecht III, 250; Hurtado Pozo, Partie spéciale, N 1213; PK StGB-Trechsel/Crameri, Art. 146, N 31; Stratenwerth/Jenny/Bommer, BT I, § 15 N 60.

79 Kritisch dazu: BSK StGB II-Maeder/Niggli, Art. 146, N 270 f.; Stratenwerth/Jenny/Bommer, BT I, § 15 N 64.

haben könnte, ist im vorliegenden Zusammenhang nicht weiter zu erläutern. Entscheidend ist jedoch, dass der Täter die Lüge mit Blick auf die ganze tatbestandsmässige Motivations- und Kausalkette äussert. Es muss sich mithin um eine Lüge handeln, der eine Schädigungs- und Bereicherungstendenz innewohnt, was z.B. bei in Vertragsverhandlungen vorgetäuschter Sympathie nicht der Fall ist.[80]

2. Arglistformel 1948

a) Bedeutung der Arglist für die Gesetzgeber von 1937 und 1994

Zum Brennpunkt der Lehre und Rechtsprechung zur schweizerischen Betrugsstrafnorm hat sich der Hinweis im Gesetzestext entwickelt, wonach der Täter „arglistig" vorgehen müsse. Im Gesetzgebungsverfahren, das zum Erlass des schweizerischen Strafgesetzbuches vom 21. *Dezember* 1937 geführt hat, war dem Wort Arglist nicht die Bedeutung zugedacht, eine besondere Qualität der Lüge oder gar eine Opfermitverantwortung zu kennzeichnen.[81] Die Ansicht, der Gesetzgeber habe mit dem Vorbehalt der Arglist eine Risikoverteilung zwischen Täter und Opfer vorgenommen,[82] lässt sich nicht mit der Genese des Strafgesetzbuches begründen.

Anders verhält es sich mit der Revision des Vermögens- und Urkundenstrafrechts vom 17. Juni 1994.[83] In der Zwischenzeit hatte das Bundesgericht der Arglist die Konturen verliehen, auf die sogleich einzugehen sein wird. In der Botschaft vom 24. April 1991 verwarf der Bundesrat das Ansinnen, die Arglisthürde abzuschaffen. Als Grund führte er an, diese habe sich in der Praxis be-

---

80 Die von Ackermann, Leichtsinn, 81, zitierte Grundregel für Verkäufer, den Hund des Kunden auch gegen das eigene Empfinden zu loben, ist deshalb unabhängig von Arglist und Opfermitverantwortung von vornherein nicht betrugsrelevant, obwohl sich ein solches Verhalten als unüberprüfbare Lüge über die innere Tatsache der Sympathie verstehen lässt. Betrugsrelevant wird vorgespiegelte Sympathie, wenn diese als wesentliche Grundlage des Zwecks der Zahlung des Opfers gedacht ist, insbesondere bei „Romance-Scamming".

81 Hafter, 263 f., der in der 1911 ernannten Expertenkommission mitgewirkt hatte, Botschaft 918 des Bundesrates an die Bundesversammlung zu einem Gesetzesentwurf enthaltend das schweizerische Strafgesetzbuch vom 23. Juli 1918, BBl 1918 IV 1 ff., 3; weitere Hinweise bei: Jean-Richard-dit-Bressel, Köderprinzip, 85 f.

82 Sägesser, N 450 f.; Wismer, 31.

83 Bundesgesetz über die Änderung des Schweizerischen Strafgesetzbuchs und des Militärstraftesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) vom 17. Juni 1994, in Kraft seit 1. Januar 1995, AS 1994 2290.

währt.[84] Der National- und der Ständerat stimmten dem diskussionslos zu.[85] Damit ist ein gesetzgeberischer Wille dokumentiert, dass dem Adverb „arglistig" im Betrugstatbestand die *Bedeutung* zukommen solle, die es *nach dem Stand der Rechtsprechung im Jahr 1991* hatte, und dass an dieser Praxis festzuhalten sei, da sie sich bewährt habe. Das Stichwort „Opfermitverantwortung" und eine entsprechende zweite Teststufe[86] waren nicht Gegenstand der vom Gesetzgeber gutgeheissenen Praxis.

b) Entwicklung der Arglistformel durch das Bundesgericht

Nach dem Inkrafttreten des Strafgesetzbuches im Jahr 1942 hat das Bundesgericht der Arglist mit seiner Rechtsprechung die Konturen verliehen, die im Grundsatz bis heute massgeblich sind. Dabei liess es sich von einer im Jahr 1912 im Gesetzgebungsverfahren geführten Diskussion inspirieren, bei der die Expertenkommission den Vorschlag, besondere Anforderungen an die Art der Täuschung zu stellen, zwar mit Interesse würdigte, ihn aber verwarf, weil die Idee noch nicht ausgereift erschien.[87] Leitentscheid um Leitentscheid entwickelte das Bundesgericht die Arglistformel, die es im Jahr 1948 folgendermassen zusammenfasste:

> „Zum Tatbestand des Betruges genügt nicht, dass der Täter in der Absicht, sich oder einen andern unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen irreführt oder den Irrtum eines andern benützt, sondern Art. 148 Abs. 1 StGB[88] verlangt ausserdem, dass der Täter arglistig handle. Das tut er nicht schon immer dann, wenn er lügt. Arglist liegt nicht vor, wenn der andere die Lüge ohne besondere Mühe überprüfen kann, ihm die Überprüfung zuzumuten ist und ihn der Täter weder absichtlich davon abhält, noch nach den Umständen voraussieht, dass der Getäuschte die Überprüfung unterlassen werde.[89] Allein auf diese Rechtsprechung kann sich der Täter nur berufen, wenn ihm nichts vorzuwerfen ist als eine einfache Lüge. Baut er ein ganzes Lügengebäude auf, das von besonderer Hinterhältigkeit zeugt, wendet er Kniffe an (manœuvres frauduleuses)[90] oder

---

84 BBl 1991 II, 1018.

85 AB 1993 N III 940; 1993 S V 958 f.

86 Unten, III.3.a), v.a. III.3.a)cc).

87 Diskussion der zweiten Expertenkommission an der Sitzung vom 26. September 1912, in: Schweizerisches Strafgesetzbuch, Protokoll der zweiten Expertenkommission, Bd. II, September–Oktober 1912 (EK 1912 II), 338 ff., zitiert in BGE 72 IV 13.

88 Seit dem 1. Januar 1995 Art. 146 Abs. 1 StGB, mit wenigen redaktionellen Änderungen gegenüber Art. 148 Abs. 1 aStGB, die für die Frage der Arglist ohne Bedeutung sind.

89 Hinweise im Zitat: BGE 72 IV 13, 123, 128, 159.

90 Hinweis im Zitat: vgl. Garraud, Traité du droit pénal français (3) 6 333 ff.

> stützt er die Lüge sonstwie durch Machenschaften (mise en scène)[91], so handelt er arglistig, unbekümmert darum, ob der Getäuschte sich durch Überprüfung der Angaben selbst schützen könnte."[92]

Das Bundesgericht unterschied somit eine einfache und eine erweiterte Lüge. Bei der *erweiterten Lüge*, die bis heute mit den Ausdrücken „Machenschaften" und „Lügengebäude" beschrieben wird, war die Überprüfbarkeit ohne Belang. Anders verhielt es sich schon damals mit der *einfachen Lüge*, die dadurch arglistig wurde, dass es mit der Überprüfbarkeit im Argen lag. Das Bundesgericht unterschied vier alternative Hemmnisse der Überprüfung, nämlich, dass diese (1) besondere Mühe erfordert, (2) unzumutbar ist, (3) vom Täter verhindert wird oder (4) für den Täter nach den Umständen voraussehbarerweise unterbleiben wird.

Zwar haben die Arglistkriterien bei der einfachen Lüge einen Bezug zu dem Gesichtspunkt, der erst viel später unter der Bezeichnung „Opfermitverantwortung" Einzug in die Rechtsprechung erhalten sollte. Es ist jedoch zu beachten, dass das Adverb „arglistig" im Gesetzestext *ausschliesslich das Verhalten des Täters* näher beschreibt. Zur Beurteilung der von ihm verwendeten Lüge war nicht zu prüfen, wie das Opfer konkret auf die Lüge reagiert hat, sondern nur, welche Möglichkeiten der Überprüfung ihm offenstanden. So war auch der früh gefundene und oft zitierte Leitsatz des Bundesgerichts gemeint:

> „Wer allzu leichtgläubig auf eine Lüge hereinfällt, wo er sich mit einem Mindestmass an Aufmerksamkeit durch Überprüfung der falschen Angaben selbst hätte schützen können, soll nicht den Strafrichter anrufen."[93]

Das war ausschliesslich als Massstab für die qualifizierte Täuschungshandlung gedacht und bedeutete nicht, dass die konkrete Eigenverantwortlichkeit des Opfers zu berücksichtigen war.

Die herrschende Lehre der 1940er- und 1950er-Jahre nahm die Einführung einer Arglisthürde durch das Bundesgericht keineswegs mit Wohlwollen auf, sondern übte scharfe Kritik.[94]

---

91 Hinweis im Zitat: BGE 73 IV 23.

92 BGE 74 IV 146 E. 1 S. 151 f.

93 BGE 72 IV 128; u.a. zitiert in: BGE 77 IV 85; 92 IV 65; 99 IV 78; 100 IV 274; 119 IV 35; 288; 120 IV 133; 187; 122 IV 205; 248; 126 IV 171; 128 IV 20; 135 IV 79 ff.

94 Hinweise bei: Jean-Richard-dit-Bressel, Köderprinzip, 85 f. und 90.

3. Opfermitverantwortung 1993

a) Wesen und Inhalt

Mit der Zeit änderte sich die Haltung der Lehre. In den 1980er-Jahren äusserten namhafte Stimmen Bedauern darüber, dass die Arglisthürde zu einer Leerformel verkomme, die kaum je eine Verurteilung verhindere. In jener Zeit nahm das Postulat der Opfermitverantwortung Einzug in das Schrifttum, zu dessen Verankerung im schweizerischen Strafrechtsdenken zwei vielbeachtete Dissertationen einen wesentlichen Beitrag leisteten.[95] Im Jahr 1993 verwendete das Bundesgericht das Stichwort „Opfermitverantwortung" erstmals in einem publizierten Entscheid, und zwar im „Rigi-Fall".[96]

aa) Sachverhalt des Leitentscheids

Das Opfer war eine durch einen Vizedirektor vertretene Bank. Der Vizedirektor hatte den Täter an einer früheren Arbeitsstelle als seinen Nachfolger kennengelernt. Auch der Täter wechselte die Stelle und arbeitete bei einer finanzstarken Firmengruppe. Aus dieser Position gab er dem Vizedirektor ohne jeden Wahrheitsbezug vor, von den deutschen Eigentümern dieser Gruppe beauftragt worden zu sein, als Strohmann eine Liegenschaft auf der Rigi unter Umgehung der schweizerischen Bewilligungsvorschriften zu erwerben. Dafür und für weitere Anschaffungen seiner angeblichen Auftraggeber beantragte der Täter einen Kredit im Betrag von 700 000 Franken, den ihm der Vizedirektor gewährte, um die finanzstarke Firmengruppe als Kundin zu gewinnen. Dabei prüfte er das angebliche Auftragsverhältnis weder durch Unterlagen noch durch Nachfrage bei den Gruppen-Eigentümern.[97]

bb) Erhöhung der Anforderungen an die Arglist des Täterverhaltens

Das Bundesgericht verneinte zunächst die Arglist deshalb, weil die verschiedenen Lügen z.B. durch Verlangen einer Vollmacht der angeblichen Auftraggeber überprüfbar und zudem nicht so raffiniert aufeinander abgestimmt gewesen seien, dass ein Lügengebäude vorliege:

> „Ein Lügengebäude und folglich Arglist ist erst anzunehmen, wenn die Lügen von besonderer Hinterhältigkeit zeugen und derart raffiniert aufeinander ab-

---

95 Ellmer, passim; Wismer, passim; Zusammenfassung dieser Dissertationen und weitere Hinweise in: Jean-Richard-dit-Bressel, Köderprinzip, 90 ff.

96 BGE 119 IV 28.

97 BGE 119 IV 28 E. 2.a S. 31 f.

> gestimmt sind, dass sich auch das kritische Opfer täuschen lässt. Ist das nicht der Fall, scheidet Arglist jedenfalls dann aus, wenn sowohl das vom Täter gezeichnete Bild insgesamt, als Ganzes, wie auch die falschen Angaben für sich allein in zumutbarer Weise überprüfbar gewesen wären und schon die Aufdeckung einer einzigen Lüge zur Aufdeckung des ganzen Schwindels geführt hätte."[98]

Bis zu diesem Punkt bewegte sich die Argumentation des Bundesgerichts grundsätzlich im Rahmen des bisherigen Verständnisses, wonach die Arglist nur unter dem Gesichtspunkt des Täterverhaltens zu beurteilen war. Daran änderte die Erhöhung der Anforderung an das Lügengebäude durch Einführung des „*kritischen Opfers*" als Massstab nichts. Wie die „besonnene Person" bei der Nötigung und Erpressung[99] bezweckt diese Figur die Objektivierung der Anforderungen und eben gerade nicht die Berücksichtigung des konkreten Opferverhaltens.[100] Wenige Jahre später stellte das Bundesgericht klar, dass das auch bei Machenschaften gelte.[101]

Bei der einfachen Lüge musste weiterhin die Überprüfbarkeit erschwert sein, während für die erweiterte Lüge neu die Anforderung galt, einem kritischen Opfer standzuhalten. Damit hat die *Unterscheidung von einfacher und erweiterter Lüge ihre Bedeutung verloren*, da sich ein kritisches Opfer dadurch auszeichnen muss, zumutbare Überprüfungen vorzunehmen. Letztlich geht es nun durchwegs um die Überprüfbarkeit.[102] Gleichwohl fragt die Rechtsprechung bis heute stets danach, ob Machenschaften oder ein Lügengebäude vorliegen.[103] Doch all das betrifft nicht die Opfermitverantwortung, sondern ist Ausdruck des Bestrebens, beim Betrug die Anforderungen an die Gefährlichkeit und kriminelle Energie des Verhaltens des Täters zu erhöhen.

cc) Berücksichtigung des Opferverhaltens als zusätzliche Teststufe

Das Bundesgericht brachte beim Rigi-Fall das Stichwort „Opfermitverantwortung erst im Rahmen einer *Eventualbegründung* ins Spiel: Die Bank sei verpflichtet, sich der Mitwirkung bei einem unrechtmässigen oder sittenwidrigen

---

98 BGE 119 IV 28 E. 3.c S. 36; Anwendung auf den konkreten Sachverhalt in E. 3.d S. 36 f.

99 Oben, II.1.b)bb).

100 Anscheinend anderer Meinung: Sägesser, N 339, die die Rechtsprechung des Bundesgerichts so versteht, dass es nicht massgeblich sei, „wie ein durchschnittlich vorsichtiger und erfahrener Dritter nach objektivierter Betrachtung auf die Täuschung reagiert hätte".

101 BGE 122 IV 197 E. 3.d. S. 205, wo dies allerdings irreführend als „Grundgedanke des Einbezugs des Opfers" bezeichnet wird.

102 So ausdrücklich in BGE 135 IV 76 E. 5.2 S. 82; gleicher Meinung: Ackermann, Leichtsinn, 88.

103 Z.B. BGE 147 IV 73 E. 3.2 S. 78 f.

Geschäft des Kunden zu enthalten und bei Anzeichen entsprechende Abklärungen zu treffen. Auf diese Erwägungen folgt nahtlos folgende weitere Überlegung:

> „[Die Bank] hat bei der Kreditvergabe zudem die elementarsten Vorsichtsmassnahmen missachtet. Auf die mündliche Zusicherung, für die Rückzahlung hafte ein begüterter Dritter, gewährte sie einen Kredit in der Höhe von mehreren hunderttausend Franken, ohne die Verhältnisse näher abzuklären und Sicherheiten zu verlangen. Bei dieser Sachlage ist die Arglist auch unter dem Gesichtspunkt der Opfermitverantwortung zu verneinen."[104]

Mit dem Rigi-Fall nahm das Bundesgericht den Begriff der *Opfermitverantwortung in* seine *Standardformulierungen zur Arglist* auf. Dabei fasste es jeweils im Grundsatz die traditionelle Arglistformel mit erhöhten Anforderungen an die erweiterte Lüge zusammen. Daran schloss in der Regel der Hinweis an, dass unter dem Gesichtspunkt der Opfermitverantwortung Arglist zu verneinen sei, wenn das Opfer „die grundlegendsten Vorsichtsmassnahmen nicht beachtet" habe, was nicht bei jeder Fahrlässigkeit des Opfers, sondern nur in Ausnahmefällen zu bejahen sei.[105]

Aus dieser ständig wiederholten Formel folgte, dass zu den Themen Arglist und Opfermitverantwortung ein *zweistufiger Test* durchzuführen war. Auf der ersten Stufe war das Täterverhalten zu prüfen, mit erhöhten Anforderungen an die Raffinesse des Lügengebäudes. Verhielt sich der Täter unter diesen Gesichtspunkten arglistig, war der Betrug noch nicht zu bejahen. Vielmehr war zusätzlich zu prüfen, ob das Opfer die grundlegendsten Vorsichtsmassnahmen beachtet habe. War dies zu verneinen, verhinderte dies die Verurteilung wegen Betrugs ungeachtet des arglistigen Täterverhaltens.[106]

Der zweistufige Test gemäss der 1993 begründeten Rechtsprechung liess sich in der Kurzformel „*Opfermitverantwortung bricht Arglist*" zusammenfassen. Nach hier verwendeter Terminologie ist deshalb die Opfermitverantwortung

---

104 BGE 122 IV 197 E. 3.f S. 38.

105 BGE 147 IV 73 E. 3.2 S. 80; 143 IV 302 E. 141 S. 306 f.; 142 IV 153 E. 2.2.2 S. 155; 135 IV 76 E. 5.2 S. 81; 126 IV 165 E. 2.a S. 172; 119 IV 28 Regeste.

106 Diese Zweistufigkeit zeigt BGE 135 IV 76 E. 5.2 S. 81 in umgekehrter Reihenfolge. Nach ausführlichen Erörterungen über die Opfermitverantwortung leitet das Bundesgericht die klassische Arglistformel mit erhöhten Anforderungen an die erweiterte Lüge folgendermassen ein: „Arglist wird nach all dem – soweit das Opfer sich mithin nicht in leichtfertiger Weise seiner Selbstschutzmöglichkeiten begibt – in ständiger Rechtsprechung bejaht, wenn […]".

nicht ein Synonym für Arglist oder ein Teilaspekt davon,[107] sondern das Ergebnis einer separaten Fragestellung, die nicht den aus der Sicht des Täters bestehenden Selbstschutzmöglichkeiten des Opfers, sondern den von diesem konkret vorgenommenen Sorgfaltsmassnahmen gilt.

Die so verstandene *Opfermitverantwortung* hatte anscheinend *nicht oft eine selbständige Bedeutung* in dem Sinne, dass die Arglist des Täterverhaltens zu bejahen war, der Betrug jedoch an der Missachtung der Vorsichtsmassnahmen durch das Opfer scheiterte. Beim Rigi-Fall war dies nicht der Fall. In einem neueren in der amtlichen Sammlung publizierten Entscheid, wo das Bundesgericht in der Regeste die Opfermitverantwortung hervorhob, verneinte es den Betrug, weil es für die Online-Verkäuferin zumutbar gewesen wäre, einen Drucker zum Preis von 2 200 Franken nur gegen Vorauskasse oder nach wenigstens rudimentärer Kreditprüfung zu liefern.[108] Damit entfiel Arglist bereits nach der klassischen Formel wegen der Überprüfbarkeit der einfachen Lüge. Eine zweite Teststufe und damit die Berufung auf die Opfermitverantwortung war unnötig. Anders verhielt es sich in einem Prozessbetrugsfall, wo das Bundesgericht die Arglist der Täuschung bejahte, weil sie der Kläger in einer förmlichen Parteiaussage unter der Strafdrohung von Art. 306 StGB bestätigt hatte;[109] gleichwohl entlastete ihn das Bundesgericht teilweise vom Betrugsvorwurf, weil sich das Opfer als beklagte Partei im Zivilprozess nicht adäquat zur Wehr gesetzt hatte.[110] In wie vielen Fällen der reichen Kasuistik[111] die zweite Teststufe in diesem Sinne eine selbständige Bedeutung hatte, lässt sich nicht ohne vertiefte Analyse beurteilen.

b) Begründung

Weshalb ist zusätzlich zur Arglist des Täterverhaltens auf einer weiteren Teststufe auch das Opferverhalten zu beurteilen? Das Bundesgericht verwies in diesem Zusammenhang auf *Präventionsziele*:

---

107 Trotz deutlicher Hinweise auf den Zweistufen-Test beschreibt auch das Bundesgericht die Opfermitverantwortung als Aspekt der Arglist, z.B. in BGE 135 IV 76 E. 5.2 S. 79 ff.; ebenso: Ackermann, Leichtsinn, 79; Sägesser, N 337, 369 f., die anscheinend beide Aspekte als Einheit sieht, obwohl sie ihre Analyse der Rechtsprechung überzeugend in „opferseitige Kriterien", N 195 ff., und „täterseitige Kriterien", N 279 ff., gliedert; Thommen, 35 f., der bei Opfermitverantwortung die Arglist des Täterverhaltens verneint, d.h. die Opfermitverantwortung nicht der Kausalität und dem Irrtum zurechnet, aber in Fällen mit Opfermitverantwortung gleichwohl für die Strafbarkeit als Versuch votiert.

108 BGE 142 IV 153.

109 Urteil des Bundesgerichts 6B_751/2018 vom 2. Oktober 2019 E. 1.5.2.

110 BGer 6B_751/2018 E. 1.5.3.

111 Umfassende Zusammenstellung bei: Graf, 60 ff.

> „Le principe de coresponsabilité doit amener les victimes potentielles à faire preuve d'un minimum de prudence. Il s'agit d'une mesure de prévention du crime, la concrétisation d'un programme de politique criminelle."[112]

Damit wurde dem Strafrecht eine vollkommen neue Aufgabe zugewiesen. Seit jeher war ihm neben der Kompensationsfunktion auch die Präventionsfunktion zugedacht, den Täter von weiteren Taten abzuhalten und Tatgeneigte abzuschrecken.[113] Sicher ist es auch richtig, potenzielle Opfer zu warnen und zur Vorsicht zu mahnen. Ebenso kann es durchaus angebracht sein, nachteilige Folgen an qualifizierte Unvorsichtigkeit zu knüpfen, z.B. die Kürzung oder Verweigerung von Versicherungsleistungen. Aber es ist nicht zweckmässig, dazu das materielle Strafrecht einzusetzen und einen Täter, der den Tatbestand des Betrugs einschliesslich der Arglist durch sein Verhalten erfüllt hat, mit dem Freispruch zu belohnen.[114] Diesen Standpunkte nimmt nun auch das Bundesgericht in einem richtungsweisenden Entscheid ein, den es am 13. September 2021 in Fünferbesetzung gefällt hat:

> „Der mit Art. 146 StGB bezweckte Vermögensschutz orientiert sich [...] notwendigerweise auch am Grundsatz von Treu und Glauben.[115] Wenn der Schutz des Strafrechts gegen den betrügerischen Angriff nur erhalten bliebe, wenn sich das Zielpublikum einer erhöhten Abwehrverantwortung unterzöge, so schränkte dies den Schutz von Treu und Glauben im Geschäftsverkehr empfindlich ein. Die Ausnutzung von sozialadäquatem Vertrauen ist regelmässig als arglistig zu werten. Im Übrigen kann es nicht Aufgabe des Strafrechts sein, das (potentielle oder tatsächliche) Opfer zu grösserer Vorsicht zu erziehen.[116]"[117]

4. Unterschiedliche Massstäbe für starke und schwache Opfer

Wie hiervor im Zusammenhang mit dem Wucher angemerkt worden ist,[118] unterschied die Rechtsprechung vor dem 13. September 2021 zwischen schwachen, schützenswerten Opfern, deren Leichtsinn den Täter nicht entlastet,

---

112 BGE 128 IV 18 E. 3.a S. 21, mit Hinweis auf Cassani.

113 So finden sich generalpräventive Strafbegründungen bereits im Deuteronomium, 13:12, 17:13, 19:20.

114 Ebenfalls kritisch: Braun, 104.

115 Hinweis im Zitat: Nydegger, 307 ff.

116 Hinweise im Zitat: Nydegger, 297 ff.; Jean-Richard-dit-Bressel, Köderprinzip, 99).

117 Urteil des Bundesgerichts 6B_184/2020 vom 13. September 2021 E. 2.1.5. Dieser Entscheid ist nach dem ursprünglichen Abschluss des vorliegenden Manuskripts ergangen.

118 Oben, II.1.c)bb).

und solchen, die zum Selbstschutz in der Lage wären, dies aber unterlassen.[119] Damit wurde das *Schuldprinzip*[120] *auf das Opfer ausgedehnt*. Dementsprechend wollten gewichtige Lehrmeinungen an die Fahrlässigkeitsdogmatik anknüpfen.[121] Für das Mass der vom Opfer verlangten Sorgfalt stellte das Bundesgericht zusätzlich auf dessen Beweggründe ab. Wer Vermögensdispositionen „aus reinem Altruismus" erwog, musste weniger kritisch sein, als jemand, der dies „geblendet von überzogenen Gewinnaussichten" tat.[122] Folglich kam es nicht nur auf den Grad und die Wirkungen, sondern auch auf den Sympathiegehalt der Schwäche des Opfers an, hätten doch sonst hilfsbereite Naivität und blinde Gier gleich behandelt werden müssen.

Die besonderen Verhältnisse des konkreten Opfers[123] sind weiterhin relevant, wenn die Lüge für einen „durchschnittlich vorsichtigen und erfahrenen Dritten" leicht durchschaubar und damit nicht arglistig ist.[124] Doch ist auch dann die Lage des Opfers nur zu berücksichtigen, „soweit der Täter diese kennt und ausnützt".[125] Dies folgt als entscheidender Gesichtspunkt aus dem Wesen des Betrugs als Vorsatzdelikt. Das entscheidende Kriterium ist deshalb nicht der Zustand des Opfers, sondern der *Modus operandi des Täters*. Wie suchte er sein Opfer aus? Was liess ihn auf dessen Inferiorität schliessen? Wie passte er sein Täuschungsverhalten seinen Erkenntnissen über spezifische Schwachstellen des Opfers an? Die Arglistformel von 1948 ist ein taugliches Hilfsmittel zur Beurteilung der vom Täter einkalkulierten Schwäche des Opfers. Hingegen trübt es den Blick auf das Verschulden des Täters, im Rahmen einer separaten, vom Verhalten und den Intentionen des Täters gelösten Teststufe nach dem Opferverschulden zu fragen.

---

119 Zur Anwendung unterschiedlicher Massstäbe für starke und schwache Opfer steht die Figur des „kritischen Opfers" in einem *Spannungsverhältnis*, nach dessen Täuschungsresistenz seit dem „Rigi-Fall" Lügengebäude und Machenschaften zu beurteilen sind, vgl. oben, III.3.a)bb).

120 Oben, I.1.a).

121 Ackermann, Leichtsinn, 91; Ellmer, 284 ff.

122 BGer 6B_683/2013 E. 2.2.

123 Z.B. Verliebtheit, dazu: Urteile des Bundesgerichts 1B_591/2011 vom 18. Juni 2012 E. 5.3; 6B_518/2012 vom 5. Februar 2013 E. 3.3.

124 BGer 6B_383/2013 E. 2.1.

125 BGE 120 IV 186 E. 1.a S. 188; 125 IV 124 E. 3.a S. 128; 126 IV 165 E. 2.a S. 172; 128 IV 18 E. 3.a S. 21.

5. Opfermitverantwortung bei Betrugsversuch

a) Abgrenzung und Interaktion von Täter- und Opferverhalten

Das Kriterium, dass das Opfer die grundlegendsten Vorsichtsmassnahmen beachten muss, entspricht ausschliesslich einer Anforderung an das *Verhalten des Opfers*. Das im Gesetzestext enthaltene Adverb „arglistig" gehört zu den Verben „irreführt" bzw. „bestärkt" und kennzeichnet damit einzig das *Verhalten des Täters*. Ob das Verhalten des Opfers den von der Betrugsstrafnorm aufgestellten Kriterien genügt, ist eine Frage der Kausalität oder des tatbestandsmässigen Erfolgs und damit eindeutig kein Aspekt der Arglist.[126]

Zwar bringt es die *Interaktion zwischen Täter und Opfer* mit sich, dass das Verhalten des Opfers das Verhalten des Täters beeinflusst. So ist es denkbar, dass der Täter es zunächst mit einer einfachen Lüge versucht, deren Überprüfung durch Rückfragen zumutbar ist. Nimmt das Opfer schon nach der überprüfbaren einfachen Lüge die vom Täter angestrebte Vermögensdisposition vor, erübrigt es sich für den Täter, durch Vorlegen gefälschter Urkunden oder Nachschieben eines Lügengebäudes seine einfache Lüge überzeugender erscheinen zu lassen, so dass er das Tatbestandsmerkmal der Arglist wenigstens in objektiver Hinsicht nicht verwirklicht. Zu diesem Ergebnis führt bereits die klassische Arglistformel, die der Interaktion zwischen Täter und Opfer hinreichend Rechnung tragen kann, ohne dass ein separater Opfermitverantwortungs-Test zu bemühen wäre.

Die der eigentlichen Arglist nachgelagerte Opfermitverantwortung käme indessen zum Tragen, wenn das unkritische Opfer dem Täter blind vertraut und die für ein kritisches Opfer *täuschenden Lügengebäude und Machenschaften*, mit denen es der Täter bedient hat, überhaupt *nicht würdigt*. Solcherlei ist bei Massenbetrügen und serienmässigen Anlagebetrügen an der Tagesordnung.[127] Der Täter hat im Hinblick auf eine unrechtmässige Bereicherung arglistig gehandelt, doch das Opfer hat „die grundlegendsten Vorsichtsmassnahmen nicht beachtet".

---

126 Gleicher Meinung: BSK StGB II-Maeder/Niggli, Art. 146 N 69; in dem Sinne nun auch BGer 6B_184/2020 E. 2.1.3.

127 Eindrücklich dokumentiert durch die Wiedergabe von Opferaussagen in BGer 6B_184/2020 E. 2.2.2.

b) *Wesen und Arten des Versuchs*

Irrt sich das Opfer überhaupt nicht oder nicht im erforderlichen Motivationszusammenhang, obwohl der Täter mit arglistigen Lügen auf dieses eingewirkt hat, so liegt ein *strafbarer Versuch* zu einem Betrug vor, entsprechend der Bestimmung von Art. 22 Abs. 1 StGB:

> „Führt der Täter, nachdem er mit der Ausführung eines Verbrechens oder Vergehens begonnen hat, die strafbare Tätigkeit nicht zu Ende oder tritt der zur Vollendung der Tat gehörende Erfolg nicht ein oder kann dieser nicht eintreten, so kann das Gericht die Strafe mildern."

Die Formulierung will die *drei Formen des Versuchs* abdecken, die in dem vor dem Jahr 2007 geltenden Strafgesetzbuch noch getrennt geregelt waren: den unvollendeten Versuch,[128] den vollendeten Versuch[129] und den untauglichen Versuch,[130] der unvollendet oder vollendet sein kann. Bei der seit Anfang des Jahrs 2007 geltenden Revision des allgemeinen Teils des Strafgesetzbuchs wollte der Gesetzgeber nicht etwa eine dieser Ausprägungen des Versuchs abschaffen, sondern es war ihm nur daran gelegen, die Gesetzgebung zu vereinfachen.[131]

Charakteristisch für alle Formen des Versuchs ist es, dass der Täter zumindest im Sinne des Eventualvorsatzes den ganzen Unrechtstatbestand verwirklichen will, wobei sich dieser Wille nur auf die Tatsachen und nicht auch auf deren rechtliche Würdigung zu beziehen braucht.[132] Das lässt sich auch so ausdrü-

---

128 Art. 21 Abs. 1 aStGB: „Führt der Täter, nachdem er mit der Ausführung eines Verbrechens oder eines Vergehens begonnen hat, die strafbare Tätigkeit nicht zu Ende, so kann er milder bestraft werden."

129 Art. 22 Abs. 1 aStGB: „Wird die strafbare Tätigkeit zu Ende geführt, tritt aber der zur Vollendung des Verbrechens oder des Vergehens gehörende Erfolg nicht ein, so kann der Täter milder bestraft werden."

130 Art. 23 Abs. 1 aStGB: „Ist das Mittel, womit jemand ein Verbrechen oder ein Vergehen auszuführen versucht, oder der Gegenstand, woran er es auszuführen versucht, derart, dass die Tat mit einem solchen Mittel oder an einem solchen Gegenstande überhaupt nicht ausgeführt werden könnte, so kann der Richter die Strafe nach freiem Ermessen mildern."

131 Botschaft des Bundesrates zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21. September 1998, BBl 1999, 1979 ff., 2010.

132 Statt vieler: BSK StGB I-Niggli/Maeder, Art. 12, N 14, Art. 22, N 1.

cken, dass der Täter mit der Ausführung der Tat beginnt und dabei den *subjektiven Tatbestand vollständig*, den objektiven Tatbestand jedoch nicht oder nur teilweise erfüllt.[133]

c) Vollendeter Betrugsversuch

aa) Vermögensdisposition ohne tatbestandsmässigen Irrtum

Hat der Täter das Opfer mit allen Fassetten seines arglistigen Täuschungskonzeptes konfrontiert, ohne dass dieses irrt, so hat er einen *vollendeten Versuch* begangen. Typischerweise wird es mangels Irrtums weder zu einer Vermögensdisposition noch zu einem Schaden kommen. Nimmt aber das Opfer *trotz Ausbleibens des tatbestandsmässigen Irrtums oder des Motivationszusammenhangs* mit der Täuschung die vom Täter angestrebte *Vermögensdisposition* vor, ändert das grundsätzlich nichts am Umstand, dass ein strafbarer Versuch vorliegt, jedenfalls dann, wenn das Opferverhalten nicht als Einwilligung auf einer adäquaten Informationsbasis zu verstehen ist.

Eine *Einwilligung des Opfers* lässt sich diskutieren, wenn dieses einen auf einem raffinierten Lügengebäude beruhenden *Bettelbetrug* durchschaut, aber dem Täter aus Mitleid oder als Entgelt für den Unterhaltungswert seiner Geschichte den gewünschten Betrag aushändigt. Die rechtfertigende Wirkung der Einwilligung erscheint hier allerdings deshalb zweifelhaft, weil das tatbestandsmässige Verhalten vor dieser erfolgte und der Täter auf die Täuschungswirkung seiner Geschichte baute und nicht darauf, dass diese die Bereitschaft zu einer einvernehmlichen Zahlung herbeiführen wird.

Keine Einwilligung des Opfers steht im Fall des *Versicherungsexperten* zur Diskussion, der den betrügerischen Charakter einer mit gefälschten Urkunden dokumentierten Schadensmeldung vermutet, aber sich wegen des kleinen Schadensbetrags angesichts des Aufwandes und Prozessrisikos einer Leistungsverweigerung aus wirtschaftlichen Gründen für die Auszahlung der Schadenssumme und gleichzeitige Versicherungskündigung entscheidet.[134] Gemäss der Regel „wer zweifelt, irrt“[135] lässt sich die nicht gesicherte Vermutung des Versicherungsexperten als Irrtum auslegen. Doch auch bei Verneinung eines Irrtums liegt keine freie Vermögensdisposition im Sinne einer

---

133 Statt vieler: Thommen, 34.

134 Beispiel aus der Praxis des Verfassers als Bezirksanwalt in Dielsdorf, 1996–1998, wobei eine erstinstanzliche Verurteilung wegen Betrugsversuchs rechtskräftig wurde.

135 Thommen, 35, mit Hinweis auf das deutsche Recht gemäss Arzt Gunther/Weber Ulrich, Strafrecht Besonderer Teil, Lehrbuch, Bielefeld 2000, § 20 N 65.

Einwilligung vor, denn die arglistigen Vorkehren lassen den Experten ein Prozessrisiko erkennen, das für eine Versicherungsgesellschaft bei Kleinschäden nicht zumutbar ist.[136] Es gehört in solchen Fällen durchaus zu Täterkalkül, dass sich das Opfer nicht nur bei einem Irrtum im engeren Sinne, sondern auch aufgrund solcher Erwägungen zur Vermögensdisposition motivieren lassen könnte.[137]

bb) Opferschwäche beim Anlagebetrug

Die auf Wirtschaftsdelikte spezialisierten Strafverfolgungsbehörden haben sich routinemässig damit zu befassen, dass ein *Anlageprodukt systematisch mit für die Risikobeurteilung relevanten Tatsachenbehauptungen angepriesen* wird, deren objektive Falschheit sich nur, aber immerhin mit aufwendigen Ermittlungen der Strafbehörden nachweisen lässt. Es liegt nahe, dass auch das Opfer eine solche Lüge nicht ohne besondere Mühe überprüfen konnte. Bei den Einvernahmen der Opfer zeigt es sich indessen häufig, dass sich viele keine Gedanken über die relevanten falschen Tatsachen gemacht oder aber vergessen haben, was den Ausschlag zu ihrem Investitionsentscheid gegeben hat. Solche Investoren gehen auf diffuse Art davon aus, der Täter sei „vertrauenswürdig", es gehe „mit rechten Dingen" zu, und das Produkt sei „gut und sicher".[138] In solchen Fällen fehlt es am Nachweis, dass das Opfer durch eine falsche Vorstellung über eine konkrete Tatsache zur Investition veranlasst worden ist. Damit ist das *Tatbestandsmerkmal des Irrtums, die erste Erfolgsstufe, nicht erfüllt*, ebenso wenig der dazu führende Motivationszusammenhang. Folglich ist es für die Beurteilung, ob der objektive Tatbestand erfüllt sei, unerheblich, dass das Opfer gleichwohl zu seinem Schaden die vom Täter geförderte Vermögensdisposition vorgenommen hat.

cc) Einschlägige Bundesgerichtsentscheide

In einem Fall mit breiter Anpreisung von Anlageprodukten bestand die für die Risikobeurteilung relevante Tatsachenbehauptung darin, dass ein Unternehmen mit einem genau definierten vorteilhaften Rating die Deckung des von den Investoren eingezahlten Kapitals der Beteiligungsgesellschaft garantiere, was auf jedem *Zeichnungsschein* erwähnt war. Die Anklage setzte darauf, dass in allen Fällen, in denen die Anleger einen solchen Zeichnungsschein unter-

136 In dem Sinne auch: BGE 143 IV 203 E. 1.3 S. 304 ff.; Arzt, Leichsinnige, 64; Teichmann/Weiss, 517 (Zustimmung zu BGE 143 IV 302).

137 So auch BGer 6B_184/2020 E. 2.2.3, dort in Bezug auf Massenbetrug.

138 Dieselbe Beobachtung berichtet Ackermann, Leichtsinn, 83, ordnet sie aber anders ein.

schrieben haben, zumindest ein strafbarer Betrugsversuch vorliege, der sich zufolge Gewerbsmässigkeit mit den vollendeten Taten zu einer Einheit verbinde. Das Bundesgericht bestätigte diese Taktik im Grundsatz:

> „Die Vorinstanz geht offenbar davon aus, dass in allen Fällen keine ‚Täuschung' erfolgte, in welchen die Anleger nicht wegen des unter anderem in den Zeichnungsscheinen zugesicherten Kapitalschutzes, sondern aus andern Gründen Aktien erwarben (siehe Urteil S. 16/17), weshalb auch keine Arglist vorliegen kann und daher nicht nur Betrug, sondern auch Betrugsversuch ausser Betracht fällt. Mit dieser Erwägung scheint die Vorinstanz zu verkennen, dass die Vorspiegelung von Tatsachen schon darin besteht, dass in den Zeichnungsscheinen, welche die Anleger unterschrieben, wahrheitswidrig ein Kapitalschutz zugesichert wurde. Es ist unerheblich, ob die Anleger diese unwahre Angabe als relevant erachteten und überhaupt zur Kenntnis nahmen. Daher ist in den Fällen, in denen die Geschädigten die Aktien nicht wegen des zugesicherten Kapitalschutzes, sondern aus andern Gründen erwarben, Betrugsversuch gegeben unter der Voraussetzung, dass die wahrheitswidrige Zusicherung eines Kapitalschutzes gegenüber den einzelnen Anlegern arglistig ist."[139]

Damit verwirft das Bundesgericht sinngemäss die mögliche These, in Analogie zu Art. 148 StGB[140] sei die Opfermitverantwortung beim Betrug als *objektive Strafbarkeitsbedingung* zu verstehen.[141] Das Fehlen einer solchen hätte die Strafbarkeit wegen Versuchs ausgeschlossen.

Die zitierten Ausführungen des Bundesgerichts gehen implizit davon aus, dass *Arglist und Opfermitverantwortung zwei getrennte Kriterien* sind. Denn es bezeichnet die Reaktion des Opfers als für die Beurteilung des Täuschungsverhaltens des Täters als „unerheblich". Unerheblich auf dieser Stufe ist mithin auch, ob die Opfer die elementarsten Sorgfaltspflichten beachtet haben.[142] Das Bundesgericht verdeutlicht dies in dem vorn erwähnten ganz neuen Entscheid, wo es darum ging, dass der Täter den Opfern gestützt auf eine automatische Telefoninteraktion unberechtigte Rechnungen zustellte:

---

139 Urteil des Bundesgerichts 6B_717/2012 vom 7. September 2013 E. 3.3.2.

140 Oben, II.2.a)bb).

141 BSK StGB II-Maeder/Niggli, Art. 146, N 102, unter ablehnendem Hinweis auf die Vorauflage BSK StGB II-Arzt, 3. A., Art. 146, N 104 ff.

142 In dem Sinne auch Thommen, 37, der im Ergebnis die Meinung vertritt, „dass die Täuschung für sich und ohne das Opferverhalten betrachtet objektiv arglistig" sein kann.

> „[D]ie Aufmerksamkeit und Vorsicht, die das Opfer effektiv aufbringt (resp. vermissen lässt), [ist] bei einem an sich tauglichen Täuschungsangriff nicht massgebend dafür, ob die Arglist zu bejahen oder zu verneinen ist (sondern nur dafür, ob ein versuchtes oder ein vollendetes Delikt vorliegt)."[143]

In den weiteren Erwägungen zu erstgenannten Entscheid erkannte das Bundesgericht, dass der Hinweis auf den Kapitalschutz im Zeichnungsschein eine ohne besondere Mühe überprüfbare einfache Lüge sei, dass der Täter aber teilweise Machenschaften eingesetzt habe, um diese Lüge zu stützen. Es erachtete die Schwelle zum strafbaren Versuch nur dann als überschritten, wenn das jeweilige Opfer zusätzlich zum Zeichnungsschein mit solchen Machenschaften konkret in Berührung gekommen sein sollte. Dies könnte so verstanden werden, dass der *Betrug nur dem vollendeten Versuch zugänglich* sein solle oder dass für die Strafbarkeit des Betrugsversuchs zumindest das Tatbestandsmerkmal der arglistigen Irreführung objektiv vollständig verwirklicht sein müsse.

d) Unvollendeter Betrugsversuch

Ein Grund, weshalb beim Betrug nur vollendeter und nicht auch unvollendeter Versuch strafbar sein soll, wird vom Bundesgericht im Zeichnungsschein-Entscheid nicht dargelegt und ist auch sonst nicht ersichtlich. Wenn der Täter beim Opfer in der *Absicht, mit Machenschaften nachzudoppeln*, vorerst eine noch nicht arglistige einfache Lüge platziert, hat er damit die Schwelle zum strafbaren Versuch überschritten, denn er hat „mit Tatentschluss ein objektives Tatbestandsmerkmal erfüllt".[144] Eine Lüge ist ein Tatbestandsmerkmal des Betrugs, das in dem für die Schwellentheorie massgeblichen Sinn erfüllt ist, auch wenn sie noch nicht in einen Gesamtzusammenhang gestellt ist, mit dem das weitere Tatbestandsmerkmal der Arglist verwirklicht wird.

Lässt sich dem Täter indessen nur die Bereitschaft, *bei Bedarf zu einem späteren Zeitpunkt* nachzudoppeln, nachweisen, so liegt in Bezug auf die Arglist nur ein *bedingter Tatentschluss* vor. Einen solchen lässt das Bundesgericht im hiervor zitierten Entscheid nicht genügen.[145] Dies ist mit der übrigen Rechtsprechung zu Schwellentheorie vereinbar, denn der Punkt, von dem es in der

143 BGer 6B_184/2020 E. 2.1.3.

144 BGE 131 IV 100 E. 7.2.1 S. 104.

145 BGer 6B_717/2012 E. 3.7.

Regel kein Zurück gibt, wird in diesem Fall nicht schon mit der Lüge erreicht, sondern erst mit dem Eintritt der Bedingung, dass das Opfer kritische Rückfragen an den Täter richtet und nach Unterlagen verlangt.[146]

Ein solches Zusammenspiel von Täter- und Opferverhalten ist in Fällen zu beobachten, in denen nach Auffassung des Bundesgerichts die vom Opfer *tatsächlich vorgenommenen Massnahmen* zur Überprüfung genügten.[147] So würdigte es das Verhalten der Täterin anlässlich der Exploration durch den medizinischen Gutachter als „besondere betrügerische Machenschaften", „namentlich die übertriebene Darstellung ihrer Schmerzen und der Einschränkung ihrer Bewegungsfreiheit in Verbindung mit der verkrampften antalgischen Haltung ihres rechten Arms sowie die vorgespielten Schwierigkeiten beim Entkleiden". Gleichwohl hob das Bundesgericht hervor, dass der medizinische Experte nicht ausschliesslich auf die Darstellung der der Täterin abgestellt, sondern deren Angaben im Rahmen seiner Möglichkeiten überprüft habe.[148] Dabei handelte es sich weitgehend um Massnahmen im Rahmen der dreistündigen Exploration, die die Täterin zu immer weiteren Inszenierungen veranlasst haben mögen. Doch ist in diesem Fall das Bundesgericht davon ausgegangen, dass die Inszenierung eine „systematische Vorbereitung" erfordert habe. Das Übertreten der Schwelle der Praxis des Experten in der Absicht, ihm die gut einstudierten Symptome möglichst glaubhaft vorzuspielen, entspricht auch der Schwelle zum strafbaren Versuch. Nach dieser bewährten Rechtsprechung wäre die Täterin genauso strafbar gewesen, wenn sie auf einen weniger kritischen Experten getroffen wäre und ihre vorbereitete Inszenierung nur teilweise hätte aufführen müssen.[149]

e) Untauglicher Betrugsversuch

Es gibt nicht nur den Fall, dass es sich für den Täter wegen Leichtgläubigkeit des Opfers erübrigt, sämtliche vorbereiteten Täuschungsmassnahmen zu ergreifen. Denkbar ist es auch, dass der Täter aus bestimmten Gründen annimmt, sein Opfer habe eine Schwäche, die er gezielt für eine betrugsrelevante Täuschung ausnützen will, die für ein Opfer ohne solche Schwäche leicht durchschaubar ist. Ein solches Verhalten gilt nach der Rechtsprechung als arg-

---

146 Kein Tatentschluss liegt im bedingten Handlungswillen, BSK StGB I-Niggli/Maeder, Art. 22, N 3.

147 Zusammenstellung bei: Sägesser, N 230 ff.

148 Urteil des Bundesgerichts 6B_46/2010 vom 19. April 2010 E. 4.3.

149 Arzt, Leichtsinnige, 58, überzeugend zur Fragwürdigkeit, dem Versicherungsunternehmen das mögliche Versagen des mit der Prüfung beauftragten Experten als Opfermitverantwortung anzurechnen.

listig.[150] Geht der Täter *irrtümlich* von einer solchen *Schwäche des Opfers* aus, ist es für sein Täuschungskonzept in doppelter Hinsicht ein untaugliches Objekt, einerseits, weil die Lüge diesem Opfer gegenüber unwirksam ist, und andererseits, weil die Lüge gegenüber einem starken Opfer nicht arglistig ist. Der Täter hat demnach einen vollendeten Versuch am untauglichen Objekt begangen, der strafbar ist, wenn er nicht gemäss Art. 22 Abs. 2 StGB „aus groben Unverstand" gemeint hat, das Opfer sei mit einer bestimmten Schwäche geschlagen.

Der Täter, der in der Absicht der Täuschung und unrechtmässigen Bereicherung *massenweise plumpe Lügen* verbreitet,[151] rechnet aufgrund von statistischen Überlegungen und somit aus bestimmten Gründen damit, auf Opfer zu treffen, die aufgrund einer Schwächesituation dafür empfänglich sind. Die kriminalistische Erfahrung gibt diesem Täter recht. Er stellt diese Überlegung jedenfalls nicht aus grobem Unverstand an. In Bezug auf jeden Adressaten der plumpen Lüge hält es der Täter ernsthaft für möglich, dass es sich dabei um ein geeignetes Opfer handeln könnte. Sähe er das nicht so, würde er sich die Mühe eines Versuchs sparen. Es verhält sich ähnlich wie beim Erwerb eines Lotteriescheins. Damit ist seine Lüge in jedem Fall für das taugliche Opfer bestimmt und folglich arglistig, auch wenn es nach dem „Lotterie-Prinzip" in den meisten Fällen beim untauglichen Versuch bleibt. In seinem vorgenannten neuen Entscheid würdigt es das Bundesgericht denn auch als Arglistmechanismus, dass der Täter zehntausend Scheinrechnungen versandte und damit nur gerade 174 Opfer zur Vermögensdisposition motivieren konnte:

> „Aus Tätersicht war es zwingend erforderlich, einen weiten Personenkreis anzusprechen, um einen wirtschaftlichen Taterfolg zu erzielen. So betrachtet handelt es sich bei den 174 Personen um eine signifikante Grösse. Nicht die ‚Erfolgsquote' des täuschenden Vorgehens zählt, sondern dessen qualitative Eignung, den zumutbaren Selbstschutz von potentiellen Opfern – und sei es wie hier nur eine Minderheit der insgesamt erreichten Personen – zu überwinden und sie im Sinn von Art. 146 Abs. 1 StGB in die Irre zu führen."[152]

f) Fazit zum Betrugsversuch

Im Ergebnis zeigt es sich, dass es der Bestrafung des Täters wegen Betrugsversuchs nicht entgegensteht, wenn das Opfer „die grundlegendsten Vorsichtsmassnahmen nicht beachtet" hat, wenn es mit Lügen des Täters in Berührung gekommen ist, die von der Absicht unrechtmässiger Bereicherung getragen

---

150 Oben, II.2.c)bb), III.4.

151 Bei diesem Modus operandi verneinte die Praxis die Arglist schon vor 1993, BBl 1991 II, 1017 f.

152 BGer 6B_184/2020 E. 2.1.4.

sind und insgesamt das Tatbestandsmerkmal der Arglist erfüllen.[153] Dies ist auch bei massenweise verbreiteten plumpen Lügen der Fall, da der Täter bei diesem Vorgehen damit rechnet, auf das dafür empfängliche schwache Opfer zu treffen. Demnach führt die der Feststellung der klassischen Arglist nachgelagerte Prüfung der *Opfermitverantwortung nicht zur Straflosigkeit*, sondern lediglich dazu, dass das Gericht die Vollendung des Betrugs verneint und die Strafe wegen Versuchs mildert.[154]

Vorsichtsmassnahmen des Opfers im Sinne von Rückfragen können jedoch eine Bedeutung erlangen, wenn erst diese im Sinne der Schwellentheorie den Tatentschluss des Täters wecken, seine überprüfbare einfache Lüge durch Machenschaften oder weitere Lügen zu ergänzen, die insgesamt den Anforderungen an die Arglist genügen. Insofern ist das „Angriffsparadigma", dem die klassische Arglistformel verpflichtet ist, dafür geeignet, der *Interaktion zwischen Täter und Opfer* hinreichend Rechnung zu tragen.[155]

6. Unlauterer Wettbewerb als Auffangnorm

Das Problem, dass die Unvorsichtigkeit des Opfers den arglistig handelnden Täter von der Strafbarkeit entlasten könnte, wird durch die neue bundesgerichtliche Rechtsprechung im Scheinrechnungs-Fall entschärft. Gleichwohl hat unlauterer Wettbewerb gemäss Art. 23 UWG in Verbindung Art. 3 Abs. 1 Bst. b UWG *im kommerziellen Bereich* weiterhin eine Bedeutung als Auffangnorm zu Betrug, wenn der erforderliche Strafantrag vorliegt:

> „Unlauter handelt insbesondere, wer: b. über sich, seine Firma, seine Geschäftsbezeichnung, seine Waren, Werke oder Leistungen, deren Preise, die vorrätige Menge, die Art der Verkaufsveranstaltung oder über seine Geschäftsverhältnisse unrichtige oder irreführende Angaben macht oder in entsprechender Weise Dritte im Wettbewerb begünstigt."

Arglist ist für die Strafbarkeit gemäss dieser Norm nicht erforderlich. Nach dem Wortlaut handelt es sich an sich um ein *abstraktes Gefährdungsdelikt*, da sich falsche Angaben auch in Auslagen und Massenmedien und damit ohne konkrete Ansprechperson machen lassen.

Allerdings war bis vor dem 1. April 2012 für die Strafbarkeit eine konkrete Gefährdung erforderlich, da sonst niemand zum *Strafantrag* berechtigt war. Dem hat die Einführung des Klage- und Strafantragsrecht des Bundes gemäss Art. 10 Abs. 3 UWG in Verbindung mit Art. 23 Abs. 2 UWG Abhilfe geschaffen.

---

153 So im Ergebnis auch: Braun, 104; Thommen, 35 f.

154 BGer 6B_184/2020 E. 2 passim.

155 Anscheinend anderer Meinung: Ackermann, Leichtsinn, 86.

Das Klagerecht besteht namentlich dann, „wenn: b. die Interessen mehrerer Personen oder einer Gruppe von Angehörigen einer Branche oder andere Kollektivinteressen bedroht oder verletzt sind". Zum Strafantrag berechtigt und damit gemäss Art. 118 Abs. 4 StPO als potenzieller Privatkläger zu informieren ist das Staatssekretariat für Wirtschaft (SECO).[156]

Es ist durchaus *im Sinne der Gesetzgebungsorgane*, auf den unlauteren Wettbewerb auszuweichen, wenn der Betrug am Fehlen der Arglist oder an dem für deren Nachweis erforderlichen Aufwand scheitert. In der Beratung des Nationalrats zu einer Initiative zur Abschaffung der Arglisthürde beim Betrug begründete der Kommissionssprecher den Antrag auf Ablehnung, dem der Rat in der Folge zustimmte, unter anderem mit dem folgenden Hinweis:

> „Ein Weg über das Bundesgesetz gegen den unlauteren Wettbewerb wird als unter Umständen zielführender erachtet."[157]

Auch in den Materialien zur Revision des Vermögensstrafrechts von 1994 findet sich im Rahmen der Begründung der Beibehaltung der Arglisthürde beim Betrug ein Hinweis auf die Abgrenzung zum unlauteren Wettbewerb.[158]

IV. Schlussbetrachtung

1. Begrüssung der Rückkehr zur klassischen Arglisthürde

Der Versuch, im Strafrecht ein System von potenzieller Opfermitverantwortung zu skizzieren (Titel II) hat ergeben, dass sich nur wenige vage Ansätze dazu finden lassen. Die grösste Bedeutung hat die Kenntlichmachung des Opferwillens, wenn dieser als Tatbestandsmerkmal von Bedeutung ist und sich nicht selbstverständlich aus den Umständen ergibt. Damit besteht ein enger Zusammenhang zwischen der Opfermitverantwortung und dem Unrechtstatbestand. Beim Betrug hat dieser Aspekt kaum eine Bedeutung, denn er ist gekennzeichnet durch die Manipulation des vom Täter im Grundsatz erkannten Opferwillens. Die Opfermitverantwortung beim Betrug erweist sich als zusätzliches Kriterium ausserhalb des Unrechtstatbestands. Sie steht aufgrund dessen *in der Strafrechtsordnung als isoliertes Phänomen* da, dem es mangels Einbettung in einen Gesamtzusammenhang an Überzeugungskraft fehlt.[159]

---

156 Verordnung über das Klagerecht des Bundes im Rahmen des Bundesgesetzes gegen den unlauteren Wettbewerb vom 12. Oktober 2011, SR 241.3.

157 AB 2013 N 1371 ff., 1373, zur Initiative Jositsch, 12.438, Betrug ohne Arglisthürde.

158 BBl 1991 II, 1018.

159 Graf, 87, sieht darin zu Recht „kriminalpolitische Willkür"; vgl. auch Arzt, Leichtsinnige, 50.

Die Opfermitverantwortung im Betrug wurde mit dem Zweck begründet, der menschlichen Schwäche (Titel I) entgegenzuwirken und das *Opfer zur Vorsicht zu mahnen*, indem sie den Täter bei qualifizierter Unvorsichtigkeit des Opfers von Schuld und Strafe entlastet. Es handelte sich in dieser Form um eine singuläre Erscheinung, die quer zu den Aufgaben stand, die das Strafrecht sonst zu erfüllen hat. Im Vorfeld des Präventionsforums vom 23. März 2021 interviewte ein Kamera-Team Passanten auf der Strasse und stellte ihnen unter anderem die Frage, ob eine Opfermitverantwortung beim Betrug potenzielle Opfer zu mehr Vorsicht bewegen würde. Dies wurde durchwegs verneint. Diese Einschätzung wirkt überzeugend, zumal sich die Bestrafung des Täters nicht mit einem Schadensausgleich durch eine Versicherungsleistung vergleichen lässt. Die volle Restitution gemäss Art. 70 Abs. 1 in fine StGB ist zwar eine erwünschte, aber so seltene Nebenfolge des Strafverfahrens, dass die Annahme, das potenzielle Opfer könnte sein Verhalten danach ausrichten, lebensfremd erscheint.[160]

Entsprechend dem Ergebnis der vorliegenden Betrachtung *genügt* die *klassische Arglistformel* von 1948 vollumfänglich. Diese entspricht dem Willen des Gesetzgebers.[161] Insbesondere ist es ausreichend, „wenn die Frage der Arglist richtigerweise als Frage der Täuschungsqualität behandelt wird, wobei Leichtsinn nicht als Aufhebungsgrund an sich bestehender Arglist zu verstehen ist“[162]. Die zweckmässigen Anforderungen an die Täuschungsqualität gemäss der ursprünglichen Formel vermögen sämtliche nicht strafwürdigen Verhaltensweisen aus dem Tatbestand herauszufiltern, namentlich marktübliche Verkaufsstrategien mit Schmeicheleien, durchschaubaren Übertreibungen und überschwänglichen Werturteilen. Es ist deshalb zu begrüssen, dass es das Bundesgericht nun ablehnt, einem Täter, der arglistig gehandelt hat, in Form der Opfermitverantwortung eine zusätzliche Verteidigungswaffe in die Hand zu geben, die zur vollständigen Entlastung führen kann.[163]

Für die Strafbehörden führte die der Arglist nachgelagerte Opfermitverantwortung zu einem weiteren *komplexen Beweisthema*, das in Fällen mit zahlreichen Opfern einen sehr *grossen Zusatzaufwand* verursachte.[164] Mit der Opfermitverantwortung in der nun überwundenen Form ging ferner eine *übermässige Rechtsunsicherheit* einher, welche Vorsichtsmassnahmen zu den grundlegendsten gehören sollen. „Das bundesgerichtliche Dickicht der Opfer-

160 Gleicher Meinung: Arzt, Leichtsinnige, 49.

161 Oben, III.2.a).

162 BSK StGB II-Maeder/Niggli, Art. 146, N 101.

163 BGer 6B_184/2020 E. 2.1.3.

164 Ackermann, Leichtsinn, 91; Arzt, Leichtsinnige, 46, 48.

mitverantwortung ist nur schwer zu durchdringen."[165] Auf diese Art liess das System die Strafjustiz auf Kosten der Steuerpflichtigen eine oft zufällige Auswahl von Fällen mit einem übertriebenen Aufwand und hohem Freispruchrisiko führen, was zur Folge hatte, dass mangels Kapazität ein Teil der Fälle „auf die Halde gelegt" werden musste und nur mit erheblicher Verzögerung bearbeitet werden konnte,[166] soweit die Verfahren nicht ohne nähere Prüfung wegen des ersten Anscheins einer Opfermitverantwortung in Verletzung des Grundsatzes „in dubio pro duriore" eingestellt wurden.[167] Angesichts der Rechtsunsicherheit und der Abkoppelung vom Tatverhalten ist der Einwand, dass gute Justiz eben ihren Preis habe, in Bezug auf die Opfermitverantwortung nicht berechtigt.

2. Möglichkeiten zur Berücksichtigung der Opfermitverantwortung

Eine Möglichkeit, der Opfermitverantwortung Rechnung zu tragen, bietet das *Opportunitätsprinzip*. Sehr weit geht der Vorschlag, diesem bei geringem Interesse der Öffentlichkeit im Vermögensstrafrecht umfassende, nicht auf den Betrug beschränkte Geltung zu verleihen, wenn das Opfer die zumutbaren Vorsichtsmassnahmen schuldhaft nicht ergriffen hat.[168] Problematisch daran ist, dass die überlasteten Strafverfolgungsbehörden, die den Einwand der Opfermitverantwortung vor allem als Mittel zur Verkürzung der Pendenzenlisten schätzen, dadurch einen zusätzlichen Anreiz erhielten, zahlreiche Fälle voreilig ab Blatt einzustellen.[169] Das „geringe Interesse der Öffentlichkeit" ist ein flexibles Mass. Die ernsthafte Abklärung, welche Vorsichtsmassnahmen zumutbar sind und ob das Opfer sie ergriffen hat, erfordert erheblichen Aufwand. Zudem sind diese Voraussetzungen des Opportunitätsprinzips mit Rechtsunsicherheiten behaftet, die geeignet sind, das Beschwerden-Karussell anzutreiben.

Hingegen kann es angebracht sein, einer qualifiziert unvorsichtigen geschädigten Person wegen Rechtsmissbrauchs die *Konstituierung als Privatkläger* gemäss Art. 118 Abs. 1 StPO zu *verwehren*. Dies ist gestützt auf Art. 2 ZGB[170], der

---

165 Konklusion von Graf, 83, nach eingehender Analyse der Kasuistik.

166 Arzt, Leichtsinnige, 71; Braun, 107.

167 BGer 1B_591/2011 E. 5.3 zu „in dubio pro duriore" bei potenzieller Opfermitverantwortung.

168 Vorschlag von Graf, 89.

169 In dem Sinne auch: Arzt, Leichtsinnige, 74.

170 Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (ZGB, SR 2010).

sich auch auf den Strafprozess erstreckt, bereits de lege lata möglich.[171] Nach erfolgter Konstituierung lässt sich die Parteistellung mit einer Verfügung entziehen, sobald die Grundlagen für den Rechtsmissbrauch ermittelt sind.[172] Der Entzug der Parteistellung bewirkt, dass die Interessen der geschädigten Person bei Entscheiden, das Verfahren wegen Unerheblichkeit der zusätzlichen Strafe gemäss Art. 8 Abs. 2 und 3 StPO oder wegen Wiedergutmachung gemäss Art. 53 StGB einzustellen, nicht zu berücksichtigen sind. Ohne Parteistellung können die geschädigten Personen kein abgekürztes Verfahren gemäss Art. 358 StPO verhindern. Schliesslich sind sie mangels Parteistellung auch daran gehindert, ihre Zivilansprüche adhäsiv im Strafverfahren beurteilen zu lassen oder dieses zur Beweismittelbeschaffung für ein ordentliches Zivilverfahren zu nutzen. Damit ist der Sorge, dass das qualifiziert unsorgfältige Opfer keinen strafrechtlichen Schutz verdiene, hinreichend Rechnung getragen.

Literaturverzeichnis

Ackermann Jürg-Beat, „Sträflicher Leichtsinn" oder strafbarer Betrug? – zur rationalen Kriminalisierung der Lüge, in: Ackermann Jürg-Beat/Hilf Marianne Johanna (Hrsg.), Alles Lüge? – Betrug, Betrüger und Betrogene in der Strafrechtspraxis, Zürich 2014, 75 ff.

Ackermann Jürg-Beat et al., Strafrecht Individualinteressen, Bern 2019.

Annotierter Kommentar StGB, in: Graf Damian K. (Hrsg.), Bern 2020 (zit. AK StGB-Bearbeiter/in, Art. XX, N YY).

Arzt Gunther, Über den Nutzen der Rechtsunsicherheit, recht 2001, 166 ff.

Arzt Gunther, Leichtsinnige juristische Personen – Vom Sinn und Unsinn des Leichtsinns als Reduktion des Schutzes gegen Betrüger, in: Ackermann Jürg-Beat/Hilf Marianne Johanna (Hrsg.), Alles Lüge? – Betrug, Betrüger und Betrogene in der Strafrechtspraxis, Zürich 2014, 41 ff.

Basler Kommentar zum Bundesgesetz gegen den unlauteren Wettbewerb (UWG), in: Hilty Reto M./Arpagaus Reto (Hrsg.), Basel 2013 (zit. BSK UWG-Bearbeiter/in, Art. XX, N YY).

Basler Kommentar zum Obligationenrecht, Band I (Art. 1–529 OR), in: Widmer Lüchinger Corinne/Oser David (Hrsg.), 7. A., Basel 2019 (zit. BSK OR I-Bearbeiter/in, Art. XX, N YY).

---

171 Das Gebot von Treu und Glauben und das Rechtsmissbrauchsverbot von Art. 3 Abs. 2 Bst. a und b StPO sprechen zwar nur die Strafbehörden an, doch die Rechtsprechung weitet diese Grundsätze auf Parteien und andere Verfahrensbeteiligte aus, namentlich zur Prüfung der Gültigkeit der Konstituierung als Partei: BGE 125 IV 79 E. 1.d S. 82 (Parteistellung des Doping-Opfers); 105 IV 229 passim (Strafantrag wegen Entziehung von Unmündigen); BSK ZGB I-Honsell, Art. 2, N 54.

172 BGE 105 IV 220 E. 1 S. 231: „Dass sich die Frage des Rechtsmissbrauchs erst im späteren Verlaufe des Verfahrens stellen kann, zeigt gerade der vorliegende Fall, wo sie vorerst von keiner Seite aufgeworfen wurde, weil der entsprechende Sachverhalt nicht hinreichend abgeklärt war."

Basler Kommentar zum Strafrecht, Band I (Art. 1–110 StGB, Jugendstrafgesetz), in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), 4. A., Basel 2019 (zit. BSK StGB I-Bearbeiter/in, Art. XX, N YY).

Basler Kommentar zum Strafrecht, Band II (Art. 111–392 StGB), in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), 4. A., Basel 2019 (zit. BSK StGB I-Bearbeiter/in, Art. XX, N YY).

Basler Kommentar zum Zivilgesetzbuch, Band I (Art. 1–456 ZGB), in: Geiser Thomas/Fountoulakis Christiana (Hrsg.), 6. A., Basel 2018 (zit. BSK ZGB I-Bearbeiter/in, Art. XX, N YY).

Boll Damian, Verteidigung der ersten Stunde gemäss schweizerischer StPO, Zürich 2020.

Braun Robert, Anlagebetrug aus strafrechtlicher Sicht – Problemfelder und Lösungsansätze, fp 2010, 103 ff.

Cassani Ursula, Der Begriff der arglistigen Täuschung als kriminalpolitische Herausforderung, ZStrR 117 (1999) 174 ff.

Commentaire Roman du Code pénal, Tome I (Art. 1-110 CP), in: Moreillon Laurent et al. (Editeurs), 2e éd., Bâle 2021 (cit. CR CP I-auteur/e, Art. XX, N YY).

Commentaire Roman du Code pénal, Tome II (Art. 111–392 CP), in: Macaluso Alain/Moreillon Laurent/Queloz Nicolas (Editeurs), 2e éd., Bâle 2021 (cit. CR CP I-auteur/e, Art. XX, N YY).

Donatsch Andreas, Strafrecht III, Delikte gegen den Einzelnen, 11. A., Zürich 2018.

Donatsch Andreas/Tag Brigitte, Strafrecht I, Verbrechenslehre, 9. A., Zürich 2013.

Ellmer Manfred, Betrug und Opfermitverantwortung, Diss. Erlangen-Nürnberg 1984/85.

Furrer Andreas et al. (Hrsg.), Obligationenrecht, Zürich 2018.

Graf Damian K., Schützt das Strafrecht auch Dumme? Zur Opfermitverantwortung beim Betrug, ZStrR 139 (2021), 55 ff.

Hafter Ernst, Schweizerisches Strafrecht, Besonderer Teil, Hälfte I, Berlin 1937.

Handkommentar zum Schweizerischen Strafgesetzbuch, in: Wohlers Wolfgang/Godenzi Gunhild/Schlegel Stephan, 4. A., Bern 2020 (zit. HK StGB-Bearbeiter/in, Art. XX, N YY).

Hurtado Pozo Jozé, Droit pénal, Partie spéciale, Zürich 2009.

Jean-Richard-dit-Bressel Marc, „Am Köder vorbei in die Falle", Arglist, Opfermitverantwortung und „Köderprinzip" bei Serienbetrügen (Art. 146 StGB), in: Cavallo Angela et al. (Hrsg.), Liber amicorum für Andreas Donatsch, Zürich 2012, 75 ff.

Jean-Richard-dit-Bressel Marc, Informationsgefälle und Waffengleichheit, in: Ackermann Jürg-Beat/Wohlers Wolfgang (Hrsg.), Umfangreiche Wirtschaftsstrafverfahren in Theorie und Praxis, Zürich 2008, 139 ff.

Käser Beatrice, Sozialleistungsbetrug – Sozialversicherungsbetrug / Sozialversicherungsmissbrauch, Zürich 2012.

Kaufmann Ariane, Das Unmittelbarkeitsprinzip und die Folgen seiner Einschränkung in der Schweizerischen Strafprozessordnung, Zürich 2013.

Kommentar zum Bundesgesetz gegen den unlauteren Wettbewerb (UWG), in: Heizmann Reto A./Loacker Leander D. (Hrsg.), Zürich/St. Gallen 2017 (zit. K UWG-Bearbeiter/in, Art. XX, N YY).

Nydegger Micha, Grund und Grenzen der Arglist beim Betrug, in: ZStrR 131 (2013), 301 ff.
Praxiskommentar zum schweizerischen Strafgesetzbuch, in: Trechsel Stefan/Pieth Mark (Hrsg.), 4. A., Zürich/St. Gallen 2021 (zit. PK StGB-Bearbeiter/in, Art. XX, N YY).
Sägesser Heidi, Opfermitverantwortung beim Betrug, Bern 2014.
Stratenwerth Günter, Schweizerisches Strafrecht, Allgemeiner Teil I, Die Straftat, 4. A., Bern 2011.
Stratenwerth Günter/Jenny Guido/Bommer Felix, Schweizerisches Strafrecht, Besonderer Teil I, Straftaten gegen Individualinteressen, 7. A., Bern 2010.
Teichmann Fabian/Weiss Marco, Opfermitverantwortung beim Versicherungsbetrug, Urteilsbesprechung BGE 143 IV 302, Anwaltsrevue 2018, 513 ff.
Thommen Marc, Opfermitverantwortung beim Betrug, ZStrR 126 (2008), 17 ff.
Urwyler Thierry, Das Teilnahmerecht der Verteidigung am Explorationsgespräch des psychiatrischen Sachverständigen mit der beschuldigten Person im Lichte der EMRK, Zürich 2019.
Vischer Markus/Galli Dario, BGer 4A_141/2017: Opfermitverantwortung bei der zivilrechtlichen absichtlichen Täuschung, AJP 2017,1393 ff.
Wismer Willi, Das Tatbestandsmerkmal der Arglist beim Betrug, Diss. Zürich 1988.
Zehnder Stefanie, Die Heilung strafbehördlicher Verfahrensfehler durch Rechtsmittelgerichte, Zürich 2016.

Zuletzt erschienene Bände bei EIZ Publishing, Zürich

Band 201 **Challenges, risks and threats for security in Europe**
11th Network Europe Conference, Warsaw, 19th–22nd May 2019
Andreas Kellerhals/Tobias Baumgartner (Hrsg.), mit Beiträgen von Viorel Cibotaru, Attila Vincze, Przemyslaw Saganek, Jelena Ceranic, Aleksei V. Dolzhikov, Alena F. Douhan, Darina Dvornichenko, Vadym Barskyy, Itay Fischhendler, Verena Murschetz, Jürgen Scheffran, Tobias Baumgartner, 2019 – CHF 49.90/39.90.

Band 202 **Elftes Zürcher Präventionsforum**
Neue Technologien im Dienste der Prävention:
Möglichkeiten – Risiken
Christian Schwarzenegger/Rolf Nägeli (Hrsg.), mit Beiträgen von Ulf Blanke, Ladina Cavelti, Ulrich Schimpel, Jasmine Stössel, Thomas Wenk, Bettina Zahnd, 2020 – CHF 49.90/39.90.

Band 203 **Jahrbuch Wirtschaftsrecht Schweiz – EU**
Überblick und Kommentar 2019/2020
Andreas Kellerhals/Tobias Baumgartner (Hrsg.), mit Beiträgen von Tobias Baumgartner, Mathis Berger, Alexander Brunner, Theodor Bühler, Balthasar Dengler, Jana Fischer, Alfred Früh, Thomas Geiser, Pascal Grolimund, Stefan Härtner, Ulrike I. Heinrich, Isabel Höhener, Samuel Jost, Brigitta Kratz, David Mamane, Laura Manz, Michael Mayer, Urs Meier, Peter Rechsteiner, Antoine Schnegg, René Schreiber, Kurt Sieht, Stefan Sulzer, Wesselina Uebe, 2020 – CHF 49.90.

Band 204 **Kapitalmarkt – Recht und Transaktionen XV**
Thomas U. Reutter/Thomas Werlen (Hrsg.), mit Beiträgen von Marion Bähler, Christina Del Vecchio, Olivier Favre, Jürg Frick, Arie Gerszt, Sonja Maire, Alex Nikitine, Thomas U. Reutter, Annette Weber, 2020 – CHF 39.90.

Band 205 **Verantwortlichkeit im Unternehmensrecht X**
Verantwortlichkeitsprozesse – Tagungsband 2020
Rolf Sethe/Peter R. Isler (Hrsg.), mit Beiträgen von Lukas Fahrländer, Peter Forstmoser, Peter R. Isler, Marcel Küchler, Stephan Mazan, Peter Reichart, Ernst F. Schmid, Rolf Sethe, Martin Waldburger, 2021 – CHF 44.90.

Band 206 **Gewalt gegen Frauen**
Fachtagung Bedrohungsmanagement – Tagungsband 2019
Christian Schwarzenegger, Reinhard Brunner (Hrsg.), mit Beiträgen von Reinhard Brunner, Regina Carstensen, Rosa Maria Martinez, Rahel Ott, Christian Schwarzenegger, Luzia Siegrist, Claudia Wiederkehr, 2021 – CHF 39.90.

Band 207 **Venture Capital Reinvented: Markt, Recht, Steuern**
7. Tagung zu Private Equity – Tagungsband 2020
Dieter Gericke (Hrsg.), mit Beiträgen von Martin Frey, Dieter Gericke, Reto Heuberger, Margrit Marti, Lukas Morscher, Daniel Oehri, Julia Schieber, Lukas Staub, Oliver Triebold, Christian Wenger, 2021 – CHF 44.90.

Band 208 **Die aktienrechtliche Sanierung**
11. Tagung Sanierung und Insolvenz von Unternehmen – Tagungsband 2020
THOMAS SPRECHER (Hrsg.), mit Beiträgen von Marc Bernheim, Sikander von Bhicknapahari, Gaudenz Geiger, Oliver Kälin, Livia Keller, Brigitte Knecht, Giorgio Meier-Mazzucato, Reto Schiltknecht, 2021 – CHF 39.90.

Band 209 **Jahrbuch Wirtschaftsrecht Schweiz – EU**
Überblick und Kommentar 2020/21
ANDREAS KELLERHALS, TOBIAS BAUMGARTNER (Hrsg.), mit Beiträgen von Tobias Baumgartner, André S. Berne, Alexander Brunner, Balthasar Denger, Janick Elsener, Jana Fischer, Thomas Geiser, Ulrike I. Heinrich, Helmut Heiss, Isabel Höhener, Brigitta Kratz, Violeta Kuzmanovic, David Mamane, Michael Mayer, Peter Rechsteiner, René Schreiber, Kurt Siehr, Stefan Sulzer, Wesselina Uebe, Andreas R. Ziegler, Laura P. Zilio, 2021 – CHF 49.90.

Band 210 **Innovation und Disruption: Sanierungen, Exits, LIBOR-Ablösung und Blockchain**
16. Tagung zu Kapitalmarkt – Recht und Transaktionen – Tagungsband 2020
THOMAS U. REUTTER, DR. THOMAS WERLEN (Hrsg.), mit Beiträgen von Sophie Bastardoz, Anna Capaul, Hans-Jakob Diem, Benjamin Leisinger, Daniel Raun, Patrick Schärli, Urs Schenker, Christian Schmid, Cornelia Stengel, Stefan Tränkle, Christoph Vonlanthen, 2021 – CHF 39.90.

Band 211 **Current Challenges of European Integration**
12th Network Europe Conference, 9 – 10 November 2020
TOBIAS BAUMGARTNER, ANDREAS KELLERHALS (Hrsg.), mit Beiträgen von André S. Berne, Jelena Ceranic Perisic, Viorel Cibotaru, Alex de Ruyter, Ivana Kunda, Tobias Lock, Lee McGowan, Peter Christian Müller-Graff, Tatjana Muravska, Attila Vincze, 2021 – CHF 39.90.

Weitere Publikationen und Monografien, erschienen bei EIZ-Publishing, Zürich

Schweiz – Europäische Union
Grundlagen, Bilaterale Abkommen, Autonomer Nachvollzug
Matthias Oesch, 2020 – CHF 44.90.

Ein Plus für die Demokratie
Minimalstandard für die Mitsprache von Parlament und Volk
beim Rahmenabkommen oder bei weiteren Verträgen mit der EU
Thomas Pfisterer, 2021 – CHF 44.90/34.90.

Internet Governance at the Point of No Return
Rolf H. Weber, 2021 – CHF 39.00.

Grundprobleme der Invaliditätsbemessung in der Invalidenversicherung
Philipp Egli, Martina Filippo, Thomas Gächter, Michael E. Meier, 2021 – CHF 54.90/44.90.

Begegnungen
Beiträge von Assistierenden zum 50. Geburtstag von Thomas Gächter
Kerstin Noëlle Vokinger, Matthias Kradolfer, Philipp Egli (Hrsg.), mit Beiträgen von Matthias Appenzeller, Meret Baumann, Petra Betschart-Koller, Brigitte Blum-Schneider, Caroline Brugger Schmidt, Danka Dusek, Philipp Egli, Martina Filippo, Maya Geckeler Hunziker, Kaspar Gerber, Sarah Hack-Leoni, Silvio Hauser, Matthias Kradolfer, Michael E. Meier, Eva Slavik, Jürg Marcel Tiefenthal, Dania Tremp, Thuy Xuan Truong, Dominique Vogt, Kerstin Noëlle Vokinger, 2021 – CHF 49.90/39.90.

«Vielfalt in der Einheit» am Ende?
Jürg Marcel Tiefenthal, 2021 – CHF 54.90.

Kommentar zur Schaffhauser Verwaltungsrechtspflege
Verwaltungsrechtspflegegesetz (VRG) – Justizgesetz (JG)
Kilian Meyer, Oliver Herrmann, Stefan Bilger (Hrsg.), mit Beiträgen von Andreas Baeckert, Cristina Baumgartner-Spahn, Stefan Bilger, Susanne Bollinger, Nina Dajcar, Alfons Fratschöl, Natalie Greh, Nicole Heingärtner, Oliver Herrmann, Natascha Honegger, Basil Hotz, Beat Keller, Arnold Marti, Kilian Meyer, Beatrice Moll, Alexander Rihs, Christian Ritzmann, Patrick Spahn, Beat Sulzberger, Daniel Sutter, Nihat Tektas, Konrad Waldvogel, Dina Weil, 2021 – CHF 79.00/99.00.