Digitaler Verbraucherschutz

4

Dominik Pins, Michelle Walther, Jana Krüger, Gunnar Stevens, Veronika Krauss und Sima Amirkhani

Inhaltsverzeichnis

4.1 Datenschutz ... 137
4.1.1 Entwicklungslinien des Datenschutzes ... 138
4.1.2 Prinzipien des Datenschutzes ... 142
4.1.3 Datenschutz im staatlichen und zivilen Sektor ... 147
4.1.3.1 Staatlicher Sektor ... 148
4.1.3.2 Ziviler Sektor ... 149
4.1.4 Datentreuhänder ... 151
4.1.5 Datenschutztechniken ... 153
4.1.5.1 Verschlüsseln und Anonymisieren ... 153
4.1.5.2 Privacy by Design ... 155
4.1.6 Datenschutzverhalten ... 156
4.1.7 Gebrauchstauglicher Datenschutz ... 163

Ergänzende Information Die elektronische Version dieses Kapitels enthält Zusatzmaterial, auf das über folgenden Link zugegriffen werden kann [https://doi.org/10.1007/978-3-662-68706-2_4].

D. Pins (✉)
Human Centered Engineering & Design, Fraunhofer-Institut für Angewandte Informationstechnik, Sankt Augustin, Deutschland

M. Walther · J. Krüger · G. Stevens
Institut für Verbraucherinformatik, Hochschule Bonn-Rhein-Sieg, Sankt Augustin, Deutschland

V. Krauss · S. Amirkhani
Lehrstuhl Wirtschaftsinformatik, insb. IT-Sicherheit, Universität Siegen, Siegen, Deutschland

© Der/die Autor(en) 2024

A. Boden et al. (Hrsg.), *Verbraucherinformatik*,
https://doi.org/10.1007/978-3-662-68706-2_4

4.2 Verbrauchertäuschung und Onlinebetrug ... 164
4.2.1 Dark Patterns ... 167
4.2.2 Onlinebetrug ... 169
4.3 Social Engineering ... 172
4.3.1 Ziele und Motivation ... 173
4.3.2 Typen und Angriffsformen ... 174
4.3.3 Kommunikationskanäle und -medien ... 175
4.3.4 Manipulationstechniken ... 177
4.3.5 Prozessmodelle ... 178
4.4 Prävention und Resilienz ... 181
4.4.1 Sicherheitsprävention ... 182
4.4.1.1 Verbraucherbildung ... 182
4.4.1.2 Betrugserkennung ... 184
4.4.2 Digitale Resilienz ... 188
4.4.2.1 „Blaming“ und „Shaming“ ... 188
4.4.2.2 Coping-Ansätze ... 190
4.5 Zusammenfassung ... 191
4.6 Übungen ... 191
Literatur ... 192

Die Marktwirtschaft entlastet Verbraucher:innen davon, sich selbst mit Gütern versorgen zu müssen, indem sie ihnen eine Vielzahl von Möglichkeiten bietet, Waren und Dienstleistungen zur Befriedigung ihrer Bedürfnisse zu beziehen. Gleichzeitig birgt dies eine Reihe von Gefahren, vor denen Verbraucher:innen geschützt werden müssen.

Im Laufe der Geschichte haben sich dabei die Schutzbedürftigkeit, wie auch die Schutzmaßnahmen und -gesetze vor dem Hintergrund gesellschaftlicher und technologischer Entwicklungen immer wieder gewandelt. Bereits im Mittelalter gab es erste Bestimmungen zum Schutz der Verbraucher:innen, wie zum Beispiel die Augsburger Stadtordnung aus dem 12. Jahrhundert, welche die Verwendung falscher Maße und Gewichte unter Strafe stellte. Mit zunehmender Industrialisierung wurde die Transparenz von Verbraucherinformationen immer wichtiger. In der Bundesrepublik wurde eine Reihe von Gesetzen und Verordnungen zum Schutz der Verbraucher:innen. Dazu gehört die Fertigpackungsverordnung zur Angabe der Füllmenge, das Textilkennzeichnungsgesetz zur Angabe verarbeiteter Stoffe sowie das Gesetz zu Allgemeinen Geschäftsbedingungen (AGB-Gesetz), das eingeführt wurde, um Verbraucher:innen vor einseitigen Klauseln im „Kleingedruckten“ von Verträgen zu schützen.

Durch den fortschreitenden digitalen Wandel ergeben sich neue Herausforderungen für den Verbraucherschutz, die angegangen werden müssen. Dazu gehören Fragen der Datensicherheit und des Datenschutzes. Sollte der Datenschutz zunächst Bürger:innen vor dem Datenmissbrauch staatlicher Stellen schützen, so ist es heute ebenso wichtig, Verbraucher:innen die Kontrolle über ihre persönlichen Informationen im zivilen Sektor zu ermöglichen. So hinterlassen Verbraucher:innen Spuren in vielen Lebensbereichen, insbesondere im digitalen Raum. Daten sammelnde Dienste und Geräte, vor allem Smartphones, dringen immer tiefer in private Bereiche wie das Zuhause vor, das als Symbol der Privatsphäre gilt. Hierdurch steigt das Risiko, dass ihre Daten durch kommerzielle Unter-

nehmen ausgebeutet und verwertet werden. Darüber hinaus können sensible Daten in die Hände von Kriminellen gelangen, was die Cyberkriminalität im Internet zu einem bedeutenden Problem macht.

Mit der Digitalisierung sind zudem neue Risiken der Verbrauchertäuschung und des Onlinebetrugs verbunden, da Waren und Dienstleistungen nicht mehr auf sinnliche Weise erfahrbar und physisch erlebbar sind und digitale Transaktionen und Interaktionen zunehmend im digitalen Raum stattfinden. Dies schafft neue Möglichkeiten für Täuschung und betrügerische Praktiken, gegen die Verbraucher geschützt werden müssen. Hierbei ist der Übergang zwischen Verbrauchermanipulation, Verbrauchertäuschung, Onlinebetrug und Cyberkriminalität fließend. Der Verbraucherschutz bleibt somit ein sich wandelndes und entscheidendes Anliegen, um die Rechte und Interessen der Verbraucher:innen in einer sich ständig verändernden digitalen Welt zu schützen. So schreibt z. B. das *BMUV* auf seiner Webseite: „Es gehört daher zu den Aufgaben des digitalen Verbraucherschutzes im BMUV, Fairness, Wahlfreiheit, Transparenz und die Rechte der Verbraucherinnen und Verbraucher in der digitalen Welt zu stärken“ (BMUV 2023).

Als eine Einführung in den digitalen Verbraucherschutz gibt das Kapitel ein Überblick über den Datenschutz sowie verschiedene Arten von Verbrauchermanipulation und Onlinebetrug. Insbesondere wird das Social Engineering als häufigste Methode zur Verbrauchermanipulation im digitalen Raum beleuchtet.

Lernziele

Im Rahmen dieses Kapitels werden Ihnen folgende Inhalte vermittelt:

- Sie lernen die wichtigen Konzepte des Datenschutzes kennen.
- Sie lernen verschiedene Modelle zur Privatsphäre und des Datenschutzverhaltens sowie Gestaltungsprinzipien zur Umsetzung eines verbraucherfreundlichen Datenschutzes kennen.
- Sie lernen, was Cyberkriminalität, Onlinebetrug und Social Engineering sind und dass verschiedene Arten von Betrug verschiedene Problemlösungen brauchen.
- Sie lernen, dass der Fokus bei Cybersicherheit auf dem Menschen als dem schwächsten Glied liegt, welche Sicherheitsverhaltensweisen von Verbraucher:innen existieren, welche Copingmechanismen Opfer nutzen, was zu digitaler Resilienz dazugehört, welche Präventionsmaßnahmen es gibt und welche Maßnahmen zum Erkennen von Onlinebetrug existieren.

4.1 Datenschutz

Ein wesentlicher Aspekt des digitalen Verbraucherschutzes liegt im Schutz personenbezogener Daten zur Wahrung der Privatsphäre von Verbraucher:innen.

Privatsphäre versteht sich im Allgemeinen als Ort oder Zustand, an bzw. in dem der Mensch sich und sein Verhalten vor anderen Akteuren (wie Personen, Regierungen oder Unternehmen) abschirmen kann. Insbesondere Arbeiten aus den Sozial- und Rechtswissenschaften machen jedoch deutlich, dass der Begriff durchaus verschiedene Bedeutungen und Nuancen aufweist. Während sich das allgemeine Verständnis zunächst auch in vielen theoretischen Konstrukten wiederfindet (Habermas 2015; Rössler 2001; Warren und Brandeis 1890; Westin 2015), nehmen diese bei genauerer Betrachtung jedoch unterschiedliche Aspekte in den Fokus. So lässt sich der Begriff der Privatheit aus soziologischer Perspektive als Gegenpol zum Begriff Öffentlichkeit oder öffentlicher Raum abgrenzen und definiert somit Lebens- und Tätigkeitsbereiche wie das Familienleben, Freizeitaktivitäten und insbesondere das Zuhause als allgemeingültiger Bereich des privaten Lebens (Fuchs-Heinritz 2013). Neben einer räumlichen Perspektive gibt es zudem eine dezisionale sowie eine informationelle Verständnisweise von Privatheit (Rössler 2001). Erstere adressiert die Sicherung von Entscheidungs- und Handlungsspielräumen bzw. den Schutz vor Fremdbestimmung, während Letztere beim digitalen Verbraucherschutz eine wichtige Rolle spielt, weshalb sie im Folgenden näher erläutert werden soll.

Unter informationeller Privatsphäre versteht man den Anspruch auf Schutz von persönlichen Daten (Rössler 2001) und die Kontrollmöglichkeit für Individuen, Zeitpunkt, Art und Umfang, in dem persönliche Informationen mit anderen ausgetauscht und von anderen genutzt werden, zu bestimmen (Li et al. 2010). Sie stehen in enger Verbindung mit der räumlichen (oder auch physischen) Privatheit, da durch die Durchdringung digitaler Medien und Internet-of-Things(IoT)-Geräten sehr viele Daten aus dem persönlichen Umfeld von Verbraucher:innen erfasst werden können (Westin 2015). Wenn jemand persönliche Informationen offenlegt, indem er auf einer Webseite ein Nutzerkonto eröffnet oder Urlaubsfotos teilt, könnten diese Informationen an Dritte weitergeleitet werden. Die Datenverwendung und -verbreitung liegt dann außerhalb des Einflussbereichs der Nutzer:innen.

Außer in den Sozialwissenschaften ist die Privatsphäre auch in den Rechtswissenschaften ein wichtiger und festgeschriebener Begriff. Auch hier herrscht die Bedeutung vor, dass jener familiär-häusliche Bereich den Gegenpol zur Öffentlichkeit darstellt, ohne die Einwilligung der betreffenden Person anderen nicht zugänglich ist und ihr in diesem Bereich das Recht auf freie Entfaltung der Persönlichkeit einräumt. Dies ist insbesondere durch Artikel 2 Absatz 1 GG, dem Recht auf freie Entfaltung, sowie Artikel 13 GG „Unverletzlichkeit der Wohnung“ und Artikel 10 GG „Post- und Fernmeldegeheimnis“ geregelt, die zusätzlich den Schutzbereich für Privatsphäre festlegen.

4.1.1 Entwicklungslinien des Datenschutzes

Das moderne Verständnis des Datenschutzes ist durch den technologischen Fortschritt im Bereich der Datenverarbeitung geprägt. Während sich historisch seit der Antike vor allem die räumliche Abgrenzung zwischen privatem und öffentlichem Bereich als Definition ab-

zeichnet (Habermas 2015), entwickelt sich seit Ende des 19. Jahrhunderts und insbesondere durch die rasante Entwicklung von Medientechnologien (allen voran die kompakter werdenden und schneller verarbeitenden Geräte in der Fotografie) auch eine Betrachtung von informationeller Privatheit immer mehr ab (Warren und Brandeis 1890; Westin 2015). Dies begann einerseits mit der Möglichkeit, von nun an Fotos von anderen Personen (und potenziell ohne deren Wissen) schneller und unkomplizierter aufzunehmen und zu verbreiten (Warren und Brandeis 1890). Andererseits vereinfachten auch die kompakteren technischen Möglichkeiten seit den 1950ern, bspw. die Erfindung der Kreditkarte, die Erfassung und Speicherung von Daten (Westin 2015). Während Westin in den 1970ern dadurch vorwiegend eine steigende Überwachung durch Behörden und Regierungen prophezeite, die zu einer Bedrohung des Individuums und seiner Privatsphäre führen würde, zeigt sich heute, dass vor allem wirtschaftliche Akteur:innen Daten – insbesondere die personenbezogenen ihrer Kund:innen – für ihre Geschäftsmodelle nutzen (Masur et al. 2018).

Mit vermehrtem Aufkommen der Erhebung von Daten zur Überwachung der Bürger:innen durch den Staat (Westin 2015) wurden auch die Stimmen seitens der Verbraucher:innen laut, in Deutschland spätestens im Zuge der geplanten Volkszählung 1983 (Wiesner 2021). Daraus folgte eine kritische Auseinandersetzung mit Privatheit, woraufhin das Bundesverfassungsgericht schließlich urteilte, dass eine solche systematische Befragung gegen das Grundgesetz verstößt, und folglich den Bürger:innen das Recht auf informationelle Selbstbestimmung einräumte (Masur et al. 2018).

In den Anfangstagen der elektronischen Datensammlung gab es kaum Regeln, Gesetze und Vorschriften zum Schutz der informationellen Privatsphäre. Die Regierung mitsamt ihren Behörden und vor allem die später gegründeten digitalen Unternehmen konnten personenbezogene Daten weitgehend uneingeschränkt erheben, sammeln und verarbeiten. Erst mit der Zeit wurde die Bevölkerung durch Aktivitäten von Initiativen wie dem Chaos Computer Club sensibilisiert, und es bildeten sich gesetzliche Vorschriften und Organisationen wie die Datenschutzaufsicht heraus, um sicherzustellen, dass staatliche Stellen und Unternehmen die Privatsphäre ihrer Kund:innen und Bürger:innen respektieren und die Datenschutzregeln einhalten (Rost 2013). Doch selbst heute noch gelingt es Unternehmen, massenhaft personenbezogene Daten zu sammeln, um sie für eigene Zwecke zu verwenden und wirtschaftlich zu vermarkten (Rost 2013).

In den 1950ern ging man in den Rechtswissenschaften insbesondere von der Sphärentheorie aus, die im Kern zwischen drei Sphären unterscheidet (Witt 2010):

Intimsphäre. Dies ist der innerste und am stärksten geschützte Bereich der Persönlichkeit. Hierzu gehören private Gedanken, Emotionen und persönliche Lebensentscheidungen. Der Intimbereich wird als „unantastbarer Kernbereich privater Lebensgestaltung“ aufgefasst und unterliegt einem besonders hohen Schutz vor Eingriffen.

Privatsphäre. Die Privatsphäre umfasst persönliche Angelegenheiten, die nicht unmittelbar den Intimbereich betreffen, aber dennoch einen hohen Schutz vor Eingriffen genießen. Hierzu gehören beispielsweise die familiären Beziehungen, die Wohnung, die Kommunikation und persönliche Daten.

Individualsphäre (auch als Sozialsphäre oder Öffentlichkeitssphäre bezeichnet). Dies ist der äußerste Bereich der Persönlichkeit; er umfasst Aktivitäten und Handlungen in der Öffentlichkeit. In diesem Bereich sind Eingriffe und Regulierungen am wenigsten stark ausgeprägt, da sie weniger stark in die individuelle Freiheit eingreifen.

Dieses Verständnis erweist sich jedoch zunehmend als ungeeignet, die informationelle Selbstbestimmung im digitalen Zeitalter zu schützen. So werden Chatbots private Gedanken anvertraut oder in Cloud-basierten Diensten gespeichert; die elektronische Bildverarbeitung ermöglicht es, Emotionen auf Fotos und Videoübertragungen zu erkennen; oder durch das Smart Home werden familiäre Beziehungen und häusliche Kommunikation digital aufgezeichnet. Da die Sphären zunehmend ineinanderfließen und überlappen, ergeben sich neue Herausforderungen, bspw. in Bezug auf die Frage, wie der Kernbereich privater Lebensgestaltung sowohl vor staatlicher Kontrolle als auch vor kommerzieller Verwertung geschützt werden kann (vgl. Abb. 4.1).

Ein weiterer Aspekt betrifft die Frage, wie die Einhaltung gesetzlicher Vorschriften kontrolliert werden kann. Das Feld der Datenschutzaufsicht hat sich z. B. seit den 2000ern weiterentwickelt, sodass sich Datenschützer:innen zunehmend auch in Berater:innen- und Auditor:innen-Tätigkeiten wiederfinden. Eine weitere Verschiebung in der Perspektive des Datenschutzfokus fand auch durch die sich verbreitende Verfügbarkeit von Heim-PCs und weiteren (vernetzten) Endgeräten sowie den damit genutzten Programmen und Services (Online-Einkaufen, -Banking etc.) statt, die dazu führten, dass auch die Abwehr von Angriffen im Privaten auf die darauf enthaltenen Datenbestände, die bisher in den Bereich der Datensicherheit fallen, ebenfalls durch die Datenschutzaufsicht untersucht werden (Rost 2013).

Die stetige Verbreitung mobiler Endgeräte in der Gesellschaft und die Digitalisierung von Alltagspraktiken und Hobbys, wie das Lesen von Büchern, Urlaubsreisen, Kochen oder Freizeit mit Freund:innen, führen schließlich dazu, dass Verbraucher:innen bewusst und unbewusst Datenspuren hinterlassen. Diese lassen Rückschlüsse auf ihre Person und ihr Verhalten zu und geben damit Einblicke in ihre Privatsphäre, sei dies gewollt oder nicht. Dass zum Beispiel über soziale Medien wie Facebook, Instagram oder TikTok Nachrichten, Bilder und Videos mit entsprechenden Meta-Daten (Aufenthaltsort, Gerätedaten etc.) geteilt werden, ist weithin bekannt und sollte Nutzer:innen weitestgehend bewusst sein.

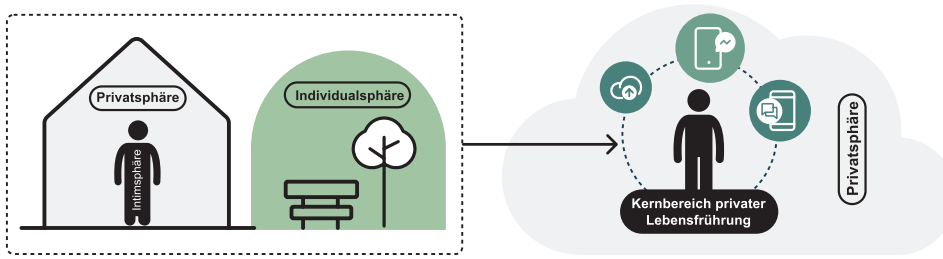


Abb. 4.1 Durch die digitale Auflösung der Sphären ergeben sich neue Herausforderungen um Kernbereiche privater Lebensgestaltung zu schützen

Alex Kuhn zeigt am Beispiel eines E-Readers, welche Rückschlüsse durch das digitale Lesen möglich werden, die mit dem lauten (Vor-)Lesen eines Buches vergleichbar sind (Kuhn 2019). Durch Reader-Analytics können neben den Interessen und Genres somit Nutzer:innen-Informationen darüber gewonnen werden, wann und wie häufig das Gerät (oder die App) zum Lesen genutzt wird, an welchen Stellen unterbrochen wird, ob Abschnitte gar übersprungen werden und welche Textstellen ggf. markiert werden. Diese können dann für Nutzungsmuster, Ableitung von Leser:innentypen, Themen/Genretrends sowie als Qualitätsindikatoren von (neuen) Autor:innen ausgewertet werden (Kuhn 2019).

Das moderne Verständnis des Datenschutzes ist dabei als Individualrecht konzipiert. Während Verbraucher:innen bei der Erfassung von personenbezogenen Daten im privaten Bereich direkte Kontrolle darüber ausüben können, welche Daten gesammelt und verarbeitet werden und somit unmittelbarer Verbraucherschutz gegeben ist, erweist sich der Schutz von Daten im öffentlichen Raum sowohl technisch als auch konzeptionell schwieriger. Hierunter fallen beispielsweise Sprachaufnahmen von Haushaltsmitgliedern oder Besucher:innen bei Verwendung von Sprachassistenten, aber auch die Veröffentlichung von Bildern, auf denen eine Person ungewollt oder unbemerkt fotografiert wurde, in den sozialen Medien. Dieser Konflikt ist auch als **Multi-Party-Privacy-Konflikt** bekannt (Salehzadeh Niksirat et al. 2021; Such und Criado 2018).

In Smart-Home-Haushalten gibt es häufig eine:n Administrator:in, der:die die entsprechenden Geräte einrichtet und verwaltet und somit auch die Nutzung durch alle Personen einsehen kann (Pins et al. 2020; Geeng und Roesner 2019) – und dies, obwohl andere Haushaltsmitglieder sich selbst trotz weniger Zugriffsrechte oder -möglichkeiten als Eigentümer der Geräte betrachten (Meng et al. 2021). Dadurch kann ein Machtgefälle innerhalb von Haushalten (oder Familien) entstehen, das durch geteilte Geräte oder offene Zugänge noch verstärkt wird (Geeng und Roesner 2019). Neben einer individuellen Selbstbestimmung sollte hierbei also auch eine kollektive Form der informationellen Selbststimmung in den Zugriffsmöglichkeiten berücksichtigt werden, bei der Betroffene mitbestimmen können, wer diese Daten für welche Zwecke nutzen darf (Stevens und Boden 2022).

Auf öffentlichen Plätzen, in öffentlichen Gebäuden, aber oftmals auch in privaten Haushalten wird darauf hingewiesen, dass Bereiche videoüberwacht werden. Weiterhin müssen bei öffentlichen Veranstaltungen die Besucher:innen und Teilnehmer:innen in der Regel im Vorfeld darin einwilligen, dass Fotos und Videoaufnahmen während der Veranstaltung gemacht und später veröffentlicht werden dürfen, auf denen sie ggf. zu erkennen sind.

Das Kunsturhebergesetz (KUG) § 22 (KunstUrhG 1907) regelt mit dem Recht am eigenen Bild in § 22, dass eine Einwilligung des Abgebildeten erforderlich ist, wenn das Bildnis veröffentlicht werden soll (Mause 2019). Ausnahmen davon sind in § 23 festgehalten, die sich beispielsweise auf Fotos beziehen, bei denen die Personen lediglich als „Beiwerk“ erscheinen, wie bspw. auf Fotos mit Sehenswürdigkeiten („Panoramafreiheit“) oder auf Versammlungen (KunstUrhG 1907). Diese Ausnahmen gelten jedoch nur, solange ein berechtigtes Interesse der abgebildeten Person nicht verletzt wird. Kommt es hier zu einer Verletzung, sind die strafrechtlichen Folgen in den § 33 ff. KUG geregelt.

Bei der Kenntnisnahme von Hinweisen in überwachten Bereichen oder der Einwilligung in die Erstellung und Veröffentlichung von Bildern und Videoaufnahmen kommt es im Sinne der informationellen Selbstbestimmung darauf an, ob hierbei alle wichtigen Informationen (z. B. Zweck der Datensammlung oder Aufnahme) sichtbar und in zumutbarer Weise vermittelt wurden, um Verbraucher:innen in ihrem freiwilligen und selbstbestimmten Handeln, den Bereich betreten zu wollen, zu stärken (Aldenhoff 2019).

Bei der Grenzziehung zur Wahrung von digitaler Privatsphäre lässt sich abschließend ein ständiges Wechselspiel aus Machtverhältnissen feststellen, bei dem jedoch häufig eine Asymmetrie zu Lasten der Verbraucher:innen vorliegt. Dies liegt zum einen daran, dass Unternehmen über mehr Ressourcen verfügen, um Lobbyarbeit zu betreiben und um Gesetze zu beeinflussen. Zudem sind sie in der Lage, komplexe Technologien und Praktiken zum Sammeln und Verwenden von Daten zu entwickeln und zu nutzen. Insbesondere herrscht eine Informationsasymmetrie, weil Unternehmen einen besseren Überblick darüber haben, welche Daten erhoben und wofür diese genutzt werden. Demgegenüber haben Verbraucher:innen oft begrenzte Ressourcen und eine geringere technische Expertise. Sie sind meist nicht in der Lage, die Auswirkungen von Datenpraktiken in vollem Umfang zu verstehen oder sich wirksam dagegen zu verteidigen. Ferner werden die Nutzungs- und Vertragsbedingungen meist durch die Unternehmen einseitig vorgegeben und Verbraucher:innen teilweise durch undurchsichtige Dialoggestaltung zu einer Einwilligung gedrängt.

Die Ausgestaltung von personenbezogenen Verfahren (auch zur Abwälzung von Risiken) macht mithin fraglich, inwiefern Verbraucher:innen Handlungsalternativen geboten bekommen und überhaupt selbstbestimmt handeln können (Rost 2013). Selbstbestimmung seitens der Verbraucher:innen ist nur insoweit gegeben, als er:sie entscheiden kann, ob er:sie der Datennutzung zustimmt oder nicht. Die Art der Datennutzung kann dabei aber nur selten ausgehandelt werden, sondern lediglich, ob man den Service nutzen möchte oder nicht (Aldenhoff 2019).

Gemäß der Idee der informationellen Selbstbestimmung muss eine Einwilligung aber immer freiwillig erfolgen und Kontrollmöglichkeiten für Verbraucher:innen mit sich bringen, damit Datenschutz möglich ist. Das Teilen von Inhalten in den sozialen Medien oder von Informationen beim digitalen Lesen als Eingriff in die Privatsphäre ist abschließend nie absolut bzw. als unvermeidbar zu verstehen, sondern obliegt den Nutzer:innen und ihren Handlungen, ob bzw. auf welche Art und Weise sie Produkte und Dienste nutzen.

4.1.2 Prinzipien des Datenschutzes

In der Europäischen Union basiert der Datenschutz auf grundlegenden Prinzipien, die vor allem aus den Vorgaben abgeleitet werden können, die in der **DSGVO** (Datenschutz-Grundverordnung) festgeschrieben sind. Die DSGVO, auch bekannt als GDPR (General Data Protection Regulation), ist am 25. Mai 2018 in Kraft getreten. Ihr Hauptziel ist es, die informationelle Selbstbestimmung der Bürger:innen in der EU zu stärken und zu regulieren, wann und wie personenbezogene Daten gesammelt, verarbeitet und gespeichert werden dürfen.

Die Regulierung bezieht sich nicht auf alle Daten, sondern speziell auf personenbezogene Daten. Laut Artikel 4 DSGVO sind personenbezogene Daten demnach

> [...] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
>
> Artikel 4 (1), DSGVO (Auszug)

Einige der grundlegenden Eckpfeiler des Datenschutzes werden durch die folgenden Kernprinzipien dargestellt (Witt 2010):

- **Informationelle Selbstbestimmung.** Die informationelle Selbstbestimmung ist das Recht einer Person, selbst zu entscheiden, welche persönlichen Informationen über sie erfasst, verarbeitet, gespeichert und weitergegeben werden dürfen. Sie betont die individuelle Kontrolle über die eigenen persönlichen Daten. Danach dürfen Unternehmen und Organisationen persönliche Daten grundsätzlich nur dann sammeln und verwenden, wenn sie hierfür die ausdrückliche Zustimmung der betroffenen Person erhalten haben.
- **Prinzip des Verbots mit Erlaubnisvorbehalt.** Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten ist im Grundsatz verboten. Dieses Verbot kann aufgehoben werden, wenn eine gesetzliche Grundlage bzw. ausdrückliche Genehmigung vorliegt. Eine solche liegt z. B. bei der freiwilligen Einwilligung durch den Betroffenen vor. Hierbei ist die verarbeitende Stelle dafür verantwortlich sicherzustellen, dass die Einwilligung ordnungsgemäß eingeholt und dokumentiert wird. Die Einwilligung muss freiwillig und informiert erfolgen und darf jederzeit widerrufen werden. Die Einwilligung darf nur auf konkrete, vorab spezifizierte Verarbeitungszwecke bezogen sein.
- **Prinzip der Transparenz.** Personenbezogene Daten müssen auf rechtmäßige Weise, fair und transparent verarbeitet werden. Die betroffene Person muss über die Datenverarbeitung informiert sein. Hierbei sollten die Betroffenen die Möglichkeit haben, die Verarbeitung ihrer Daten nachzuverfolgen. Dies bedeutet, dass sie Informationen darüber erhalten sollten, wann und wie ihre Daten verwendet werden und wer Zugriff auf sie hat.
- **Prinzip der Zweckbindung.** Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden. Die Daten dürfen nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist. Die Zweckbindung fördert die informationelle Selbstbestimmung, indem sie sicherstellt, dass die betroffene Person darüber informiert ist, wozu ihre Daten verwendet werden. Dies ermöglicht es der Person, die Tragweite ihrer Einwilligung besser zu verstehen und fundierte Entscheidungen über die Verwendung ihrer Daten zu treffen.

- **Prinzip der Datensparsamkeit.** Es dürfen nur die Daten erhoben werden, die für die Zwecke, für die sie verarbeitet werden, erforderlich sind. Die Daten müssen auf das notwendige Minimum beschränkt sein. Ferner dürfen Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- **Prinzip der korrekten, sicheren Aufbewahrung.** Die Daten müssen korrekt und auf dem neuesten Stand sein. Angemessene Maßnahmen müssen ergriffen werden, um unrichtige oder unvollständige Daten zu korrigieren oder zu löschen. Ferner müssen geeignete technische und organisatorische Maßnahmen ergriffen werden, um die Daten vor unbefugtem Zugriff zu schützen.

  Ein erhöhter Schutzbedarf besteht bei Daten, die als besonders sensibel eingestuft werden und Auskunft über weltanschauliche Überzeugungen, genetische Merkmale oder das Sexualleben einer Person geben.

Die Regelungen zum Datenschutz stärken ferner die Rechte von Verbraucher:innen, Kontrolle über die Datenverarbeitung auszuüben. Hierzu gehören insbesondere folgende Verbraucherrechte:

- **Recht auf Auskunft.** Betroffene haben das Recht, von der verantwortlichen Stelle Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten. Diese Informationen sollten in einer klaren und einfachen Sprache bereitgestellt werden.
- **Recht auf Löschung und Korrektur.** Betroffene haben das Recht auf Berichtigung, Löschung und Datenübertragbarkeit. Sie können Daten löschen bzw. unvollständige oder unrichtige Daten korrigieren lassen.
- **Recht auf Datenübertragbarkeit.** Betroffene haben das Recht, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, um sie an eine andere Organisation zu übertragen.
- **Recht zum Widerspruch gegenüber automatisierter Entscheidung**. Betroffene haben das Recht, gegen automatisierte Entscheidungen, einschließlich Profiling, Widerspruch einzulegen. Dieses Recht ermöglicht es den Personen, menschliche Intervention in automatisierte Entscheidungen zu verlangen.

Die Schutz- und Abwehrrechte der DSGVO sind sehr allgemein gefasst und weisen einen Interpretationsspielraum auf, wenn es um die Umsetzung geht. Insbesondere steht die DSGVO im Spannungsfeld, dass einerseits die Innovationsfähigkeit der Organisationen gewahrt bzw. gefördert und damit die Umsetzung möglichst offengehalten wird. Andererseits erschwert dies die Prüfung, ob die Rechte eingehalten werden (z. B. hinsichtlich der Vollständigkeit von Informationen) oder wie Meldeverfahren zu gestalten sind, die sowohl der DSGVO als auch der Forderung der Verbraucher:innen nach Schutz der Privatsphäre Rechnung tragen (z. B. im Hinblick auf Transparenz) (Pins et al. 2022).

Ein Beispiel hierfür stellt das Prinzip der Zweckbindung dar. So schreibt die DSGVO vor, dass Daten nur für „festgelegte, eindeutige und legitime“ (Artikel 5 DSGVO) Zwecke genutzt werden dürfen. Diese Zwecke müssen dabei im Vorfeld kommuniziert werden.

Studien zum verbraucherfreundlichen Datenschutz zeigen jedoch, dass die Formulierungen zur Zweckbindung in der Praxis oftmals noch vage oder aber sehr komplex gehalten sind (Alizadeh et al. 2019; Jakobi et al. 2020) und eine effektive informationelle Selbstbestimmung hierdurch nicht möglich ist (Jakobi et al. 2020).

Ein anderes Beispiel stellt das Recht auf Datenübertragbarkeit nach Artikel 20 dar. Demnach soll ein Datenexport es den Benutzer:innen ermöglichen, alle ihre Daten herunterzuladen und sie gegebenenfalls bei einer anderen Organisation zu importieren oder einfach als persönliche Sicherungskopie aufzubewahren. Jedoch sind in der Regel die maschinenlesbaren Formate von Organisation zu Organisation sehr unterschiedlich strukturiert (Cena et al. 2016), was eine generelle Verknüpfung von Daten unterschiedlicher Hersteller erschwert (Pins et al. 2021; Cena et al. 2016). Abb. 4.2 zeigt z. B., dass die Anbieter zweier Sprachassistenzsysteme die Daten im JSON-Format bzw. im CSV-Format bereitstellen. Bei der Anforderung einer Kopie der Daten kommt noch hinzu, dass die maschinenlesbaren Formate aus Laiensicht nur schwer verständlich sind (Pins et al. 2021).

```
1  // Type some code ->
2
3  "header": "Voice Assistant",
4  "title": "Spiel bitte Bayern gesagt",
5   "titleUrl": "https://www.searchengine.com /search?q\u003dSpiel+bitte+Bayern",
6    "subtitles": [{
7    "name": "Alles klar, ich spiele Bayern von Musikdienst ab."
8  }],
9
10 "time": "2020-07-06T11:27:17.214Z",
11 "products": ["Voice Assistant"],
12   "locationInfos": [{
13   "name": "Ungefähre Gegend",
14   "url": "https://www.gpsdata.com/@?api\XYZ ",
15   "source": "Von meinem Gerät"
16 }]
17 },{
18
19 "header": "Voice Assistant",
20 "title": "rufe Hans Meier an gesagt",
21 "titleUrl": "https://www.searchengine.com/search?q\u003drufe+Hans+Meier+an",
22 "time": "2020-07-06T13:59:50.154Z",
23 "audioFiles": ["2019-12-27_13_59_51_393_UTC.mp3"],
24 "products": ["Voice Assistant"],
25 "details": [{
26   "name": "Per Hotword gestartet"
27 }],
28
29 "locationInfos": [{
30   "name": "Ungefähre Gegend",
31   "url": "https://www.gpsdata.com/@?api\XYZ",
32   "source": "Von meinem Gerät"
```

```
22 2019-02-03T11:45:33.269Z, VA spiele that's life,3b09c69b2280a6eeec108dfbb2073cb75002adfe.wav,"Hier ist That's Life von Andr
23 2020-08-14T12:42:10.449Z," wohin ist der mond",9f5accea8c590df9314380574a5d7085a1925cc0.wav,Möchtest du die Wegbeschreibung z
24 2019-05-10T17:56:25.358Z,VA setze einen timer auf eine stunde drei und vierzig minuten und nenne ihn spätzle aufsetzen, 17fe8
25 Data Not Available,Data Not Available,1761b3c40d150866499b30d8d7edc4983f3baed1.wav,Not Applicable
26 2019-05-03T10:16:46.314Z, VA zurück,83a0f71377371fb7e846db7827e8af891a17ea4e.wav,Ich habe momentan Schwierigkeiten auf deine
27 2020-11-04T07:44:21.287Z,VA wiedergabe stoppen,ca81c10e4ea9c6e030056b83d8e0d30072393ad5.wav,Not Applicable
28 2020-11-08T13:31:49.528Z,VA spiel Radio,782bdc2e0b4d9dd3b8c10564bfec17e85c23da2c.wav,Radio aus der Audiothek.
29 Data Not Available,Data Not Available,0e061291faed7c71d25392c57b2c42173216a7ed.wav,Was möchtest du nun tun?
30 2020-11-17T15:20:29.466Z,VA wiedergabestopp,9cfb880ebd1b09a33b03a9dd63320fc9ce297a6c.wav,Not Applicable
31 2019-05-07T19:17:33.884Z,VA zeige mir rezepte mit spätzle,c00d31432e105247017e6fe9cb6a22486fdc148d.wav,"Mit spätzle könntest
```

Abb. 4.2 Formate für Sprachassistenten-Nutzungsdaten

Datenauskunft bei Sprachassistenten

Im Forschungsprojekt *CheckMyVA* wurde eine Browser-Erweiterung entwickelt, die Verbraucher:innen darin unterstützen soll, ihre (Interaktions-)Daten mit Sprachassistenten beim Hersteller anzufordern und mittels Datenvisualisierung zu verstehen, da die erhaltenen Rohdaten für Laien schwer zu verstehen waren (Abb. 4.2).

Hieran ist zu erkennen, dass Unternehmen unterschiedliche Speicherformate verwenden und ein schnelles Verstehen der Datenstruktur und ihrer inhaltlichen Bedeutung schwer möglich ist. Durch ein zusätzlich entwickeltes Dashboard werden diese Daten visuell aufbereitet, sodass Nutzende erste Muster des eigenen Verhaltens erkennen und ableiten können. Die untenstehende Abbildung zeigt dazu Ausschnitte eines Tools zur Visualisierung der Interaktionsdaten mit einem Sprachassistenten. Dieses beinhaltet unter anderem einen Zeitstrahl auf dem die einzelnen Interaktionspunkte abgebildet werden (links).

Nutzende haben dabei die Möglichkeit, auf der Basis der verwendeten Begriffe individuelle Kategorien zu bilden, die sich durch Farbkodierungen voneinander unterscheiden lassen (z. B. umfasst die Kategorie „Musik“ Begriffe wie „Playlist“, „Lied“, „spiele“ etc.). Zu jedem Datenpunkt erscheint zudem ein Infofenster, wenn Nutzende mit der Maus darüberfahren (siehe Abb. rechts oben). Weitere Elemente des Dashboards sind u. a. eine Liste mit verwendeten Begriffen und Befehlen der Nutzenden, einer Häufigkeitsverteilung der unterschiedlichen Kategorien, die Häufigkeit der Verwendung eines Geräts (siehe Abb. rechts unten) oder auch eine Heatmap, die anzeigt, an welchen Tagen und zu welcher Uhrzeit typischerweise ein Befehl verwendet wird.

Über die Projektwebseite (https://checkmyva.de/) kann die Browser-Erweiterung heruntergeladen und genutzt werden.

4.1.3 Datenschutz im staatlichen und zivilen Sektor

In modernen Gesellschaften werden personenbezogene Daten in verschiedenen Bereichen erhoben, in denen Menschen verschiedene Rollen einnehmen und in verschiedenen Abhängigkeitsverhältnissen stehen, die sich auf die informationelle Selbstbestimmung auswirken (siehe Abb. 4.3).

Hinsichtlich des Datenschutzes sind dies insbesondere der staatliche, der betriebliche und der kommerzielle Sektor, in denen der:die Einzelne jeweils in seiner:ihrer Rolle als Bürger:in, Arbeitnehmer:in und als Verbraucher:in in Erscheinung tritt.

Beim staatlichen Sektor besteht zwischen dem Staat und dem Bürger eine hierarchische Beziehung, bei der sich der Einzelne an die herrschenden Gesetze halten muss (z. B. besteht eine Meldepflicht sowie die Pflicht zur Steuererklärung). In einer liberalen Demokratie sind Bürger:innen mit einer Reihe von Rechten gegenüber dem Staat ausgestattet, wie z. B. mit dem Recht auf politische Partizipation durch Wahlen und Meinungsäußerung. Hierzu gehören sowohl Abwehrrechte von staatlicher Willkür als auch das Recht auf informationelle Selbstbestimmung und Datenschutz.

Im zivilen Bereich herrscht keine hierarchische Beziehung vor, sondern die Beziehung ist vom Prinzip der Vertragsfreiheit geprägt. In seiner:ihrer Rolle als Arbeitnehmer:in, Kund:in oder sonstigem:r Vertragspartner:in ist die Person dem Gegenüber gleichgestellt. Jedoch sind faktisch die Beziehungen durch Macht- und Informationsasymmetrien geprägt, aus denen sich spezielle Schutzbedürfnisse und Schutzrechte ergeben. So strahlen insbesondere die Rechte zum Schutz der informationellen Selbstbestimmung im staatlichen Bereich auch auf die privatrechtlich geregelten Beziehungen aus (Witt 2010).

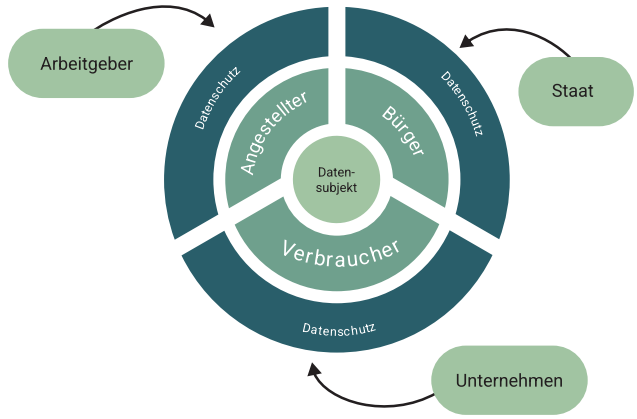


Abb. 4.3 Bereiche des Datenschutzes

4.1.3.1 Staatlicher Sektor

Im Rahmen der Erfüllung seiner staatlichen Aufgaben der Verwaltung und dem Schutz seiner Bürger:innen erhebt und verarbeitet der Staat eine breite Reihe von personenbezogenen Daten, darunter Informationen aus Melderegistern, Steuerdaten, aber auch aus der Überwachung von Orten und der Erhebung von Daten zur Kriminalitäts- und Terrorbekämpfung (Wiesner 2021). Aufgrund der historischen Erfahrungen aus der Nazi-Ära und der DDR war man in Deutschland schon früh für die Gefahr missbräuchlicher staatlicher Datennutzung sensibilisiert. Im digitalen Zeitalter wurde spätestens seit der NSA-Affäre im Jahr 2013 die breite Öffentlichkeit über die Gefahren staatlicher Überwachung informiert. Durch den Whistleblower Edward Snowden wurde bekannt, dass staatliche Behörden weltweit die elektronische Kommunikation überwachen und dies mit dem Schutz vor Angriffen und Terror begründen (Mause 2019). In liberalen Demokratien wird seit Langem darüber debattiert, wie die Rolle des Staates im Bereich des Datenschutzes gestaltet sein sollte und inwieweit er in die verschiedenen gesellschaftlichen Bereiche eingreifen darf. Dies geschieht vor dem Hintergrund der Auffassung, dass Privatsphäre buchstäblich als individuelle Privatsache betrachtet wird (Mause 2019).

In Deutschland gibt es immer wieder Bestrebungen, eine Vorratsdatenspeicherung durchzusetzen, bei der alle Telekommunikationsvorgänge (Telefon-, Handy-, und Internetverbindungen) vorsorglich, d. h. anlasslos, gespeichert werden sollen, um allgemeine Sicherheit zu gewährleisten und Terrorismus sowie Kriminalität zu bekämpfen. Dies war zeitweise möglich; so trat 2006 eine entsprechende Regelung in Kraft, die zwischenzeitlich außer Kraft gesetzt wurde und nach knapp vier Jahren zuletzt 2019 erneut wieder ausgesetzt worden ist (Wiesner 2021). Aus Sicht des Europäischen Gerichtshofes ist die flächendeckende und pauschale Speicherung von Internet- und Telefonverbindungsdaten nicht zulässig, wie es das Gericht in drei Urteilen für das Vereinigte Königreich, Frankreich und Belgien verkündete (Wiesner 2021).

In der COVID-Pandemie wurde die Diskussion, welche Datenerhebung durch den Staat legitim ist, besonders relevant. So wurden zum Schutz der allgemeinen Gesundheit (und zur Eindämmung der Verbreitung des Virus) im größeren Maße Daten erfasst, die zum Teil hochsensibel waren (wie z. B. Gesundheitsdaten), die neben Freiheitsbeeinträchtigungen durch den eingeführten Lockdown zu Zumutungen hinsichtlich der demokratischen Bürgerrechte führten (Wiesner 2021).

Aus diesem Grund bleibt aus verantwortungsvoller Perspektive abzuwägen, inwiefern eine Einschränkung von Freiheit tatsächlich und auch wirksam zu einer Reduktion von Risiken führen kann, um so das Sicherheitsbedürfnis zu befriedigen (Mainzer 2018). Dies zeigt sich auch bei dem Wunsch vieler Staaten, einen „Zweitschlüssel“ zur Entschlüsselung verschlüsselter Daten (siehe Abschn. 4.4.1) zu erhalten. Experten äußerten sich hierzu jedoch kritisch, da dies nur einen weiteren möglichen Zugangspunkt für Kriminelle und Terrorist:innen ermöglichen würde und entsprechend bzw. folglich schlimmere Konsequenzen mit sich bringen würde als lediglich die fehlende Entschlüsselungsmöglichkeit durch den Staat (Abelson et al. 2015).

4.1.3.2 Ziviler Sektor

Im Zuge der aufkommenden Datenökonomie sind verschiedene Daten-Geschäftsmodelle entstanden, bei denen Unternehmen durch die Verwertung von Nutzungsdaten bessere Produkte und Services versprechen. Die gesammelten Daten sowie ihre Auswertung können in dreierlei Hinsicht verwertet werden (Stevens und Bossauer 2017):

1. zur internen Nutzung, um die Qualität bestehender Angebote zu verbessern,
2. zur Generierung neuer datengetriebener Services und
3. als Ware, die an Dritte verkauft oder mit ihnen geteilt wird.

Während für Punkt 1 insbesondere technische und funktionale Daten von Bedeutung sind, dienen Nutzungsdaten für Punkt 2 und 3 vor allem zur Erstellung von Nutzerprofilen (engl. Profiling).

Ein aktuelles Thema stellt ferner die Nutzung anonymisierter Datenbestände durch KI-Modelle dar. Bei der Anonymisierung erfolgt eine Abspaltung der Daten der betreffenden Person (bzw. der personenbezogenen Daten), sodass diese hinsichtlich des Datenschutzrechts im engeren Sinne herausfallen. Auch wenn durch die Daten nicht auf eine einzelne Person zurückgeschlossen werden kann, so können KI-Modelle trotzdem Daten verwenden, um Verbraucher:innen in Typen und Gruppen zu segmentieren (Sixt 2018). Beispielsweise können das Alter oder der Wohnort verwendet werden, um bestimmte Verhaltensweisen dieser Personengruppe vorherzusagen (z. B. hohe Zahlungsbereitschaft, Vorliebe für bestimmte Konsumgüter etc.) (Abb. 4.4).

Mühlhoff (2021) nennt deshalb durch anonymisierte Daten trainierte KI-Systeme auch Predictive Models. Dieses Modell ermöglicht die Bildung von generischen Nutzerprofilen. Im zweiten Schritt können diese generischen Modelle einer:s einzelnen Nutzer:in aufgrund der Daten zugeordnet und kategorisiert werden, die diese freigegeben hat

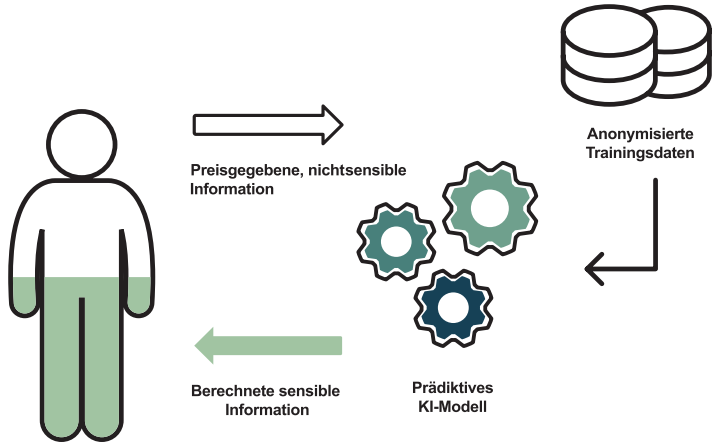


Abb. 4.4 Anonymisierte Datensätze können zum Trainieren von prädiktiven KI-Modellen genutzt werden, um sensible Informationen abzuleiten

(z. B. Browserdaten, Adressdaten, Cookie-Daten etc.). Aufgrund dieser Zusammenführung beider Teile können sensible Daten über die Betroffenen abgeleitet (z. B. persönliche Präferenzen, Neigungen und Wertvorstellungen) und individualisierte Angebote (z. B. passende Werbung, Nachrichten oder Filme) präsentiert werden. Aufgrund des verschleierten Zusammenhangs zwischen Datenpreisgabe und Datenverwertung wird die informationelle Selbstbestimmung für die einzelne Person erschwert. Ferner besteht die Gefahr von Gruppendiskriminierung durch Predictive Models sowie die Gefahr der Bildung einer Filterblase. Hierbei ist zu befürchten, dass Verbraucher:innen nur noch einseitige Inhalte und Informationen erhalten oder aber in der „Echokammer" landen, wobei soziale Kollektive nur noch mit den eigenen oder äquivalenten Meinungen konfrontiert werden.

Aufgrund der großen Nachfrage nach Kundendaten und -profilen existieren mittlerweile Unternehmen („Infomediäre"), die darauf spezialisiert sind, persönliche Daten aus unterschiedlichen Quellen zusammenzuführen, um so noch detailliertere Profile generieren zu können (Masur et al. 2018). Hierfür kaufen sie Nutzerdaten anderer Unternehmen, bereiten diese auf und verkaufen sie weiter.

Eine verschärfte Form des Profilings ist das **Scoring**. Hier werden wie beim Profiling Gemeinsamkeiten aus anonymisierten Nutzerdatenbanken identifiziert und mittels Algorithmen nach festgelegten Merkmalen gewichtet. In die so entstehende Formel werden dann konkrete personenbezogene Daten eines:einer Betroffenen eingesetzt, sodass dessen Scorewert bestimmt werden kann (Reiter und Mehner 2016). Betrachtet man Scoring aus der Verbraucherperspektive (Recki et al. 2023), so zeigt sich, dass hier Unklarheit darüber herrscht, wie sich der Score zusammensetzt. Bei einem von einer Kfz-Versicherungs-App genutzten Scoring-System, bei dem basierend auf dem Fahrverhalten Prämien berechnet werden, zweifelten Nutzer:innen die Berechnungen an, da Faktoren wie andere Verkehrsteilnehmer:innen oder die geografische Lage unberücksichtigt blieben (Recki et al. 2023). Ihre gesetzten Erwartungen wurden schließlich verletzt bzw. die Ziele der Nutzer:innen unterschieden sich von denen des Unternehmens und den darauf basierenden Berechnungen für Prämien, was schließlich zu Machtlosigkeit seitens der Nutzer:innen führte, die das Gefühl hatten, keinen Einfluss darauf nehmen zu können (Recki et al. 2023).

Das bekannteste Beispiel für Scoring ist das Sozialkreditsystem aus China, bei dem Bürger:innen in Städten wie Shanghai oder Rongchen, durch bestimmte Verhaltensweisen (wie ehrenamtliches Engagement, rechtzeitiger Zahlungen etc.) gewisse Vorteile (z. B. Überspringen von Wartelisten, Rabatte etc.) oder aber auch Nachteile erhalten können (z. B. Wegnahme von Haustieren oder der Ausschluss aus Hotels) (Universität Oldenburg 2018).

Breite Anwendung findet das Scoring auch beim Feststellen der Kreditwürdigkeit. In China arbeiten hierzu acht Großunternehmen zusammen, zu denen auch eine Social-Media-Plattform zählt. Der hierbei ermittelte Bonitäts-Score beruht dabei auf der finanziellen Situation der jeweiligen Nutzer:innen, ihrem Surf- und Einkaufsverhalten, jedoch auch ihren Online-Beziehungen (Sixt 2018). Dieser Score dient folglich nicht nur zur Bewertung der Kreditwürdigkeit, sondern eröffnet auch verbesserte Serviceleistungen oder gar ein besseres Ranking auf Dating-Webseiten (Sixt 2018).

Auch in Deutschland wird Scoring, wenn auch in kleinerem Maße, zur Bonitätsprüfung betrieben. In Deutschland gilt die Schufa (Schutzgemeinschaft für allgemeine Kreditsicherung) als eine der bekanntesten Auskunftsbehörden. Hierüber können Unternehmen Zahlungs- und Finanzauskünfte einholen, um die Kreditwürdigkeit eines:einer (potenziellen) Kund:in zu beurteilen. Weitere Einsatzbereiche für Scoring ist zudem Klout in den USA, das die Reputation eines Menschen auf Basis der Anzahl der Freund:innen in den sozialen Medien abbildet, was im Einstellungsverfahren bzw. für Bewerbungsgespräche eingesetzt wird (Sixt 2018).

Die Berechnung des Scorewerts mitsamt der Gewichtung einzelner Faktoren bleibt in der Regel unter Verschluss, weshalb Betroffene weder potenzielle Fehler korrigieren lassen noch Zusammenhänge erkennen können. Je nach Einfluss des Scorings auf die Lebensbereiche einer Person, kann dies schließlich zu Verhaltensveränderung/-anpassung führen, um negative Konsequenzen zu vermeiden. Bis 2001 hatte so beispielsweise bereits die Anfrage einer Schufa-Auskunft negativen Einfluss auf den Schufa-Score (Hornung 2014).

Beim Profiling und Scoring beruhen die Entscheidungen somit auf Wahrscheinlichkeiten für ein bestimmtes zukünftiges Verhalten, die wiederum auf den statistischen Erfahrungswerten mit der zugeordneten Vergleichsgruppe beruhen (Taeger 2016). Auskunfteien und auch Unternehmen haben deshalb ein großes Interesse daran, auf möglichst viele Daten zugreifen zu können, um das Verhalten, die Interessen oder auch Risiken z. B. hinsichtlich der Kreditwürdigkeit einer Person bestmöglich einschätzen zu können (Sixt 2018). Durch die immer bessere Zugänglichkeit zu allgemeinen Daten haben Unternehmen und Auskunfteien hierfür gute Chancen (Diercks 2016).

Profiling wie Scoring sind jedoch riskant, wenn sie die Diskriminierung von Gruppen fördern und bspw. Aspekte wie Alter, Familienstand, Gesundheitszustand, Wohnort und Geschlecht, aber auch sexuelle oder politische Interessen in die Berechnung mit einfließen (Sixt 2018). Sie sind auch deshalb riskant, weil sie selten offenlegen, wie die Berechnungen durchgeführt werden, was ein Machtungleichgewicht erzeugt, bei dem Nutzer:innen das Gefühl der Kontrolle, Handlungsfähigkeit und Einflussnahme verlieren (Recki et al. 2023; Belz 2018; Limerick et al. 2014), da ihnen keine Alternativen (für ein besseres Verhalten) aufgezeigt werden (Recki et al. 2023).

4.1.4 Datentreuhänder

Ein Ziel der EU besteht darin, die Datenwirtschaft in Europa zu fördern. Hierzu soll die Datenweitergabe zwischen unterschiedlichen Parteien gefördert werden. Dabei liegt strukturell ein Konflikt vor, der aus den unterschiedlichen Interessen und Zielen der verschiedenen Parteien entsteht, insbesondere wenn der Datennutzer (der „Agent“) die Daten nicht immer im besten Interesse des Dateninhabers (der „Principals“) verwertet. Dazu soll die neue Rolle des **Datentreuhänders** bzw. **Datenintermediärs** als neutraler Vermittler geschaffen werden, um das Vertrauen zwischen Dateninhaber:innen und Datenverarbei-

ter:innen aufrechtzuerhalten und den Principal-Agent-Konflikt im Zusammenhang mit der Datenverarbeitung zu minimieren.

Da Verbraucher:innen beim Datenschutz meist überfordert und bei der Durchsetzung ihrer Rechte in einer schwächeren Position sind, stellen Datentreuhänder für den digitalen Verbraucherschutz einen interessanten Ansatz dar. Als unabhängige Instanzen ohne wirtschaftliches Eigeninteresse können Datentreuhänder Verbraucher:innen bei der Verwaltung ihrer Daten unterstützen (Verbraucherzentrale Bundesverband e.V. 2020).

Das übergeordnete Ziel ist dabei, die Verarbeitung und den Austausch personenbezogener Daten zu erleichtern, ohne dabei die Verbraucher:innen außen vor zu lassen und sie stattdessen in ihrer digitalen Selbstbestimmung zu fördern. Herausforderungen stellen dabei vor allem eine bisher freiwillige Teilnahme der Datennutzer:innen bzw. das Fehlen eines gesetzlichen Rahmens sowie der sichere Ausschluss konfligierender Interessen insbesondere verschiedener Datennutzer:innen dar, die den Erfolg und die Nützlichkeit jener Plattformen beeinträchtigen (Verbraucherzentrale Bundesverband e.V. 2020).

Diese Art von Datenintermediären kommt bereits in der medizinischen Forschung zum Einsatz, da es hier häufig um besonders schützenswerte Daten geht. Demnach können diese Daten zur Behandlung sowie zur Erkennung möglicher Risikofaktoren beispielsweise helfen, neue Formen der Diagnose und Therapie zu entwickeln (Blankertz und Specht 2021). Die Trägerschaft solcher Datentreuhänder sollte dabei von Institutionen übernommen werden, die die Kriterien hinsichtlich

- **präziser Treuepflichten** (z. B. Grad des Datenzugriffs, Grenzen rechtsgeschäftlicher Mandate)
- **Qualitätsansprüchen** (z. B. Datensicherheit, Qualität der Verschlüsselung) und
- **Haftungsfragen** (z. B. bei einer Datenschutzverletzung)

erfüllen können (Verbraucherzentrale Bundesverband e.V. 2020).

Eine weitere Form sind **Personal Information Management Systems (PIMS**), auch Einwilligungsassistenten genannt. Sie sollen Verbraucher:innen dabei unterstützen, sich ihrer Rechte im Hinblick auf personenbezogene Daten bewusst zu werden und ihre damit verbundenen Interessen besser durchzusetzen. Dadurch soll ihnen mehr Kontrolle über ihre Daten ermöglicht werden (Blankertz und Specht 2021). Dazu bieten entsprechende Dienste beispielsweise die Möglichkeit, den Datenaustausch von verschiedenen Plattformen zusammenzutragen und somit eine Übersicht zu erhalten, auch über die mögliche Nutzung durch Dritte (Blankertz und Specht 2021).

Das Ziel dieser Systeme sollte es sein, die individuellen und kollektiven Bedürfnisse voranzutreiben und möglichst wenig Daten zu erheben bzw. zu speichern und dazu möglichst eng definierte Zwecke vorzugeben (Stevens und Boden 2022). Dies könnte beispielsweise durch eine vereinheitlichte Einwilligungserklärung, bereitgestellt durch den Datenintermediär, erreicht werden (Blankertz und Specht 2021). Potenziell wäre auch das Ziel, über diese Plattform die Wahrnehmung der Rechte zu delegieren, was jedoch durch die DSGVO bisweilen untersagt ist, so dass die Funktionalitäten für selbstbestimmtes Handeln noch eingeschränkt bleiben (Blankertz und Specht 2021).

Neben neutralen Instanzen sind aus Verbrauchersicht auch **parteiische Datentreuhänder** hilfreich, welche die Rolle eines Anwalts von Verbraucherinteressen übernehmen (Stevens und Boden 2022). Als Anwalt achtet der Treuhänder darauf, dass die Interessen von Verbraucher:innen gewahrt werden, verwaltet pseudonymisierte bzw. anonymisierte Personendaten und achtet darauf, dass deren Verwertung nicht gegen die Interessen von Verbraucher:innen genutzt werden, z. B., dass sie nicht zum Trainieren von Predictive Models für das Scoring oder zur Ermittlung dynamischer Preise genutzt werden (Verbraucherzentrale Bundesverband e.V. 2020).

4.1.5 Datenschutztechniken

Verbraucher:innen sollten hinsichtlich ihrer Privatsphäre geschützt und gestärkt werden, was zunehmend wichtiger zu werden scheint als lediglich die Sicherstellung ihres Rechts auf Privatsphäre. Denn Privatsphäre wird zunehmend zum Instrument, um Datenwirtschaft auszuweiten und zu legitimieren, wohingegen die Verhinderung oder Einschränkung oftmals in den Hintergrund zu rücken scheint (Djeffal 2019). Die Verantwortung wird dabei größtenteils den Verbraucher:innen zugeschrieben (Helm und Seubert 2020). Aus dem Grund befasst sich u. a. die Forschung damit, Verbraucher:innen auf die Risiken und Gefahren hinzuweisen und sie beim Selbstschutz zu stärken. Diese Unterstützung bezweckt dabei insbesondere, die informationelle Selbstbestimmung zu steigern oder den Schutz vor Cyberkriminellen zu erhöhen. Dazu werden Konzepte entwickelt und Initiativen gegründet, um Verbraucher:innen bspw. durch Schulungsangebote und Workshops zu sensibilisieren und zu qualifizieren.

4.1.5.1 Verschlüsseln und Anonymisieren

Die sichersten Daten sind die Daten, die nicht erhoben, nicht gespeichert bzw. nach ihrem Gebrauch sofort vernichtet werden. Dies ist jedoch nicht immer möglich. Um anhand von Daten jedoch nicht direkt auf die Personen, auf die sie bezogen sind, Rückschlüsse ziehen zu können, besteht die Möglichkeit, diese zu anonymisieren, zu pseudonymisieren oder zu verschlüsseln.

Verschlüsselung stellt ein wichtiges Verfahren dar, um Daten vor einem unberechtigten Zugriff zu schützen. Verschlüsselung ist vor allem durch den Einsatz im Rahmen der digitalen Kommunikation bekannt, wie beispielsweise beim Versenden von Nachrichten per E-Mail, Messenger oder auch beim Telefonieren. Sie findet zudem auch bei VPN-/Tor-Netzwerken als Verschlüsselungsmechanismus zum Datenschutz Verwendung.

Ähnlich wie bei der „Verschlüsselung“ eines Fahrrads mit einem Schloss ist ein hundertprozentiger Schutz nicht möglich, jedoch kann dieses den Zugriff oder Diebstahl erschweren. Grundsätzlich wird durch die Verschlüsselung bewirkt, dass versendete Informationen nicht bzw. nur schwer nachverfolgbar sind und nur vom Sender und Empfänger gelesen werden können (Ende-zu-Ende-Verschlüsselung). Dazu werden die Informationen durch rechnerische Verfahren unleserlich gemacht (kodiert) (Seele und Zapf 2017) oder über verschiedene Zwischenstationen beim Versenden umgeleitet, so dass ins-

besondere die IP-Adresse als Mittel zur Personenbestimmung nicht unmittelbar nachverfolgbar ist (Endres 2013). Den Schlüssel besitzen dabei im Idealfall nur Sender und Empfänger, um so die Nachricht entschlüsseln zu können (Seele und Zapf 2017).

Es kommt jedoch auch vor, dass Personen, Gruppen oder auch Communities eigene Codes verwenden, die nur sie verstehen, und dass Nachrichten zwar öffentlich und verständlich sind, in ihrer wahren Bedeutung aber so entfremdet, dass nur Insider sie verstehen bzw. entschlüsseln können – ein Verfahren, das auch „soziale Steganografie" genannt wird (Seele und Zapf 2017).

Oftmals liegt es in der Verantwortung der Verbraucher:innen, durch die (zusätzliche) Verwendung von Technologien, Tools und (Browser-)Plugins bestimmter Hersteller für eine ausreichende Verschlüsselung zu sorgen (Masur et al. 2018). Dies hat verschiedene Gründe. Auch wenn vielen Verbraucher:innen verschiedene Verschlüsselungsverfahren bekannt sind und darüber hinaus entsprechende Technologien und Dienste angeboten werden, fehlt ihnen oftmals das technische Know-how; zudem wissen sie oft auch nicht um die Bedeutung bzw. die sich daraus ergebenden Vorteile (Wiesner 2021). Weiterhin gehen Lösungen zur Datenverschlüsselung zu Lasten deren Usability, sodass hier die Rufe nach gebrauchstauglichen Technologien zum Schutz der Privatsphäre laut werden (Wiele und Weßelmann 2017; Karaboga et al. 2014).

Zur Aufgabenbewältigung, zur statistischen Auswertung oder zum Trainieren von KI-Modellen muss der Datenverarbeiter auf die unverschlüsselten Daten zugreifen können. Dabei ist es wichtig, zumindest datenschutzfreundliche Techniken wie die anonyme oder zumindest pseudonyme Nutzung personenbezogener Daten zu verwenden. Der Grad der Identifizierbarkeit hängt vom erreichten Anonymisierungsgrad ab (siehe Abb. 4.5).

Unter **Anonymisierung** versteht man dabei das Entfernen von Merkmalen, die sonst Rückschlüsse auf eine Person zuließen und sie somit auch angreifbar oder verletzbar ma-

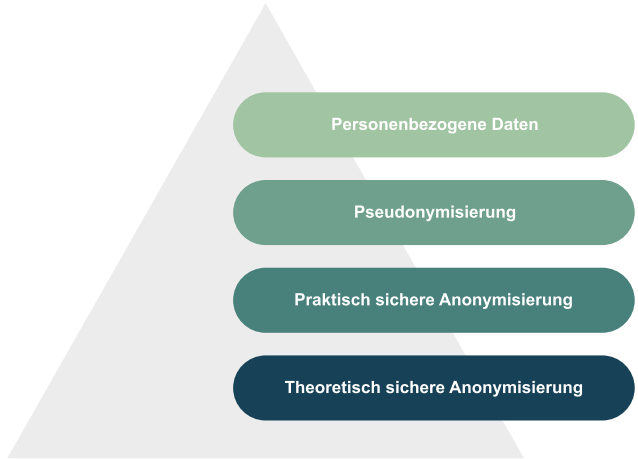


Abb. 4.5 Grad der Anonymisierung

chen. Einer Person ermöglicht Anonymität in öffentlichen Räumen zudem die Durchführung privater Verhaltensweisen, wenn die Person niemandem bekannt ist oder von niemanden erkannt wird. Auch im Internet werden ähnliche Vorkehrungen getroffen, um insbesondere weniger schnell erkannt zu werden, wenn auch das Aufrechterhalten von Anonymität langfristig jedoch kaum möglich ist (Masur et al. 2018).

Hierbei kann man zwischen der praktisch sicheren und der theoretisch sicheren Anonymisierung unterscheiden. Bei der praktisch sicheren Anonymisierung ist das Risiko, dass einzelne Personen re-identifiziert oder zurückverfolgt werden können, in der Praxis äußerst gering und nur mit hohem Aufwand zu erreichen. Bei der theoretisch sicheren, vollständigen Anonymisierung ist aufgrund wahrscheinlichkeits- und informationstheoretischer Prinzipien eine Re-Identifizierung einzelner Personen nur mit einer sehr kleinen, vorab definierten Wahrscheinlichkeit möglich. Zur Messung des Anonymisierungsgrades von Daten wurden in der Literatur verschiedene Maße vorgeschlagen (Petrlic et al. 2023). Ein Maß ist z. B. die **K-Anonymität**. Vereinfacht ausgedrückt bedeutet das, dass zu bestimmten Merkmalen einer Person im Datensatz k-1 Personen mit den gleichen Merkmalen existieren.

Im Prozess der **Pseudonymisierung** wird sichergestellt, dass Informationen ohne Hinzuziehung zusätzlicher Informationen nicht mehr zu einer Person zurückgeführt werden können. Dabei wird bspw. der Name durch ein Pseudonym ersetzt, zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Dies ermöglicht jedoch die Verarbeitung der Daten bspw. zum Zwecke des Profilings in aggregierter Form.

Doch auch auf Verbraucherseite kann ein Pseudonym helfen, sich und seine Persönlichkeit zu verschleiern. Dies zeigt sich zum Beispiel bei Autor:innen, die ihre Werke unter anderen Namen publizieren (Keber 2018) oder aber einen Nutzernamen in Foren oder sozialen Netzwerken verwenden, sofern bei diesen keine Klarnamenpflicht besteht (Matzner 2018). Die Verwendung eines Pseudonyms erleichtert es einerseits, private Informationen risikofreier zu teilen, und erschwert andererseits die Auffindbarkeit des eigenen Profils (Masur et al. 2018). Der Bedarf eines privaten (Rückzugs-)Bereichs für die Meinungsbildungs- und Meinungsäußerungsfreiheit scheint somit von Bedeutung, weshalb es durch den EuGH in seiner Entscheidung zur Vorratsdatenspeicherung berücksichtigt wurde (Keber 2018).

Die Wirksamkeit einer Anonymisierung und Pseudonymisierung greift jedoch nur, sofern die Daten nicht von Personen verarbeitet werden, die im direkten Kontakt mit der Person stehen und dadurch Rückschlüsse ziehen und Verbindungen herstellen können (Masur et al. 2018).

4.1.5.2 Privacy by Design

Eine wichtige Voraussetzung beim digitalen Verbraucherschutz ist die Gestaltung und Entwicklung von sicheren und datenschutzfreundlichen Produkten und Technologien. Mit der Zunahme datensammelnder Technologien in den 1970ern wurden auch die Herausforderungen an den Datenschutz immer größer.

Dies hat schließlich zur Entwicklung von **Privacy Enhancing Technologies (PETs)** geführt, die eine vielfältige Gruppe von Technologien und Anwendungen sind, welche die Privatsphäre schützen sollen (European Network and Information Security Agency 2014). Diese Technologien reichen von Kryptografie- und Anonymisierungstechniken bis hin zu Tools und Protokollen, welche die Sammlung, Verarbeitung und den Austausch von Daten sicherer und datenschutzfreundlicher gestalten.

Daneben finden sich sogenannte Privacy Design Patterns (Hafiz 2006). Ein Beispiel ist der „Privacy by Default"-Ansatz, der besagt, dass bei Verwendung die Standardeinstellung so sein sollte, dass Nutzer:innen nur dann zusätzliche Informationen preisgeben müssen, wenn sie dies explizit wünschen. Dieses Muster der datenschutzfreundlichen Voreinstellungen hat auch Eingang in die DSGVO gefunden.

Eine Ergänzung hier stellt **Privacy by Design** dar, die sich als Gegenbewegung zur „Surveillance by Design" versteht (Davies 2010). Der Ansatz beinhaltet sieben Grundsätze zum proaktiven und wirkungsvollen Datenschutz beim Umgang mit datenverarbeitenden Technologien (Rost und Bock 2011; Cavoukian 2009). Die Grundsätze sind in Tab. 4.1 zusammengefasst.

Die Prinzipien stellen dabei keine konkreten Lösungsansätze der Gestaltung dar (Rost und Bock 2011), sondern formulieren vielmehr allgemeine Anforderungen, was es bei der Systementwicklung zu beachten gibt (European Network and Information Security Agency. 2014). Der Ansatz verfolgt dabei den Anspruch, den Privatsphärenschutz und seine Anforderungen möglichst früh und ganzheitlich im Lebenszyklus der Systementwicklung zu berücksichtigen, um später teure, aufwendige und potenziell fehlerbehaftete Nachrüstungen und Sicherheitspatches zu vermeiden.

4.1.6 Datenschutzverhalten

Neben technischen und organisatorischen Maßnahmen hängt der Datenschutz vom Verhalten der betroffenen Personen ab. Zur Erklärung des Datenschutzverhaltens sind dabei verschiedene Ansätze herangezogen worden.

Bedürfnistheoretische Erklärungsmodelle. Ein wesentliches Erklärungsmodell stellen bedürfnistheoretische Ansätze (vgl. Kap. 2) dar. Diese Ansätze beziehen sich auf die Idee, dass Privatsphäre ein grundlegendes menschliches Bedürfnis ist. Das individuelle Datenschutzverhalten entspringt hierbei dem Bedürfnis nach Privatheit bzw. ist durch die Ziele geprägt, die mit dem Schutz der Privatheit verfolgt werden.

Das Bedürfnis nach Privatsphäre erwächst aus den Funktionen der Privatsphäre und persönlicher Räume, das psychische Wohlbefinden und die mentale Gesundheit einer Person zu schützen und zu fördern. Westin (2015) unterscheidet hierbei vier Funktionen:

- **Persönliche Autonomie (personal autonomy):** Im Privaten erleben Menschen eine gesteigerte Fähigkeit, ihre eigenen Entscheidungen zu treffen und ihr Leben unabhängig von äußeren Einflüssen zu gestalten.

Tab. 4.1 Die sieben Grundsätze des Privacy by Design (PbD, nach Cavoukian 2009)

Grundsatz	Beschreibung
1. **Proaktiv, nicht reaktiv Vorbeugung nicht Abhilfe**	PbD kommt vor dem Ergebnis, nicht danach. Sie verhindert Beeinträchtigungen der Privatsphäre bevor sie eintreten. Sie gilt präventiv und beratend und adressiert somit keine Abhilfemaßnahmen zur Behebung von aufgetretenen Datenschutzverletzungen.
2. **Datenschutz als Standard-einstellung**	Wir können uns alle einer Sache gewiss sein – die Standardeinstellungen sind entscheidend! PbD soll den größtmöglichen Schutz der Privatsphäre bringen, indem sichergestellt wird, dass personenbezogene Daten automatisch in jedem IT-System und bei allen Geschäftspraktiken geschützt werden. Wenn eine Person nichts unternimmt, bleibt der Schutz ihrer Privatsphäre immer noch intakt. Einzelpersonen sind nicht gefordert, selbst etwas für den Schutz ihrer Privatsphäre zu unternehmen – der Schutz ist bereits systemimmanent, als Standardeinstellung.
3. **Der Datenschutz in das Design eingebettet**	PbD ist in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet. Es wird nicht nach dem Vorfall als Add-on eingebaut. Das Ergebnis ist, dass der Datenschutz eine wesentliche Komponente der Kernfunktionalität wird. Datenschutz ist ein wesentlicher Bestandteil des Systems, ohne Abstriche bei der Funktionalität.
4. **Volle Funktionalität – eine Positivsumme, keine Nullsumme**	PbD will allen berechtigten Interessen und Zielen entgegenkommen, und zwar durch eine Positivsumme, die ein zufriedenstellendes Ergebnis für beide Seiten erzielt, und nicht durch einen veralteten Nullsummenansatz, bei dem schließlich unnötige Kompromisse erforderlich werden. Durch PbD wird die Vortäuschung falscher Dichotomien wie Datenschutz versus Sicherheit vermieden. PbD zeigt, dass es möglich ist, beides zugleich zu erreichen.
5. **Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus**	Nachdem PbD vor der Ersterfassung der Information in das System „eingebettet“ wurde, erstreckt sich dessen Wirkung auf den gesamten Lebenszyklus der Daten – starke Sicherheitsmaßnahmen sind für den Datenschutz unerlässlich, und zwar von Anfang bis Ende. Dadurch wird erreicht, dass alle Daten sicher gespeichert und am Ende des Prozesses sicher und rechtzeitig vernichtet werden. So sorgt PbD „von der Wiege bis zur Bahre“ durchgängig für eine sichere Datenverarbeitung.
6. **Sichtbarkeit und Transparenz – Für Offenheit sorgen**	PbD will allen Beteiligten die Sicherheit geben, dass das System unabhängig von Geschäftspraktiken oder Technologien wirklich die angekündigten Maßnahmen und Ziele verfolgt und sich einer unabhängigen Prüfung unterwirft. Seine einzelnen Komponenten und Verfahren bleiben sichtbar und transparent, und zwar gleichermaßen für Nutzer:innen und Anbieter:innen. Denken Sie daran: Vertrauen ist gut, Kontrolle ist besser.
7. **Die Wahrung der Privatsphäre der Nutzenden – Für eine nutzerzentrierte Sicherheit sorgen**	PbD erfordert vor allem von den Architekt:innen und Betreiber:innen (von IT-Systemen), dass für sie die Interessen der Einzelpersonen an erster Stelle stehen. Sie bieten Maßnahmen wie strenge datenschutzfreundliche Voreinstellungen und angemessene Benachrichtigungen an und eröffnen benutzerfreundliche Optionen. Sie sorgen für eine nutzerzentrierte Gestaltung.

- **Emotionale Freiheit (emotional release):** Das Private schafft einen Raum, Gefühle und Emotionen auszudrücken, ohne Angst vor Urteilen oder Konsequenzen haben zu müssen.
- **Selbstreflexion (self-evaluation):** Der private Raum schafft die Möglichkeit, frei über das eigene Leben und die eigenen Handlungen nachzudenken und sich selbst besser zu verstehen.
- **Kontrollierte und geschützte Kommunikation (limited and protected communication):** Die private Kommunikation schafft einen Raum, Informationen auszutauschen und zu kommunizieren, ohne dass dies von Dritten unangemessen überwacht oder beeinflusst wird.

Diese Funktionen des Privaten dienen als Instrumente, um individuelle Ziele zur Selbstverwirklichung zu erreichen (Westin 2015). Doch Westin zufolge sind genauso die Bedürfnisse nach Offenlegung, Austausch sowie Gesellschaft und Geselligkeit ein wichtiger und gleichwertiger Gegenpol.

Masur et al. (2018) nennen dazu fünf Gründe, warum Menschen ein Bedürfnis nach Austausch haben und sich anderen gegenüber selbst offenbaren:

- Soziale Anerkennung
- Aufbau und Pflege sozialer Beziehungen
- Emotionale Erleichterung
- Kontrolle und Beeinflussung des Umfelds
- Entfaltung der Identität und Persönlichkeit

Hierbei könnte der Eindruck entstehen, dass die Gründe für bzw. die Funktionen von Privatsphäre mit den Gründen für eine Selbstoffenbarung konfligieren, stattdessen ist insbesondere aus Sicht der Persönlichkeitsentwicklung dieses Wechselspiel aus privatem und öffentlichem Leben entscheidend. Nichtsdestotrotz gibt es Risiken der Selbstoffenbarung wie Ablehnung, Kontrollverlust, Integritätsverlust, Verrat, aber auch Bloßstellung (des Gegenübers) (Masur et al. 2018). Diese Risiken können jedoch auch als Konsequenz von Isolation aufgrund eines übermäßigen Privatverhaltens auftreten.

Die Grenze zwischen Privatheit und Öffentlichkeit ist jedoch nicht immer eindeutig, sondern muss kontextabhängig betrachtet werden. Ferner sind die Ziele und Bedürfnisse nach Privatheit individuell unterschiedlich und kulturell geprägt (Millham und Atkin 2018; Dogruel und Joeckel 2019).

Rational Choice Ansätze. Ein weiteres, wichtiges Erklärungsmodell zum Datenschutzverhalten von Personen sind die Rational-Choice-Theorien. Gemäß diesen Theorien handelt der Mensch auf Basis einer Kosten-Nutzen-Abwägung (vgl. Kap. 2).

Ein prominenter Vertreter dieses Ansatzes stellt die **Privacy Calculus Theory** dar, die davon ausgeht, dass bei einer Datenpreisgabe die erwarteten Vorteile und wahrgenommenen Risiken die Entscheidung von Nutzer:innen beeinflussen und entsprechend der Abwägung danach handeln (Dinev und Hart 2006).

Basierend auf der Privacy-Calculus-Theorie schlagen Krasnova und Veltri (2010) ein theoretisches Modell vor, um das Datenschutzverhalten auf sozialen Netzwerken zu erklären. In ihrem Modell argumentieren sie, dass der Hauptnutzen der Datenfreigabe bei Social-Media-Anwendungen im Genuss, in der Selbstdarstellung und in der Pflege von Beziehungen besteht. Demgegenüber stehen die Risiken und Nachteile der Datenpreisgabe, die sich in allgemeinen Datenschutzbedenken äußern. Diese Bedenken werden auch durch die wahrgenommenen möglichen Schäden und die Eintrittswahrscheinlichkeit einer Datenschutzverletzung beeinflusst.

Die Wahrnehmung der Vorteile und Risiken hängt auch von Vertrauen in die Betreiber und Anbieter der Technologie sowie vom Vertrauen in die anderen Nutzer:innen ab. Dabei gehen Krasnova und Veltri (2010) davon aus, dass das Nutzervertrauen durch die wahrgenommene Kontrolle über ihre Daten sowie das Bewusstsein über die Informationsverarbeitungspraktiken und die persönlichen Überzeugungen hinsichtlich der Effektivität der Rechtsaufsicht beeinflusst wird. Das resultierende sozialpsychologische Erklärungsmodell ist in Abb. 4.6 zusammengefasst.

Die Rational-Choice-Ansätze wurden jedoch in vielerlei Hinsicht kritisiert. Insbesondere setzt eine rationale Entscheidung voraus, dass den Betroffenen alle notwendigen Informationen zur Verfügung stehen und sie kognitiv in der Lage sind, diese zu verarbeiten. Bei der Preisgabe ihrer Daten auf einer Webseite oder beim Festlegen von Datenschutzeinstellungen müssen Verbraucher:innen beim Abwägen der Vor- und Nachteile wissen, welche Daten erhoben werden und wofür sie genau genutzt werden sollen. Ferner müssen sie sich der möglichen Risiken bewusst werden und diese in ihr Kalkül ein-

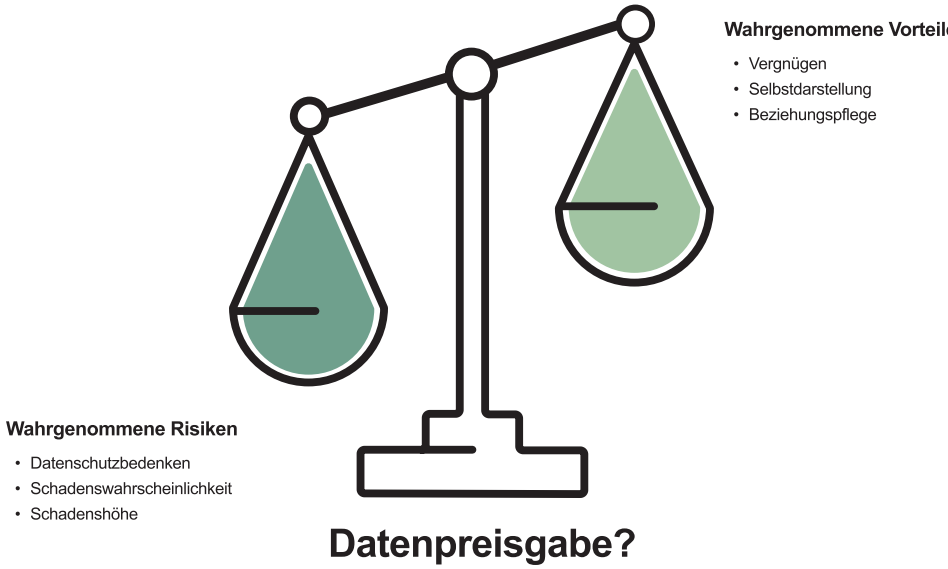


Abb. 4.6 Privacy Calculus als Erklärungsmodell des Datenschutzverhalten bei Social Media Anwendungen

beziehen. Doch es zeigt sich schon allein bei der Einwilligung in die AGBs oder Datenschutzbestimmungen eines Unternehmens digitaler Dienste, dass diese in den seltensten Fällen von Verbraucher:innen gelesen werden. Stattdessen werden sie oftmals „blind“ akzeptiert, um unmittelbar und mit geringem (Lese-/Zeit-)Aufwand die gewünschten Dienste oder Produkte nutzen zu können (McDonald und Cranor 2008). Verbraucher:innen ist daher nicht genau bewusst, welche Daten dabei konkret erfasst werden, auf welche Weise sie verarbeitet werden (und von wem) und welche Risiken und Nachteile damit verbunden sind (Jakobi et al. 2020).

Verhaltensökonomische Ansätze. Aufgrund dieser Defizite der Rational-Choice-Theorien wird das Datenschutzverhalten heutzutage oft mithilfe verhaltensökonomischer Ansätze erklärt. Verhaltensökonomische Ansätze untersuchen dabei, wie kognitive und Umweltfaktoren die Entscheidungen des Einzelnen beeinflussen (vgl. Kap. 2).

Um das Verständnis für das alltägliche Datenschutzverhalten von Einzelpersonen zu verbessern, zielen verhaltensökonomische Erklärungsmodelle darauf ab, folgende Schwächen der Rational-Choice-Ansätze zu adressieren (Alessandro Acquisti und Grossklags 2007):

- Datenschutzentscheidungen werden von unvollständigen Informationen, falschen Informationen und Täuschungstaktiken beeinflusst.
- Datenschutzentscheidungen können zu einer Vielzahl von Konsequenzen führen, die Individuen kaum in ihrer Gesamtheit berücksichtigen können.
- Datenschutzentscheidungen können aufgrund verschiedener Verhaltensanomalien und kognitiver Verzerrungen (cognitive biases) von außen als nicht rational erscheinen.

Gegenüber den Rational-Choice-Ansätzen betont dabei die Verhaltensökonomie, dass die Abwägung der Vor- und Nachteile der Datenpreisgabe auf kognitiven „Kurzschlusshandlungen“ (heuristic shortcuts) basiert (Ghaiumy Anaraky et al. 2021).

In kontrollierten Studien zum Privacy-Paradoxon (engl. „**Privacy Paradox**“) (Norberg et al. 2007) konnte hierbei die Existenz von Verhaltensweisen nachgewiesen werden, die systematisch von denen abweichen, die von der Rational-Choice-Theorie vorhergesagt werden. Das Privacy-Paradoxon bezieht sich auf die Absichten und Einstellungen des Nutzenden darüber, persönliche oder vertrauliche Informationen preiszugeben, und das tatsächliche Verhalten in einer spezifischen Situation, in dem solche Informationen offengelegt werden (Norberg et al. 2007).

Im Rahmen des Experiments wurden die Teilnehmer:innen mit einem Marketing-Szenario konfrontiert und gebeten einzuschätzen, wie hoch ihre Bereitschaft wäre, persönliche Informationen an ein kommerzielles Unternehmen weiterzugeben. Zwölf Wochen später wurden sie dann tatsächlich darum gebeten, dieselben persönlichen Informationen an eine Person weiterzugeben, die angab, ein kommerzielles Unternehmen zu vertreten. Dabei wurde eine signifikante Diskrepanz zwischen der zuvor geäußerten Bereitschaft und dem späteren tatsächlichen Verhalten festgestellt.

Fallbeispiel Privacy Paradox

Anna ist sehr besorgt um ihre Privatsphäre im Internet. Sie liest regelmäßig Artikel über Datenskandale und versucht, ihre Online-Aktivitäten so zu gestalten, dass sie so wenig Daten wie möglich preisgeben muss. Deshalb nutzt sie auch nur wenige Apps auf ihrem Smartphone und lehnt es ab, ihre Kreditkarteninformationen online zu speichern.

Eines Tages jedoch erhält Anna eine E-Mail von einem Online-Shop, den sie regelmäßig besucht. In der E-Mail wird sie darauf hingewiesen, dass sie für den Kauf von bestimmten Produkten Punkte sammeln und diese später gegen Rabatte einlösen kann. Anna ist von dieser Idee begeistert und beschließt, sich für das Punkteprogramm anzumelden.

Selbstkontrolle

Erklären Sie das Privacy Paradox mithilfe der Verhaltensökonomie.

Die beobachtete Diskrepanz lässt sich unter anderem durch das Vorliegen von kurzfristigen Vorteilen und langfristigen Risiken erklären.

Wie zuvor beschrieben, gibt es verschiedene Motivationen für die Datenpreisgabe (wie bspw. soziale Anerkennung, Freude, monetäre Anreize etc.) um dadurch zumindest kurzfristig Vorteile zu erhalten. Dem stehen oftmals langfristige Risiken gegenüber, die bei der Entscheidung weniger stark präsent sind und berücksichtigt werden (Gerber et al. 2017; A. Acquisti und Grossklags 2005). So sind sich Verbraucher:innen z. B. abstrakt bewusst, dass bspw. preisgegebene Daten miteinander verknüpft und zur Erstellung von Nutzerprofilen verwendet werden. Die konkreten Risiken sind jedoch meist nicht greifbar und werden als komplex wahrgenommen, wohingegen die Vorteile unmittelbar erfahrbar und einschätzbar sind.

Zudem ist es aus Verbraucherperspektive fast unmöglich, in meist begrenzter Zeit alle Informationen einzuholen und zu verstehen, um potenzielle Risiken hinsichtlich der Wahrscheinlichkeit ihres Eintreffens einzustufen (A. Acquisti und Grossklags 2005). Dadurch entsteht eine Informationsasymmetrie gegenüber Produkten und Dienstleistungen, bei denen Daten offengelegt werden sollen. Dies lässt sich, bezogen auf die Entscheidungsfindung, neben unvollständigen Informationen ebenfalls durch das Bounded-Rationality-Modell (begrenzte Rationalität) erklären, wonach Entscheidungen mangels Verfügbarkeit von Zeit und Berechnungsmöglichkeit nicht gut getroffen werden können (Kokolakis 2017).

Entsprechend ist das Privacy Paradox nicht als konstant zu verstehen. Zum einen ändert sich der Kontext, bei dem man über Datenschutz reflektiert, und die Situation, in der man die tatsächliche Entscheidung trifft (Gerber et al. 2017). Zum anderen ändern sich die Schutzbedürfnisse mit der Zeit. Dies kann auf eine Veränderung im Lebensstil, eine Verschiebung in den Wertvorstellungen oder neue Möglichkeiten bei der Verwendung von Produkten und Services oder auch die Verfügbarkeit von zusätzlicher Information zur Einschätzung und Bewertung neuer Informationen zurückzuführen sein.

In der Forschung wird entsprechend vorgeschlagen, die tatsächlichen Handlungen bzw. das tatsächliche Verhalten von Verbraucher:innen zu untersuchen, da diese einen höheren Erkenntnisgewinn versprechen als die oftmals eher abstrakten Einstellungen und Absichten gegenüber dem Schutz der eigenen Privatsphäre (Kokolakis 2017).

Rationaler Fatalismus. Einen weiteren Erklärungsansatz stellt das Modell des rationalen Fatalismus (engl. rational fatalism) dar (Kerwin 2012). Dem Modell zufolge findet bei der Nutzung von Internetservices keine situative Risikoabwägung statt, bei der die Vor- und Nachteile abgewogen werden. Vielmehr werden Datenschutzüberlegungen aufgrund einer Resignation eher verdrängt, da Verbraucher:innen glauben, dass sie ohnehin keine Wahl haben, oder glauben, keine Kontrolle über die Konsequenzen oder das Ergebnis zu haben. Im Falle der Privatsphäre bezieht sich dies vor allem auf die Hilflosigkeit oder mangelnde Fähigkeit, die eigene Privatsphäre ausreichend zu schützen (Xie et al. 2019).

Folglich entsteht eine Machtasymmetrie, da die hier erwähnte Kontrolle sowie die entsprechenden Möglichkeiten erst durch den Anbieter bestimmt und ermöglicht werden. Risiken und negative Folgen werden notwendigerweise in Kauf genommen, da die Folgen unausweichlich sind bzw. Verbraucher:innen auch keine Vorteile für sich erkennen, wenn sie sich ausgiebig mit dem Thema befassen bzw. ihre Risikobereitschaft verringern würden (Xie et al. 2019).

Xie et al. (2019) erkennen fatalistische Züge hierbei auf drei Ebenen:

- **Rechtliche Ebene**, da Verbraucher:innen per se keine Eigentumsrechte über ihre persönlichen Daten besitzen und sie teilweise davon ausgehen, dass die derzeitige Rechtslage nicht umfassend genug ist, um die Privatsphäre ausreichend schützen zu können.
- **Funktionelle/technische Ebene**, da Verbraucher:innen kaum eine Wahl oder die Möglichkeit haben, um Produkte und Services vollkommen nach ihren (Privatheits-) Bedürfnissen zu nutzen oder anzupassen, wie beispielsweise eine vollständig anonyme Internetnutzung. Mithin sind sie nahezu dazu gezwungen, bestimmte Produkte und Services zu nutzen.
- **Unternehmerische Ebene**, da Verbraucher:innen wissen und davon ausgehen, dass die Unternehmen hinter den Produkten und Services ihre Daten sammeln, analysieren und Nutzerprofile erstellen und sich demgegenüber hilflos fühlen, dass die Unternehmen mithilfe ihrer verfügbaren Mittel in die Privatsphäre eindringen.

Je höher der Grad an Fatalismus ist (d. h., je eher an das Vorhandensein einer höheren Macht geglaubt wird, die das Handeln und die Konsequenzen bestimmt), desto eher geben die Leute den Risiken nach und den Versuch auf, ihre Privatsphäre zu schützen. Dies lässt sich auch in anderen Bereichen wiedererkennen, wie beispielsweise beim Führen eines gesunden Lebensstils (Xie et al. 2019; Kerwin 2012).

4.1.7 Gebrauchstauglicher Datenschutz

Die Erkenntnisse zum Datenschutzverhalten haben auch Eingang in die Gestaltung gebrauchstauglicher Sicherheitsanwendungen (engl. **Usable Privacy and Security,** kurz **UPS**) gefunden. Darüber hinaus betont dieser Forschungsbereich, dass das Datenschutzverhalten nicht allein von der Motivation der Nutzer:innen, sondern auch von der Gestaltung der Sicherheitsinfrastrukturen und der Sicherheitsmechanismen abhängt.

Basierend auf der nutzer:innen-zentrierten Gestaltung von gebrauchstauglichen Produkten und Dienstleistungen (vgl. Abschn. 6.4) sollen bei den Methoden dieses Ansatzes Aufgaben und Ziele nicht nur effektiv, effizient und zufriedenstellend erreicht werden (ISO 2018), sondern dabei auch die sicherheits- und datenschutzrelevanten Bedürfnisse mitberücksichtigt werden (Sasse et al. 2016). Gegenüber der Gestaltung gebrauchstauglicher Anwendungen weist der Bereich der gebrauchstauglichen Sicherheit eine Reihe von Besonderheiten auf. Diese fassen Garfinkel und Lipford (2014) wie folgt zusammen:

- **Unmotivierte Nutzer:innen.** Die meisten Menschen nutzen Computer nicht, um ihre Sicherheit und Privatheit zu schützen; stattdessen möchten sie E-Mails senden, Webseiten durchsuchen oder Software herunterladen und dabei Sicherheit haben, die sie schützt, während sie diese Dinge tun.
- **Abstrakte Eigenschaft.** Digitale Privatheit und Sicherheit sind abstrakte Eigenschaften, bei denen viele Schutzkonzepte für die Mehrheit der Bevölkerung fremd und nicht intuitiv sind
- **Fehlendes Feedback.** Um gefährliche Fehler zu verhindern, bedarf es eines guten Feedbacks über die Konsequenzen einer Handlung. Jedoch ist gutes Feedback für die Sicherheits- und Freiheitsverwaltung ein schwieriges Problem.
- **Geist in der Flasche.** Sobald ein Geheimnis versehentlich ungeschützt war (selbst für kurze Zeit), kann man nicht sicher sein, dass es nicht bereits preisgegeben wurde. Danach gestaltet es sich äußerst schwierig bis nahezu unmöglich, den „Geist“ wieder in die „Flasche“ zu bringen.

Darüber hinaus stehen Gebrauchstauglichkeit und Datenschutz häufig in einem Spannungsfeld zueinander, da ein höherer Privatsphärenschutz zu Lasten der Gebrauchstauglichkeit eines Produkts oder einer Dienstleistung gehen kann (Gerber et al. 2015).

Ein Beispiel für dieses Spannungsfeld ist der Nachrichtenaustausch per E-Mail. So besteht eine wichtige Datenschutztechnik darin, die Kommunikation zu verschlüsseln. Ein gängiges Problem ist dabei jedoch, dass E-Mail-Korrespondenz standardmäßig unverschlüsselt ist. Dadurch können sowohl der E-Mail-Anbieter als auch die beteiligten Transportstellen die E-Mails mitlesen. Dies stellt eine erhebliche Sicherheitslücke dar und erhöht das Risiko, dass vertrauliche Informationen in die falschen Hände geraten.

Deshalb wurden große Anstrengungen unternommen, um durch zusätzliche Tools wie S/MIME oder PGP (Pretty Good Privacy) Nutzer:innen beim Verschlüsseln von E-Mails zu unterstützen: Um die Effektivität solcher Tools zu bewerten, untersuchten Whitten und

Tygar (1999) die Benutzerfreundlichkeit der Verschlüsselungssoftware von PGP Version 5.0. Die Forscher führten dabei sowohl eine heuristische Evaluation als auch einen Benutzertest durch und kamen zu dem Schluss, dass PGP in dieser Version für die durchschnittlichen Benutzer:innen äußerst schwierig zu verwenden war. Die meisten Benutzer:innen waren nicht in der Lage, die Verschlüsselung korrekt zu konfigurieren und sichere Nachrichten zu senden. Die Gründe für diese Schwierigkeiten lagen in der komplexen Benutzeroberfläche, den unklaren Anweisungen und den fehlenden Hilfestellungen.

Neben der einfachen Bedienung von Sicherheitsmechanismen besteht ein wesentliches Ziel des UPS-Ansatzes darin, das sicherheitsfördernde Verhalten zu motivieren. Eine Methodik besteht in der Anwendung von Nudging. Das Nudging zielt darauf ab, die Entscheidungssituation so zu gestalten, dass ein bestimmtes Verhalten nahegelegt wird, ohne es zu erzwingen.

Im Datenschutz können Nudges auf unterschiedliche Weise das sichere Verhalten fördern. Zum Privacy-Nudging gehört z. B., datenschutzfreundliche Optionen bei einer Dialoggestaltung hervorzuheben oder datenschutzfreundliche Einstellungen „by default“ vorauszuwählen (Cavoukian 2011). Nudging kann auch schon durch die Sortierung einer Liste erfolgen, wenn bspw. eine Liste mit verfügbaren WLANs absteigend nach ihrer Sicherheit sortiert dargestellt wird. Dies erhöht die Wahrscheinlichkeit, dass Verbraucher:innen ein sicheres Netzwerk auswählen, da sie dazu neigen, primär die oberste Option einer Liste zu wählen (Zimmermann und Renaud 2021). Ein weiteres Beispiel für Nudging ist es, direktes Feedback einer (unsicheren) Handlung zu geben (siehe Fallbeispiel unten).

Der Nudging-Effekt kann schließlich auch verstärkt werden, wenn Informationen bereitgestellt werden, die zusätzliches Bewusstsein, aber auch Aufklärung vermitteln und dadurch die Verhaltensanpassung fördern können (Sandfuchs und Kapsner 2018; Zimmermann und Renaud 2021). Diese können z. B. Vorschläge zum sicheren Verhalten sein oder das Aufzeigen möglicher Konsequenzen, die sich durch das Eintreten einer potenziellen Bedrohung ergeben (Jakobi et al. 2019).

4.2 Verbrauchertäuschung und Onlinebetrug

Die Verbrauchertäuschung stellt schon lange einen zentralen Begriff im Verbraucherschutz dar. So ist z. B. in § 123 BGB geregelt, dass ein Vertragsabschluss oder eine Willenserklärung anfechtbar ist, wenn sie durch eine arglistige Täuschung zustande gekommen ist.

Demnach tritt eine Verbrauchertäuschung dann auf, wenn ein Unternehmen oder eine Person absichtlich falsche, irreführende oder betrügerische Informationen bereitstellt oder veröffentlicht hat, um Verbraucher:innen zu täuschen oder irrezuführen. Im Allgemeinen werden folgende Tatbestände dabei als Verbrauchertäuschung gesehen:

- **Falsche oder irreführende Werbeaussagen:** Eine Werbung enthält falsche oder irreführende Informationen über ein Produkt oder eine Dienstleistung.
- **Verschweigen wichtiger Informationen:** Entscheidende Informationen werden absichtlich nicht offengelegt, um Verbraucher:innen in die Irre zu führen.
- **Irreführende Kennzeichnungen und Preisgestaltung:** Kennzeichnungen und Preise eines Produkts sind absichtlich irreführend gestaltet, um falsche Preis- oder Qualitätsvorstellungen zu erwecken.
- **Verwendung gefälschter Testimonials oder Bewertungen:** Verwendung von gefälschten Kundenbewertungen, Erfahrungsberichten oder Testimonials, um einen irreführenden, meist positiven Eindruck zu erwecken.
- **Gefälschte Marken oder irreführende Logos:** Verwendung gefälschter Marken oder Logos, um unberechtigterweise vom Image einer bekannten und angesehenen Marke zu profitieren.

Nudging zur Vergabe eines sicheren Passworts

Ein Beispiel für Nudging zeigt die folgende Abbildung, bei der es um die Vergabe eines sicheren Passworts bei der Eröffnung eines E-Mail-Postfachs geht. Links oben ist dabei ein weniger gut geeignetes Passwort zu erkennen, das durch die orangefarbige Linie signalisiert wird und links unten ein sicheres Passwort. Die Person hat jedoch in beiden Fällen die Möglichkeit, das eingegebene Passwort zu verwenden, so dass eine Wahlmöglichkeit im Sinne des Nudgings besteht. Durch weitere Hinweise und Vorschläge in der Infobox wird die Person zusätzlich darüber aufgeklärt und ermutigt, ein sicheres Passwort zu erstellen.

Fallbeispiel

Eingabemaske zur Passwortvergabe mit Hinweisen zur sicheren Passwortvergabe bei der Eröffnung eines E-Mail-Postfachs.

Der Ausdruck „Verbrauchertäuschung“ ist dabei eng mit dem Begriff „Betrug“ verknüpft, der ein weites Feld von Unwahrheit, Täuschung, Arglist und Unehrlichkeit abdeckt (Beals et al. 2015; Titus et al. 1995; Cross 2020b). So betont der UK Fraud Act (2006), dass der Kern des Betrugsdelikts in der Täuschungsabsicht liegt, d. h., dass der:die Täter:in weiß, dass die Darstellung unwahr und irreführend bzw. dazu angelegt ist, falsch interpretiert zu werden. Hierbei reicht das Vorliegen der vorsätzlichen Täuschung aus, selbst wenn für den Betroffenen kein direkter Schaden entstanden ist (UK Fraud Act 2006).

Bei Betrug und Verbrauchertäuschung müssen wir zwischen dem moralischen Empfinden und der rechtlichen Bewertung unterscheiden, zumal der Übergang zwischen erlaubtem Marketing und UX-Gestaltung hin zu unlauterer Verbrauchertäuschung und kriminellem Onlinebetrug fließend ist.

Ein Merkmal des Betrugs und der Verbrauchertäuschung ist, dass sie absichtlich geschehen. Unabsichtliche Fehler oder Meinungsverschiedenheiten über die Qualität eines Produkts fallen normalerweise nicht unter die Definition der Verbrauchertäuschung. Ein weiteres Merkmal des Betrugs ist es, dass er mit der Absicht geschieht, den anderen arglistig zu täuschen bzw. ihm zu schaden. Diesbezüglich unterscheidet Mujkanovic (2009) zwischen einer positiven und einer negativen Täuschung: „Eine Täuschungshandlung im positiven Sinne läge beispielsweise bei einer liebenswerten Unaufrichtigkeit vor, wenn ein:e Täuschende:r jemandem ein unbegründetes Kompliment machen würde mit der Absicht, dem Getäuschten eine für ihn als schön empfundene Illusion zu bereiten. Bei einer solchen Handlung läge die Absicht des Täuschenden nicht darin, dem:der Getäuschten in irgendeiner Weise zu schaden“ (Mujkanovic 2009).

Auf den ersten Blick ist dies eine sehr spitzfindige Unterscheidung. Für die Verbraucherinformatik ist sie jedoch relevant. Zum Beispiel werden beim UX-Design und beim digitalen Nudging gezielt Gestaltungsprinzipien angewendet, um menschliches Verhalten zu beeinflussen. Hinsichtlich der Ziele kann man beim Nudging zwei Formen unterscheiden:

- **White Nudging:** Positives Nudging bezieht sich darauf, dass Informationen oder subtile Anreize absichtlich so präsentiert werden, dass sie das Verhalten der Menschen in eine gewünschte Richtung lenken, aber dabei nicht notwendigerweise schädlich oder gegen das Interesse des Betroffenen sind; z. B. wenn Produktvergleichsportale datensparsamere Apps als Erstes anzeigen, um die Verbraucher:innen dazu zu ermutigen, weniger Daten von sich preiszugeben.
- **Dark Nudging:** Im Gegensatz dazu bezieht sich negatives Nudging auf die absichtliche Verwendung von irreführenden oder manipulativen Techniken, um Menschen zu täuschen oder in die Irre zu führen, oft zum eigenen Vorteil des Unternehmens oder der Organisation; z. B., wenn die UX-Gestaltung die Nutzer:innen verleiten soll, mehr Informationen über sich preiszugeben.

Insgesamt zeigt sich hier, dass die Bewertung der Täuschungshandlung vom Kontext und von der jeweiligen Intention abhängt, ob die Beeinflussung des Verbraucherverhaltens zu dessen Wohl erfolgt oder nicht. Positive Täuschung und White Nudging können ethisch

sein, wenn sie darauf abzielen, das Wohlbefinden der Verbraucher zu fördern, während negative Täuschung und Dark Nudging in der Regel als unethisch angesehen werden, da sie die Integrität und die Rechte der Verbraucher:innen verletzen können. Ein Beispiel für solches Dark Nudging besteht in der Nutzung von sogenannten Dark Patterns.

4.2.1 Dark Patterns

Dark Patterns sind Designelemente oder -techniken, die absichtlich darauf abzielen, Verbraucher:innen in irreführender oder manipulativer Weise zu beeinflussen, Handlungen auszuführen, die nicht ihren eigentlichen Absichten entsprechen und potenziell zu ihrem Nachteil sind (Brignull 2023).

Sehr häufig werden Dark Patterns im Kontext von E-Commerce und Social Media eingesetzt, aber auch, wenn es um Datensicherheit, Privacy und Zustimmung zur Datensammlung und -verarbeitung geht (Gray et al. 2021; Gunawan et al. 2022). Potenzielle Nachteile für Verbraucher:innen sind (Mathur et al. 2021; Gunawan et al. 2022):

- Verlust von Autonomie und Kontrolle, hauptsächlich in Entscheidungsprozessen
- Finanzielle Nachteile für den Nutzenden selbst oder konkurrierende Unternehmen/Angebote
- Erhöhte Arbeits- und kognitive Belastungen
- Verletzung der Privatsphäre

Dark Patterns waren lange nicht durch die Gesetzgebung reguliert, so dass ein regelrechter Wildwuchs von manipulativen Designs einsetzte. So entstanden unterschiedlichste Formen und Taxonomien von Dark Patterns, die eine Unterscheidung, Kategorisierung und nachhaltige Regulierung bis heute schwierig gestalten (Mathur et al. 2021). Eine der größten Herausforderungen ist die Geschwindigkeit, in der Dark Patterns entstehen und sich verbreiten. Demgegenüber steht der im Vergleich sehr langsame Prozess der Regulierung durch gesetzgebende Verfahren. Außerdem ist der transdisziplinäre Austausch in Forschung, Legislative und Wirtschaft durch die Vielzahl an Taxonomien, Patterneigenschaften, Implementierungen und Bezeichnungen erschwert (Gray et al. 2023).

Aktuelle Bemühungen in der Dark-Patterns-Forschung richten sich also nicht nur auf die weitere Untersuchung solcher Designs bezüglich ihrer Auswirkungen, sondern konzentrieren sich vermehrt auf das Schaffen einer einheitlichen Beschreibung und Klassifizierung. Eine verbreitete Klassifizierung zur Beschreibung und Erklärung von Dark Patterns stammt von Gray et al. (2018). Die Klassifizierung beschreibt fünf unterschiedliche Manipulationsstrategien:

1. **Hartnäckiges Drängen (Nagging)**: wiederholte Aufforderung, bestimmte Aktionen durchzuführen. Nutzende können solche Aufforderungen nicht final ablehnen, sondern haben nur die Option, die Aufforderungen zu einem späteren Zeitpunkt wieder angezeigt zu bekommen.

2. **Behinderung (Obstruction)**: Ein Prozess wird absichtlich schwieriger als notwendig gestaltet, um Nutzende von ihrem Vorhaben abzubringen (z. B. Kündigen eines Vertrags, Löschen eines Accounts).
3. **Verstecken (Sneaking)**: Relevante Informationen verstecken, tarnen oder die Bereitstellung verzögern (z. B. versteckte Kosten). Dadurch wird der Aufwand für den Nutzenden künstlich erhöht.
4. **Schnittstellenmanipulation (Interface Interference)**: Bedienschnittstellen werden so manipuliert, dass einige Optionen oder Aktionen anderen vorgezogen werden (z. B. Vorauswahl von Optionen in Formularen oder Cookie Bannern).
5. **Erzwungene Handlung (Forced Action)**: Nutzende müssen bestimmte Aktionen durchführen, um Zugriff auf eine Website, einen Service oder eine Funktionalität zu erhalten/behalten.

Ein verbreitetes Beispiel für das Forced-Action-Muster sind Cookie Walls bzw. Consent Walls (Gray et al. 2021). Sie erscheinen auf vielen Websites, um Nutzende aufzufordern, der Verwendung von Cookies oder anderen Tracking-Technologien zuzustimmen, bevor sie auf den Inhalt der Website zugreifen können (siehe Abb. 4.7).

Es bietet lediglich zwei Handlungsoptionen: Entweder kann der Nutzende alle Bedingungen, die in der Consent Wall aufgeführt sind, akzeptieren – hier geht es häufig um das Tracken und Zusammenführen von Interaktionen mit besagter Website und von vom Nutzenden bereitgestellte Informationen in Nutzendenprofilen – oder die Bedingungen geschlossen ablehnen. Letzteres allerdings durch Verlassen der Website.

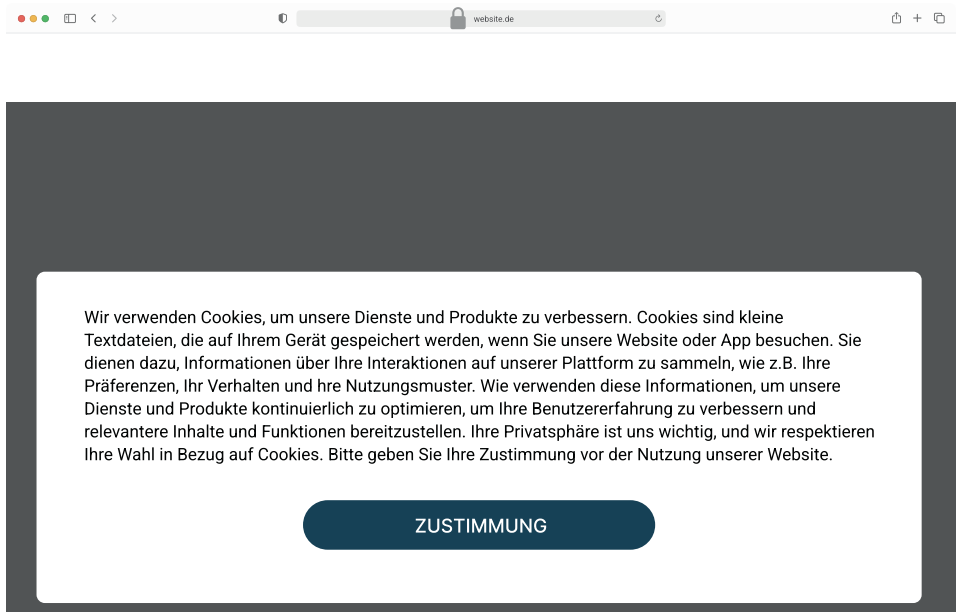


Abb. 4.7 Beispiel der Anwendung des Forced Action Pattern auf einer fiktiven Consent Wall

Consent Walls sind mittlerweile in der EU stark reguliert und in der oben beschriebenen Form durch die DSGVO verboten. So müssen Nutzende zum Beispiel einsehen und auswählen können, welche Daten gesammelt und mit welchen Drittanbietern geteilt werden – das war in der ursprünglichen Form der Consent Wall jedoch nicht möglich.

4.2.2 Onlinebetrug

Der Übergang von der arglistigen Täuschung hin zum kriminellen Betrug ist fließend. Gemeinhin handelt es sich jedoch beim Betrug oft um schwerwiegende Straftaten, während Verbrauchertäuschung sich mehr auf irreführende Praktiken bezieht, die in erster Linie zivilrechtliche Konsequenzen haben.

Durch die Digitalisierung des Alltags von Verbraucher:innen und der Zunahme des Onlinehandels sind auch die Risiken der Internetkriminalität und des Onlinebetrugs gestiegen. So weist z. B. das Bundesamt für Sicherheit in der Informationstechnik (2021) in seinem Bericht zum Digitalen Verbraucherschutz darauf hin, dass durch die Beliebtheit von Internet- und Versandhändlern sowohl die Angriffsflächen für Kriminelle zunehmen als auch die Anzahl potenzieller Opfer von Onlineattacken steigt.

Ein wesentliches Merkmal des Onlinebetrugs ist, dass er digital stattfindet bzw. bei der Durchführung auf digitale Werkzeuge und Infrastrukturen zurückgegriffen wird. So versteht Cross et al. (2014) unter Onlinebetrug betrügerische Handlungen, bei der die Betroffenen auf ein unlauteres oder irreführendes Angebot, eine Nachricht oder eine Einladung im Internet reagieren, was dazu führt, dass sie persönliche Informationen preisgeben oder finanzielle Verluste erleiden.

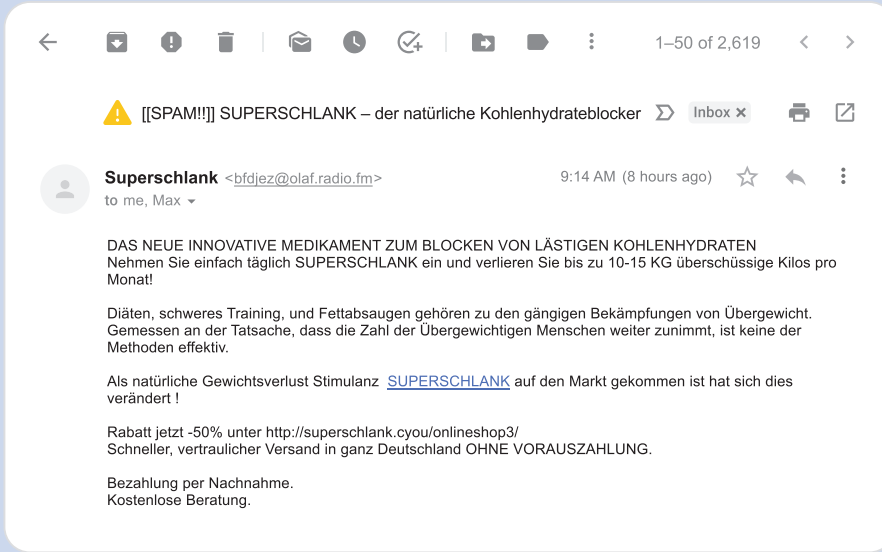
Durch Täuschung und Manipulationstechniken versuchen die Betrüger:innen, Zugang zu Informationen zu bekommen oder die Opfer zu Handlungen zu bewegen, die sie normalerweise nicht ausführen würden. Dies kann die Preisgabe von Passwörtern, die Nutzung unsicherer Zahlungsmethoden oder die Tätigung von Onlinekäufen auf Fakeshops sein. Ein Onlinebetrug kann dabei sowohl finanzielle als auch nicht-finanzielle Schäden oder negative Auswirkungen jeglicher Art für die Betroffenen verursachen.

Die bekannteste Form des Onlinebetrugs besteht sicherlich im Phishing, bei dem die Angreifer:innen versuchen, an sensible Informationen heranzukommen oder Empfänger:innen auf betrügerische Webseiten locken wollen.

Fallbeispiel: Phishing-E-Mail

Die folgende Abbildung zeigt eine typische Phishing-E-Mail. Der Text ist allgemein gehalten und enthält einen Link zu einem (vorgeblichen) Onlineshop, der vermutlich nur dazu dienen soll, an personenbezogene Daten zu kommen. Diese spezielle Phishing-E-Mail zu erkennen ist anhand mehrerer Merkmale möglich: Wie in der Ab-

bildung sichtbar, hat der E-Mail-Provider die E-Mail schon als Spam erkannt und markiert. Des Weiteren wird unter anderem der:die Empfänger:in der E-Mail nicht mit Namen angesprochen, auch dies kann ein Anzeichen für Phishing-E-Mails sein.



Hierbei haben sich viele bekannte Betrugsmaschen der Offline-Welt in die digitale Welt verlagert. Eine Klassifizierung gängiger Formen des Onlinebetrugs wurde von Beals et al. (2015) vorgeschlagen und von Button und Cross (2017) erweitert (vgl. Tab. 4.2).

Die Liste der Betrugsformen ist nahezu endlos und ändert sich ständig, da Betrüger:innen ständig neue Taktiken entwickeln, um Menschen zu täuschen und finanzielle oder persönliche Vorteile zu erlangen. Die fortschreitende Technologie und die Verbreitung des Internets verändern zudem die Möglichkeiten für Betrüger:innen, da sie neue Wege finden, um Opfer zu erreichen und auszunutzen.

Durch das Influencer-Marketing hat z. B. auch die Ausnutzung von Influencer-Praktiken für den Onlinebetrug zugenommen. Ein weiteres Beispiel ist das stärkere Aufkommen von Deep-Fakes durch die Verwendung generativer KI.

Die Klassifizierung der Formen des Onlinebetrugs betont dabei das Ziel und die Art des Betrugs (das „Was“), geht jedoch nicht genauer auf die Umsetzung und die eingesetzten Techniken des Betrugs ein (das „Wie“). Diese prozessorientierte Sicht auf den Onlinebetrug findet man demgegenüber in der Literatur unter dem Begriff „Social Engineering“.

Tab. 4.2 Kategorien und Definitionen der verschiedenen Formen von Onlinebetrug nach Beals et al. (2015) und Button und Cross (2017)

Kategorie	Definition	Beispiele
Produkt- & Dienstleitungsbetrug	Vortäuschung, ein Produkt zu liefern oder eine Dienstleistung anzubieten, die in Wirklichkeit nicht existiert oder keinen Wert hat	• Betrieb von Fake-Shops im Internet oder Online-Marktplätzen • Anbieten von Fake-Produkten • Unberechtigte Rechnungen verschicken
Identitätsbetrug	Durch Täuschung, Hacken und Social Engineering an persönliche und/oder sensible Informationen von Opfern zu gelangen und auf Grundlage dieser Daten und Informationen weitere Straftaten zu begehen	• Mittels gefälschter E-Mails (Phishing) an vertrauliche Information gelangen • Mittels Online-Flirting an Bilder und persönliche Information der Opfer gelangen
Investitionsbetrug	Betrügerische Vortäuschung von Anlagemöglichkeiten und Investitionsgewinn über das Internet	• Gefälschte Kryptowährungsprojekte • Nicht existierende Handels- & Investitionsplattformen • Verbreitung von Ponzi- und Schneeballsystemen auf Social Media und Massen-E-Mails
Inkassobetrug	Betrügerische Aktivitäten, bei denen unrechtmäßige Forderungen oder Gebühren online erhoben werden, oft unter Strafandrohung und dem Vorwand, dass das Opfer eine offene Schuld oder Verbindlichkeit hat	• Falsche Schuldenforderungen • Gefälschte Mahnungen und Inkassobüros • Falsche Steuerbescheide und Aufforderungen, Steuern nachzuzahlen
Gewinnspiel- und Preisbetrug	Das Versprechen eines nicht existierenden Gewinns oder Preises oder eines anderen Geldsegens, der nach gering erscheinender Gegenleistung für die Zahlung ausgezahlt wird	• Gefälschte Lotterien • Erbschaften (nicht existierender) Verwandter • Gefälschte Gutscheine oder Rabattangebote • Gefälschte Gewinnbenachrichtigungen
Wohltätigkeitsbetrug	Betrügerische Aktivitäten, bei denen Personen oder Organisationen vorgeben, wohltätige Zwecke zu unterstützen oder Spenden für wohltätige Zwecke zu sammeln oder falsche Mitgliedschaften werben	• Betrügerisches Ausnutzen der Hilfsbereitschaft bei Katastrophenfällen • Spendenaufrufe für nichtexistierende Organisationen • Spenden-Phishing-Mails, bei denen bekannte Hilfsorganisationen vorgetäuscht werden

(Fortsetzung)

Tab. 4.2 (Fortsetzung)

Kategorie	Definition	Beispiele
Beziehungs- und Vertrauensbetrug	Betrügerisches Vortäuschen und Aufbauen einer persönlichen Beziehung, um das Opfer zu bestimmten Handlungen oder zur Erbringung bestimmter Leistungen zu verleiten	Aufgebautes Vertrauen ausnutzen, um das Opfer darum zu bitten, • Geschenke, Geld oder Gutscheine zu schicken • Bilder zu schicken oder sexuelle Handlungen im Internet zu vollziehen • Gefälligkeiten zu erledigen wie Pakete anzunehmen oder Geld weiterzuleiten
Beschäftigungsbetrug	Betrügerische Aktivitäten im Zusammenhang mit vermeintlichem Anbieten einer Beschäftigung oder Einkommensmöglichkeit, wobei der Wunsch nach Arbeit und Karriere ausgenutzt wird	• Gefälschte Stellenangebote auf Online-Jobplattformen • Angebote zur Heimarbeit im Internet • Fake-Webseiten von Model-Agenturen • Betrügerische Business-Coaching-Onlinekurse

4.3 Social Engineering

Die verschiedenen vorangegangenen Betrugsarten zeigen, dass Kriminelle menschliche Bedürfnisse (z. B. nach Produkten, nach Geldanlagen, nach Liebe etc.) und prosoziales Verhalten (z. B. Menschen in Not zu helfen) systematisch ausnutzen.

Dieses gezielte Ausnutzen menschlicher Bedürfnisse und Verhaltensweisen wird als „Social Engineering“ (im Folgenden auch SE genannt) bezeichnet (Nohlberg 2008; Nohlberg und Kowalski 2008). Der Angreifer versucht dabei, dass Opfer durch Anreize, Mitleid oder Druck zu bestimmten Handlungen zu verleiten. Hierbei bedient der Angreifer sich oft einer falschen Identität und einer erfundenen Geschichte, um seine wahren Absichten zu verbergen und eine glaubhafte Situation vorzutäuschen (Fox 2014).

Jeder Angriff sieht anders aus und erscheint zunächst oft wie eine harmlose Alltagssituation. Dies macht es so schwer, sich gegen Social-Engineering-Angriffe zu wehren. Jedoch gibt es einige wiederkehrende Muster. Die verschiedenen Arten von Social-Engineering-Angriffen können entsprechend den in Abb. 4.8 genannten Kategorien gegliedert werden in:

- **Ziele und Motivation:** bezieht sich auf die Absichten und Beweggründe, mit denen Angreifer:innen Menschen zu täuschen oder manipulieren versuchen
- **Typen und Angriffsstrategien**: bezieht sich auf verschiedene Strategien und den Grad der Digitalisierung des Angriffs
- **Kommunikationsmedien und -kanäle:** beziehen sich auf die verschiedenen Wege und Plattformen, über die Angreifer:innen mit ihren potenziellen Opfern interagieren
- **Manipulationstechniken und Angriffstaktiken:** beziehen sich auf spezifische Taktiken und Tricks, die Angreifer:innen verwenden, um Menschen zu täuschen

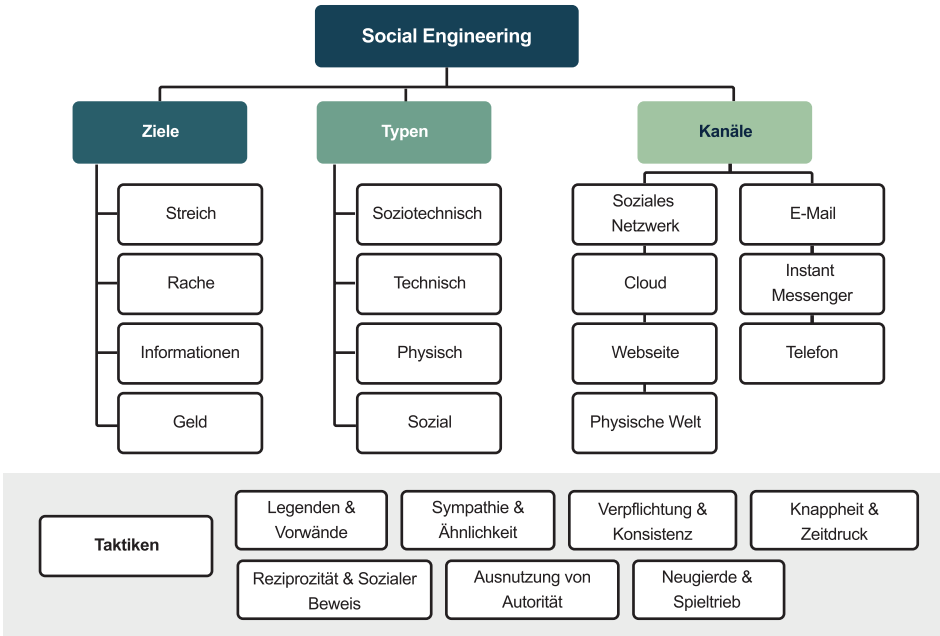


Abb. 4.8 Social-Engineering-Taxonomie (nach: Krombholz et al. 2015); all rights reserved

4.3.1 Ziele und Motivation

Social-Engineering-Angriffe können nach Motivation und Zielen der Angreifer:innen unterschieden werden.

In den Frühzeiten des Hackings ging es häufig einzig darum, sich selbst zu verwirklichen und sein eigenes Können bzw. die Inkompetenz des anderen unter Beweis zu stellen. Im weitesten Sinne lässt sich diese Form unter die Kategorie des **Streichs** ohne böse Absicht fassen. Teilweise wird diese Art von Attacken mit guter Absicht durchgeführt, um Sicherheitslücken aufzuzeigen (Hatfield 2019). Trotz der guten Absichten können solche Angriffe emotionale und technische Schäden beim Opfer zur Folge haben, weshalb auch ethische Abwägungen zu treffen sind (Hatfield 2019).

Eine weitere Motivation stellt **Rache** dar. Sie zielt meist auf die direkte Schädigung des Opfers oder seines Eigentums ab. Hierunter fällt u. a. der digitale Vandalismus, bei dem es z. B. darum geht, Daten des Opfers zu zerstören, seine Geräte und Anwendungen lahmzulegen oder unbrauchbar zu machen. Der:Die Angreifer:in kann auch darauf abzielen, den Ruf des Opfers zu schädigen, das Opfer zu mobben oder es in anderer Weise emotional zu schädigen. Gerade bei Unternehmen ist Rufschädigung ein beliebtes Mittel, um durch gezielte Manipulationen die eigene oder die Reputation eines:einer Konkurrent:in in eine intendierte positive oder negative Richtung zu lenken (Deges 2021).

Eine weitere wesentliche Motivation besteht darin, durch den Angriff **Geld zu verdienen** (Aldawood und Skinner 2019). Dies kann in mannigfaltiger Weise geschehen.

Beim Onlinebetrug geht es z. B. meist darum, das Opfer dazu zu bringen, Geld zu überweisen oder andere Wertgegenstände zu übertragen. Beim Identitätsdiebstahl versucht der:die Betrüger:in, sich die Zugangsdaten zu den Finanz- und Zahlungsdienstleistern zu verschaffen, um so Geld- und Vermögenswerte (meist über Umwege) zu übertragen (Ablon 2018; Aldawood und Skinner 2019).

Die Angriffe können ferner darauf abzielen, unberechtigten **Zugriff auf Systeme und Informationen** zu bekommen. Dieser Zugriff ist meist Mittel zum Zweck, um z. B. das Opfer auszuspähen, es zu erpressen, die Information zu verbrauchen und/oder den Zugang zu den Ressourcen für eigene Zwecke zu nutzen (Van de Merwe und Mouton 2017; Kumar et al. 2015).

Mit den erlangten Informationen (z. B. Firmenpatente oder Information über Verbraucher:innen) wird zunehmend versucht, vom Opfer Geld zu erpressen. Beim Ransomware-Angriff werden z. B. die Daten verschlüsselt, um für die Entschlüsselung Geld zu verlangen.

Beim Identitätsdiebstahl, aber auch beim Beziehungs- und Vertrauensbetrug versucht der:die Angreifer:in, an kompromittierende oder intime Information heranzukommen, um das Opfer hiermit zu erpressen (Cross 2020a).

In der Praxis treten häufig mehrere Motivlagen auf. So kann jemand aus Rache versuchen, komprimierende Informationen über eine andere Person zu erlangen und diese Information aus Gewinninteresse an Dritte verkaufen.

4.3.2 Typen und Angriffsformen

Die Social-Engineering-Angriffe lassen sich weiterhin nach ihrer Angriffsform klassifizieren (Mouton 2018; Mouton et al. 2016). Grob vereinfacht kann man zwischen physischen, sozialen, sozial-technischen und rein technischen Angriffsformen unterscheiden.

Physische Ansätze. Diese Kategorie bezieht sich auf Angriffe, bei denen Angreifer:innen physisch anwesend sind oder reale Interaktionen einsetzen, um sensible Informationen zu sammeln oder sich unbefugten Zugang zu verschaffen. Bei diesen Angriffen werden häufig physische Schwachstellen der Umgebung ausgenutzt. Zu den gängigen physischen Methoden gehören Müllcontainer-Tauchen (Dumpster Diving) bei dem weggeworfene Materialien, z. B. Briefe, Bankkarten und Werbung aus Mülleimern und Müllcontainern entwendet werden, um so mehr Informationen über die Zielperson zu erlangen. Eine andere Methodik ist das Über-die-Schulter-Schauen (Shoulder Surfing), um Passwörter oder PIN-Nummern auszuspähen.

Soziale Ansätze. Diese Kategorie bezieht sich auf das Social Engineering im engeren Sinne, bei dem durch Täuschung und Manipulationstechniken versucht wird, Personen dazu zu bringen, Informationen preiszugeben oder bestimmte Handlungen zu ergreifen.

Technische Ansätze. Technische Ansätze finden in erster Linie in digitalen Räumen statt und nutzen häufig das Internet als Plattform. Diese Angriffe nutzen die mit der Technologie und dem Online-Verhalten verbundenen Schwachstellen aus.

Sozio-technische Ansätze. Erfolgreiche Social-Engineering-Angriffe kombinieren oft mehrere der oben genannten Ansätze. Ein Beispiel dafür sind manipulative Phishing-E-Mails, durch die ein Keylogger auf dem Computer des Opfers installiert wird. Dieser erfasst alle Tastatureingaben. Die Angreifer:innen versuchen dann, sensible Informationen und Passwörter aus den erfassten Daten abzuleiten. Ein weiteres Beispiel ist der sogenannte Köderangriff, bei dem die Angreifer:innen mit Malware infizierte Speichermedien, wie USB-Laufwerke, an strategisch günstigen Orten platzieren, wo sie wahrscheinlich entdeckt werden.

Die verschiedenen Angriffsarten im Social Engineering besitzen jeweils eigene Vor- und Nachteile, die von Angreifer:innen abgewogen werden müssen. So können bei physischen Ansätzen z. B. Schwachstellen vor Ort ausgenutzt werden, oder es wird durch die physische Anwesenheit größerer Druck auf die Zielperson ausgeübt. Meistens vermeiden Angreifer:innen aber den direkten persönlichen Kontakt, um das Entdeckungsrisiko möglichst gering zu halten (Kumar et al. 2015). Außerdem erfordert es mehr Zeit und Aufwand, da Massenangriffe wie beim Phishing nicht möglich sind. Deshalb kennen sich in der Regel Angreifer und Opfer nicht persönlich, damit der:die Angreifer:in unerkannt bleiben kann (Fox 2014).

Die sozialen Ansätze bieten für die Kriminellen den Vorteil, dass eine breite Palette von Manipulationstechniken verwendet und menschliche Schwächen ausgenutzt werden können. Jedoch bedarf es neben sorgfältiger Vorbereitung und Kenntnissen über die Zielperson und den Kontext ausgefeilter Kommunikations- und Überzeugungsfähigkeiten.

Technisch durchgeführte Angriffe sind zu einem hohen Grad automatisierbar und daher weniger personalintensiv. Eine weitere Gefahr von online ausgeführten automatisierten Angriffen (wie Spam, Phishing oder gefälschten Shops) liegt in ihrer Skalierbarkeit. Für den:die Angreifer:in bietet diese Form des Angriffs weiterhin den Vorteil der Anonymität, was das Entdeckungsrisiko minimiert. Diese Angriffsform hängt jedoch davon ab, Schwachstellen und Lücken den digitalen Systemen und Infrastrukturen zu kennen bzw. zu entdecken. Es erfordert deshalb technische Expertise und Computerkenntnisse.

Die sozio-technischen Ansätze stellen die mächtigsten Werkzeuge der Social Engineers dar (Krombholz et al. 2015). Sie sind deshalb besonders wirkungsvoll, da sie sowohl die Schwachstellen der menschlichen Psyche als auch die Schwächen der Technologie ausnutzen, um ihre bösartigen Ziele zu erreichen. Sozio-technische Angriffe sind in der Regel aber in der Planung und Durchführung komplexer und erfordern ein tiefgehendes Verständnis sowohl technischer Sicherheitslücken als auch menschlicher Schwachstellen.

4.3.3 Kommunikationskanäle und -medien

Angreifer:innen können für ihre Angriffe unterschiedliche Kommunikationskanäle und -medien wie z. B. E-Mail, SMS, Website, Social Media usw. verwenden (Krombholz et al. 2015). Bei der Auswahl des richtigen Angriffskanals muss der Angreifer sein Ziel im Auge behalten und dabei die verschiedenen Vor- und Nachteile der einzelnen Kommunikationskanäle gegeneinander abwägen (Tab. 4.3).

Tab. 4.3 Vor- und Nachteile von Kommunikationskanälen aus Sicht der Angreifer:innen

E-Mails	**Vorteile:** E-Mail ist eine weit verbreitete Kommunikationsmethode, bei der viele potenzielle Opfer gleichzeitig erreicht werden können. Durch die E-Mail-Infrastruktur können Betrüger:innen leicht gefälschte Identitäten annehmen und gefälschte E-Mails senden. **Nachteile:** Viele E-Mail-Dienste verfügen über Spam-Filter und Sicherheitsmechanismen, die gefälschte E-Mails erkennen und blockieren können. Zudem sind die meisten Menschen inzwischen vorsichtiger gegenüber verdächtigen E-Mails und öffnen keine unbekannten Anhänge oder Links.
Instant Messenger & Soziale Netzwerke	**Vorteile:** Instant Messenger sind weitverbreitet, ermöglichen eine schnelle Kommunikation in Echtzeit, und die Betrüger:innen können direkt mit ihren Opfern interagieren. Ferner können Betrüger:innen in sozialen Netzwerken Informationen über ihre Ziele sammeln, um personalisierte Angriffe durchzuführen. Auch können Betrüger:innen durch gefälschte Identitäten in Social Media falsches Vertrauen erwecken. Des Weiteren können betrügerische Nachrichten in sozialen Netzwerken große Gruppen erreichen oder als Kommentare gepostet werden, um eine hohe Reichweite zu erzielen. **Nachteile:** Die meisten Instant-Messenger und Social-Media-Dienste erfordern eine Registrierung mit einer Telefonnummer oder E-Mail-Adresse, was die Anonymität einschränken kann. Ferner können Plattformbetreiber verdächtige Aktivitäten analysieren und Konten sperren. Auch sind Menschen zunehmend vorsichtiger bei Nachrichten von unbekannten Kontakten.
Webseite/ Cloud	**Vorteile:** Webseiten sind eine weitverbreitete Kommunikationsmethode, bei der viele potenzielle Opfer gleichzeitig erreicht werden können. Durch die Internet-Infrastruktur können Betrüger:innen mit gefälschten Identitäten leicht anonym Webseiten erstellen. Durch die Nachahmung bekannter Webseiten kann falsches Vertrauen bei den Opfern erzeugt werden. **Nachteile:** Webseiten sind passive Medien, deshalb bedarf es weiterer Strategien, um Opfer auf die Webseite zu locken. Menschen sind oft misstrauisch gegenüber unbekannten Webseiten und Links. Die meisten legitimen Webseiten verfügen über Sicherheitszertifikate, die gefälschte Seiten leichter erkennbar machen.
Telefon & Physische Kontakt	**Vorteile:** Telefonanrufe ermöglichen eine direkte, persönliche Interaktion und können überzeugender wirken als schriftliche Kommunikation. Dies gilt vor allem beim physischen Kontakt. Insbesondere können Betrüger:innen ihre Stimme verstellen oder vorgeben, andere Personen zu sein. Dies wird durch den Fortschritt im Bereich synthetischer Stimmen begünstigt. **Nachteile:** geringe Skalierbarkeit, da die massenhafte Durchführung von Telefonanrufen und insbesondere Hausbesuchen kosten- und zeitaufwendig sind. Die meisten Menschen prüfen die Identität von Anrufern und sind skeptisch gegenüber unbekannten Nummern/Menschen. Ferner besitzen Opfer durch die direkte Interaktion mehr Möglichkeiten, die Glaubwürdigkeit des Anrufers zu prüfen, und es braucht mehr Kompetenz, um eine falsche Identität am Telefon/ beim physischen Kontakt aufrechtzuerhalten. Insbesondere in der physischen Welt sind Menschen oft aufmerksamer und vorsichtiger gegenüber Fremden.

Insgesamt hängen die Erfolgsaussichten von Social Engineering von vielen Faktoren ab, einschließlich der Fähigkeiten des Betrügers und der Vorsicht der Zielpersonen. Neben der Art des Kommunikationskanals spielen des Weiteren auch die eingesetzten Manipulationstechniken eine entscheidende Rolle.

4.3.4 Manipulationstechniken

Angriffe lassen sich auch nach den eingesetzten Manipulationstechniken des Social Engineerings unterscheiden, mit denen das Opfer überzeugt wird, z. B. bestehende Sicherheitsvorschriften oder Schutzmaßnahmen zu missachten. Viele der Techniken haben ihren Ursprung im Marketing (Cialdini 2021), in der Sozialpsychologie (Baumeister und Bushman 2020), der Nudging-Theorie (Leonard 2008) oder dem „persuasive design“ (Fogg 2002). Betrugstechniken missbrauchen diese Forschung zu kriminellen Zwecken, weshalb sie auch als missbräuchlich genutzte Waffen bezeichnet werden (Muscanell et al. 2014; Taib et al. 2019).

Die Liste dabei ist unerschöpflich; daher können hier nur einige grundlegende Techniken und Prinzipien vorgestellt werden:

Sympathie und Ähnlichkeit (*Liking & Similarity*): Dieses Prinzip besagt, dass Personen anfälliger für den Einfluss von anderen sind, die sie mögen, mit denen sie eine gewisse Vertrautheit haben oder Ähnlichkeiten teilen, wie z. B. Geburtsort, Herkunft, Sprache, Hobbys oder andere persönliche Interessen. Ein Beispiel für diese Technik sind Phishing-E-Mails, die vorgeblich von einem:einer Freund:in oder Kolleg:in oder von jemandem mit ähnlichem Hintergrund wie der:die Empfänger:in gesendet wurden.

Knappheit und Zeitdruck (*Scarcity & Urgency*): Dieses Prinzip besagt, dass Personen Gegenstände, die selten, knapp und nur kurz verfügbar sind, als wertvoller wahrnehmen. Durch die Betonung von Knappheit neigen Menschen eher dazu, ein Gefühl der Dringlichkeit zu verspüren und schnell zu handeln. Online-Betrüger:innen nutzen dieses Prinzip, wenn vermeintlich knappe Güter beworben werden, um potenzielle Opfer zu manipulieren.

Reziprozität (*Reciprocity*): Dieses Prinzip besagt, dass Personen dazu neigen, sich verpflichtet zu fühlen, einen Gefallen zu erwidern, wenn ihnen jemand einen Gefallen getan hat. Betrüger:innen können z. B. dem Opfer einen besonderen Rabatt einräumen, jedoch bitten, aus Kostengründen die unsichere Bezahlmethode zu verwenden.

Sozialer Beweis (*Social Proof*): Dieses Prinzip besagt, dass Personen dazu neigen, den Handlungen und Verhaltensweisen anderer zu folgen. Es handelt sich um eine mentale Heuristik, bei der Menschen beeinflusst werden, indem sie beobachten, was andere tun. Betrüger:innen nutzen dieses Prinzip, indem sie gefälschte „Likes“ oder falsche Follower auf sozialen Medienplattformen erstellen oder gefälschte Bewertungen auf Online-Marktplätzen veröffentlichen.

Verpflichtung und Konsistenz (*Commitment & Consistency*): Dieses Prinzip besagt, dass Personen, sobald sie eine kleine anfängliche Verpflichtung eingegangen sind, eher dazu neigen, späteren größeren Anfragen zuzustimmen. Darüber hinaus neigen Menschen dazu, durch anfängliche Erfahrung auf den allgemeinen Charakter einer Person zu schließen. Betrüger:innen nutzen dieses Prinzip, indem sie zunächst kleine Verpflichtungen von ihren Zielpersonen erhalten und eine positive erste Wirkung erzielen. Diese anfängliche Verpflichtung und positive Wirkung beeinflussen die Einstellung des potenziellen Opfers während der weiteren Interaktion.

Falsche Identitäten und Vorwände (*Impersonation & Pretexting*): Dieses Prinzip besagt, dass die Handlung einer Person vor dem Hintergrund des Kontextes gedeutet werden. Betrüger:innen geben deshalb falsche Identitäten vor, die ihnen Glaubwürdigkeit verleihen, und nutzen Vorwände, um Kontakt mit den Opfern aufzunehmen.

Ausnutzung von Autorität (*Authority*): Dieses Prinzip besagt, dass Menschen die natürliche Tendenz haben, vermeintlichen Expert:innen oder Vorgesetzten zu vertrauen und ihnen zu gehorchen. Aus dem Grund geben sich Betrüger:innen auch als Autoritätspersonen aus, um so mehr Druck auf die Zielperson aufzubauen oder sie leichter zu manipulieren.

Neugierde und Spieltrieb (*Curiosity & Playfulness*): Dieses Prinzip setzt auf den natürlichen Spieltrieb und die menschliche Neugier. Betrüger:innen missbrauchen dies, um Menschen zu Handlungen zu verleiten, die sie normalerweise nicht tun würden, z. B. auf verdächtige Links in E-Mails zu klicken oder schädliche Dateien herunterzuladen.

Die verschiedenen Manipulationsstrategien können kombiniert werden, wie z. B. das Nutzen falscher Identitäten mit dem Prinzip der Ähnlichkeit (z. B. als entfernter Verwandter auftreten) oder das Erzeugen eines Gefühls von Knappheit oder Dringlichkeit (z. B. einen Hackerangriff behaupten und die Zielperson auffordern, schnell ihr Passwort zu ändern). In ähnlicher Weise listet Manske (2000) mehrere psychosoziale Strategien auf, die zur Manipulation der Zielperson eingesetzt werden, wie z. B. die Abwälzung der Verantwortung auf die einzelne Zielperson, das Vorspiegeln eines starken moralischen Pflichtgefühls bei der Zielperson, oder ihm:ihr das Gefühl zu geben, die Kontrolle zu haben.

4.3.5 Prozessmodelle

Ein Social-Engineering-Angriff ist keine einzelne Aktion oder Angriffshandlung, sondern stellt vielmehr einen Prozess dar, der mehrere Phasen umfasst (Aldawood und Skinner 2020; Mitnick und Simon 2003). Prozessmodelle im Bereich des Social Engineerings stellen eine strukturierte Darstellung einzelner Schritte dar, die ein:e Angreifer:in oder Betrüger:in durchläuft, um Informationen zu sammeln, Personen zu manipulieren oder betrügerische Aktivitäten durchzuführen.

In der Sicherheitsforschung dienen solche Modelle dazu, das Vorgehen von Angreifer:innen zu verstehen, Schwachstellen zu identifizieren und wirksame Gegenmaßnahmen zu entwickeln. Diesbezüglich lässt sich ein Social-Engineering-Angriff in die Vorbereitungsphase, die Durchführungsphase und die Abschlussphase unterteilen (Bhagyavati 2007).

Vorbereitungsphase (engl. *pre-attack phase*). Diese Phase bezieht sich auf den ersten Abschnitt eines Angriffs. Hier wird der Angriff sorgfältig vorbereitet; es werden potenzielle Ziele identifiziert, Zielpersonen und -objekte ausgekundschaftet und Angriffsstrategien entwickelt. Die Vorbereitungsphase ist entscheidend, da sie die Grundlage für den gesamten Angriff bildet und den Erfolg des:der Angreifers:in bei der Täuschung und Manipulation seiner Ziele maßgeblich beeinflusst. Eine effektive Vorbereitung erhöht die Chancen des:der Angreifers:in, sein Ziel zu erreichen, sei es durch das Sammeln von Informationen über das Ziel, sei es durch das Erkennen von Schwachstellen oder die Auswahl geeigneter Kanäle.

Durchführungsphase (engl. *attack phase*). Diese Phase ist der kritische Moment, in dem der:die Angreifer:in seine manipulativen Fähigkeiten einsetzt, um die Zielpersonen dazu zu bringen, Handlungen auszuführen oder Informationen preiszugeben, die seinen:ihren Zielen dienen. Hierzu gilt es eine Beziehung zur Zielperson aufzubauen und Vertrauen zu schaffen. Dabei nutzt er:sie Erkenntnisse aus der Vorbereitungsphase aus, um die Zielpersonen effektiv zu beeinflussen und die angestrebten Ziele zu erreichen. Idealerweise ist die Täuschung so perfekt, dass die Zielpersonen sich der Manipulation nicht bewusst sind. Die Wirksamkeit dieser Phase bestimmt den Erfolg des gesamten Social-Engineering-Angriffs.

Nachbereitungsphase (engl. *post-attack phase*). Diese Phase wird meist vernachlässigt, jedoch ist sie von entscheidender Bedeutung, da sie es dem:der Angreifer:in ermöglicht, die erzielten Vorteile zu sichern und gleichzeitig die Wahrscheinlichkeit seiner:ihrer Entdeckung zu verringern. Eine effektive Nachbereitung kann dazu führen, dass die Identität des:die Angreifers:in verborgen bleibt und eventuelle Gegenmaßnahmen oder Untersuchungen erschwert bzw. verzögert werden. In dieser Phase gilt es, die Spuren des Angriffs zu verwischen, den erzielten Nutzen zu maximieren, den richtigen Zeitpunkt für den Abgang zu erwischen und unentdeckt zu bleiben. Die Nachbereitung dient auch der Analyse, um aus der gewonnenen Erfahrung Fehler zu vermeiden sowie Angriffstaktiken und -prozesse zu optimieren (Tab. 4.4).

In der Praxis sind die einzelnen Phasen nicht strikt voneinander getrennt, sondern greifen nahtlos ineinander. So können in der Durchführungsphase neue Gegebenheiten und Erkenntnisse auftauchen, so dass Taktiken situativ angepasst und Kanäle gewechselt werden.

So kann in der Vorbereitungsphase ein:e Angreifer:in einen Social-Engineering-Angriff gegen Social-Media-Nutzende planen, um sie auf einen Fake-Shop zu locken. In dieser Phase identifiziert der:die Angreifer:in zunächst die Follower eines bekannten Influencers als potenzielle Ziele. Er:Sie führt eine gründliche Recherche durch, indem er:sie auf öffentlich zugängliche Informationen zugreift, um mehr über die Zielpersonen und deren

Tab. 4.4 Typische Schritte und Merkmale der verschiedenen Phasen

Vorbereitung	• Angriffsformulierung • Zielsetzung und Planentwicklung • Recherche, Ausspionierung und Informationsbeschaffung • Vorbereitung, z. B. durch Analyse der gesammelten Informationen und Untersuchung soziopsychologischer Faktoren • Wahl des richtigen Kanals und Taktikauswahl
Durchführung	• Beziehungen und Vertrauen aufbauen, einschließlich Fälschung der Identität (Bezuidenhout et al. 2010) durch das Tragen einer passenden Maske und das Spielen eines passenden Charakters (Algarni und Xu 2013), • Beziehungen ausnutzen, durch die Wahl des perfekten Zeitpunkts, mentale Tricks und Überredung (Schurz 2008) unter Verwendung professioneller Fertigkeiten (Algarni und Xu 2013)
Nachbereitung	• Verwischen von Spuren • Verwerten von Informationen und Wertgegenstände in Sicherheit bringen • Hinhalten und Gegenmaßnahmen hinauszögern

Präferenzen zu erfahren. Der:Die Angreifer:in erstellt gefälschte Profile in sozialen Medien, um eine glaubwürdige Identität zu schaffen.

In der Durchführungsphase schreibt der:die Angreifende eine gefälschte Direct Message an ausgewählte Follower:innen des Influencers. In der Nachricht gibt er sich als gute:r Bekannte:r des Influencers aus und bietet an, die vom Influencer beworbenen Produkte günstig zu beschaffen. Die Nachrichten sind gut formuliert und erzeugen Druck und Dringlichkeit. Einige Follower:innen reagieren auf die Nachricht und klicken auf den beigefügten Link, da sie glauben, dass sie der Bitte eines Freundes des Influencers Folge leisten.

Nachdem der:die Angreifende die Zahlungseingänge per MoneySafe (einer unsicheren Zahlungsmethode) erhalten hat, verschwindet er:sie vorübergehend vom Radar. Er:Sie löscht die Spuren seiner gefälschten Online-Profile und verwendet Anonymisierungsdienste, um seine:ihre Identität zu verschleiern. Gleichzeitig analysiert er:sie das Verhalten der Betroffenen und sucht nach wertvollen Informationen, die er möglicherweise für zukünftige Angriffe oder für den Verkauf auf dem Schwarzmarkt nutzen kann.

In diesem Beispiel verschmelzen alle drei Phasen nahtlos miteinander. Die Vorbereitungsphase ermöglicht es dem:der Angreifenden, relevante Ziele zu identifizieren und eine glaubwürdige Identität aufzubauen. In der Angriffsphase nutzt der:die Angreifende geschickt seine:ihre gefälschte Identität und manipulative Taktiken, um die Zielperson zu bestimmten Handlungen zu verleiten. Schließlich verschwindet der:die Angreifende in der Nach-Angriffsphase, um seine:ihre Spuren zu beseitigen und den erzielten Nutzen zu bewerten. Dies verdeutlicht, wie ein Social-Engineering-Angriff durch die Koordination dieser Phasen erfolgreich durchgeführt werden kann.

Ein weiteres bekanntes Beispiel sind Spear-Phishing-E-Mails, bei der Information aus der Vorbereitungsphase zur Durchführung des Phishing-Angriffs genutzt wird.

Fallbeispiel: Spear-Phishing-E-Mail

Eine spezielle Art von Phishing-E-Mails ist das Spear-Phishing. Diese E-Mails sind, anders als allgemeine Phishing-E-Mails, schwieriger zu erkennen (siehe folgende Abbildung). Diese E-Mail ist nicht nur namentlich adressiert, sie enthält auch Informationen, die zum potenziellen Opfer passen. Das potenzielle Opfer, Michelle, hat zum Beispiel einen Account bei Sciebo und einen geteilten Ordner, der Verbraucherinformatik heißt und von der Universität Siegen verwaltet wird. Diese Informationen wurden wahrscheinlich in der Pre-Attack-Phase vom Sender der E-Mail gesammelt und in der Attack-Phase genutzt, um das Opfer anfälliger zu machen. Allerdings wurde diese E-Mail 2023 verschickt, und in der E-Mail selbst steht das Jahr 1970.

Des Weiteren ist die URL von Sciebo „Hochschulcloud.nrw“. Diese Kleinigkeiten können übersehen werden, wenn man gestresst ist oder unter Zeitdruck steht. Zuletzt sieht man in der rechten oberen Ecke ein kleines Warndreieck des E-Mail-Providers, das davor warnt, dass die E-Mail Spam und nicht vertrauenswürdig sein könnte. Dies wird auch „Safety by design“ genannt (Harbers et al. 2018).

4.4 Prävention und Resilienz

In der digitalen Welt ist das vollständige Vermeiden von Risiken oft nicht möglich. Stattdessen ist es entscheidend, Risiken zu erkennen und zu bewerten und entsprechende Maßnahmen zu ergreifen.

Hierbei ist das Ziel des Verbraucherschutzes, durch regulatorische und technische Maßnahmen die digitale Welt möglichst sicher für Verbraucher:innen zu gestalten. Gleichzeitig gilt es aber auch das Sicherheitsverhalten von Verbraucher:innen zu stärken. Durch ihr Verhalten und ihre Entscheidungen können sie mit zum Schutz ihrer eigenen Daten und ihrer eigenen Sicherheit beitragen (Helm und Seubert 2020). Deshalb sind ein gutes Sicherheitsverhalten und Risikomanagement im Interesse des:der Einzelnen, um potenzielle Risiken im Vorfeld zu vermeiden bzw. im Schadensfall die finanziellen und psychischen Folgen möglichst zu minimieren.

Aus diesem Grund sind der Aufbau von Sicherheitsprävention und digitale Resilienz wichtige Themen des Verbraucherschutzes. Sicherheitsprävention bezieht sich dabei auf den Schutz und die Stärkung von Verbraucher:innen, um Risiken und Bedrohungen im Vorfeld zu minimieren. Digitale Resilienz bezieht sich ferner auf die Fähigkeit von Verbraucher:innen, auf digitale Bedrohungen zu reagieren und sich von ihnen zu erholen. Dies umfasst die Entwicklung von Fertigkeiten und die Aneignung von Wissen, um digitale Herausforderungen zu bewältigen. Die Kombination von Sicherheitsprävention und digitaler Resilienz kann dazu beitragen, Verbraucher:innen besser vor digitalen Risiken zu schützen und sie in die Lage zu versetzen, mit Bedrohungen umzugehen, wenn sie auftreten.

4.4.1 Sicherheitsprävention

Sicherheitsprävention bezeichnet die systematischen Bemühungen, Gefahren und Risiken in der digitalen Welt proaktiv zu erkennen, zu verhindern oder zumindest zu minimieren. In einer zunehmend vernetzten und digitalisierten Gesellschaft ist Sicherheitsprävention von entscheidender Bedeutung, um persönliche Daten, finanzielle Vermögenswerte und die allgemeine digitale Integrität zu schützen.

Viele Maßnahmen zur digitalen Sicherheitsprävention wurden für den betrieblichen Bereich entwickelt. Im betrieblichen Kontext wird bei der Entwicklung von Schutzmaßnahmen im ersten Schritt die Verwundbarkeit einer Organisation gegenüber Cyberangriffen beziffert (Kumar et al. 2015). Anschließend werden aufgrund der Analyse der Bedrohungslage Maßnahmen entwickelt, mit denen eine Organisation versuchen kann, in den verwundbaren Einheiten ihrer Organisation Angriffe zu verhindern (Wang et al. 2021).

Dieser Ansatz zur betrieblichen Sicherheitsprävention kann teilweise auf den privaten Bereich übertragen werden, allerdings gibt es wichtige Unterschiede zu beachten.

Im betrieblichen Bereich ist die Verwundbarkeit einer Organisation gegenüber Cyberangriffen oft komplexer und umfassender, da es viele Systeme, Mitarbeitende und Daten gibt, die geschützt werden müssen. Zugleich gibt es Abteilungen und geschultes Personal, das für die Gefahrenabwehr verantwortlich ist. Ferner können Betriebe durch Schulungen und Sicherheitsvorgaben stärker Einfluss auf das Verhalten von Mitarbeitenden nehmen.

Dafür sind im privaten Bereich die Sicherheitsanforderungen oft weniger komplex, da Einzelpersonen in der Regel weniger Ressourcen und Daten verwalten als Unternehmen. Im Gegensatz zu Mitarbeitenden können Verbraucher:innen auch nicht verpflichtet werden, an Schulungen und Weiterbildungen teilzunehmen. Jedoch besteht bei Verbraucher:innen eine höhere Eigenmotivation, sich zu schützen, da sie von den Folgen und den Schäden eines Cyberangriffs unmittelbar betroffen sind.

Insgesamt lässt sich der Ansatz zur digitalen Sicherheitsprävention auf den privaten Bereich übertragen, jedoch müssen die spezifischen Bedürfnisse, Motivationen, Ressourcen und Fähigkeiten der Einzelpersonen berücksichtigt werden. Die Grundprinzipien wie die Identifizierung von Verwundbarkeiten und die Entwicklung von Schutzmaßnahmen bleiben jedoch auch im privaten Bereich wichtig, um digitale Sicherheit zu gewährleisten.

4.4.1.1 Verbraucherbildung

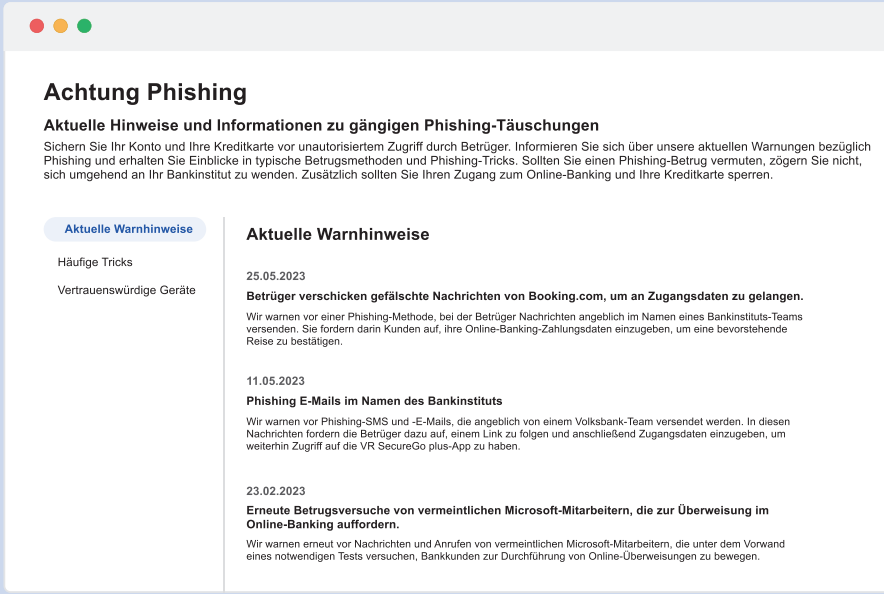
Ein wichtiger Ansatz zur Prävention ist die Bildung und Warnung der Verbraucher:innen über typische Angriffe, Angreifer:innen und deren manipulative Techniken (Fox 2014).

Fallbeispiel

Aufklärung eines Bankinstituts zum Thema Phishing

In der untenstehenden Abbildung sind Meldungen eines Bankinstituts zum Thema Phishing zu sehen. Diese Meldungen werden den Kund:innen zu bestimmten Zeiten angezeigt, wenn sie sich auf der Webseite oder in der App einloggen. Auf der Webseite gibt es dann auch noch die unten abgebildete Tabelle, wo

alle Warnhinweise zum Thema Phishing angezeigt werden und auch Hinweise gegeben werden, wie man Phishing erkennen (unter „Häufige Tricks“) und was man tun kann, um sich zu schützen (unter „Vertrauenswürdige Geräte“). Diese Warnhinweise sind ein typisches Beispiel, wie Sicherheitshinweise aussehen können, das viele große Organisationen auf ihren Plattformen zur Aufklärung über Onlinebetrugsmaschen nutzen.



Prinzipiell kann das Sicherheitstraining den Schutz von Verbraucher:innen erhöhen. Jedoch zeigen Studien, dass die erzielte Schutzwirkung von Warnungen und Sicherheitstrainings nicht sehr hoch ist (Junger et al. 2017; Wang et al. 2021), da die vermittelten Schutzmaßnahmen nur wirksam sind, wenn Menschen sie auch praktisch umsetzen (Jahankhani et al. 2012).

Um die Wirkung und das Sicherheitstraining zu verbessern, muss deshalb bei der Planung genau überlegt werden, worauf eine Intervention abzielen soll (z. B. Verbraucher:innen zu motivieren, nicht auf Links in Phishing-E-Mails zu klicken, nur sichere Bezahlmethoden zu verwenden etc.). Ferner gilt es Faktoren wie Motivation, Wissensstand und Verantwortlichkeitsgefühl, aber auch soziodemografische Faktoren wie Alter und Geschlecht der adressierten Zielgruppe bei der Planung von Interventionen zu berücksichtigen. So haben z. B. Shillair et al. (2015) in einer Versuchsreihe herausgefunden, dass das persönliche Verantwortlichkeitsgefühl einen großen Einfluss auf die Effektivität der Interventionen hat. Allerdings haben sie auch festgestellt, dass dies allein für den Erfolg der Intervention nicht ausreicht. Das Level an Informationen muss schließlich auch dem Wissensstand der Teilnehmer:innen angepasst sein, um effektiv zu sein.

Eine vielgenutzte Theorie für das Planen von Sicherheitstrainings ist die **Protection Motivation Theory (PMT)** (Boehmer et al. 2015; Shillair et al. 2015). Die PMT beschreibt, wie Menschen mit Angststimuli umgehen. Angststimuli werden oft genutzt, um Menschen dazu zu bringen, ihr Verhalten zu ändern. Leider ist Angst als Stimulus nur effektiv, wenn sie nicht zu einer Lähmung führt (Norman et al. 2015). Die PMT postuliert dabei, dass sowohl äußere als auch innere Faktoren die Entstehung von zwei unterschiedlichen kognitiven Prozessen beeinflussen können: die Bedrohungseinschätzung und die Bewältigungsbedeutung.

Die **Bedrohungseinschätzung** ist ein Prozess, bei dem die Individuen interne und externe Belohnungen gegen das wahrgenommene Risiko und ihre Verwundbarkeit abwägen. Dieser Prozess führt zur Bildung einer Bedrohungseinschätzung. Mit anderen Worten: Die Menschen bewerten, wie bedrohlich eine Situation ist, indem sie die möglichen Belohnungen mit den wahrgenommenen Risiken und ihrer eigenen Verwundbarkeit abgleichen.

Die **Bewältigungsbedeutung** hingegen bezieht sich auf einen anderen kognitiven Prozess. Hierbei werden die Effektivität präventiver Maßnahmen und die individuelle Selbstkompetenz berücksichtigt. Diese Faktoren werden verwendet, um die Kosten der präventiven Maßnahmen zu bewerten und die Bewältigungsbedeutung zu ermitteln. Anders ausgedrückt: Die Menschen evaluieren, wie gut sie in der Lage sind, mit der Bedrohung umzugehen und welche Anstrengungen oder Kosten mit der Bewältigung verbunden sind.

Das bedeutet, dass die Motivation, sich zu schützen, gering bleibt, wenn das Risiko als niedrig wahrgenommen und die Verwundbarkeit als gering eingeschätzt wird oder wenn das Selbstvertrauen niedrig ist. Wird das Risiko dagegen als sehr hoch eingeschätzt und die Wirksamkeit von Schutzmaßnahmen als niedrig betrachtet, kann dies zu einer Lähmung führen, bei der keine Notwendigkeit für Schutzmaßnahmen gesehen wird. Daher ist es entscheidend, vor Interventionen zu wissen, wer die Zielgruppe ist und wie sie Risiko, Effektivität und ähnliche Faktoren bewertet. Dies ist jedoch in der Praxis oft schwierig, insbesondere bei Informationskampagnen zum digitalen Verbraucherschutz, die sich oft an große Bevölkerungsgruppen richten und es schwer ist, diese im Voraus zu testen. Es ist wichtig, das Gleichgewicht zwischen Schutz und potenziellem Schaden bei solchen Interventionen zu berücksichtigen.

Warnhinweise und die gezielte Verbraucherbildung stellen wichtige Bausteine der Prävention dar. Es ist jedoch wichtig, dass Sicherheitsinterventionen auf die Zielgruppe abgestimmt werden, um einen positiven Effekt zu erzielen. Da dies aber nicht immer gewährleistet werden kann, gilt es, die Verbraucherbildung mit anderen Präventionsmaßnahmen wie Security-By-Design und automatisierter Betrugserkennung zu kombinieren, um Verbraucher:innen effektiv zu schützen.

4.4.1.2 Betrugserkennung

Die Betrugserkennung stellt eine wichtige Schutzmaßnahme beim digitalen Verbraucherschutz dar. Als Betrugserkennung können die Maßnahmen bezeichnet werden, mit deren Hilfe Täuschungs- und Betrugsversuche identifiziert, registriert und aufgedeckt werden können (Marschall et al. 2015).

Betrugserkennung spielt inzwischen für alle digitalen Betrugsmöglichkeiten eine ausgeprägte Rolle. Häufig genutzte Methoden hierfür sind algorithmische Verfahren, die zunehmend Methoden des maschinellen Lernens (ML) verwenden und mithilfe historischer Daten trainiert werden (Mohawesh et al. 2021). Hierbei lassen sich zwei Ansätze unterscheiden: klassifikationsbasierte und Rating-basierte Verfahren.

Bei der **klassifikatorischen Betrugserkennung** versucht das ML-Modell, die Eingabedaten in eine der zwei vordefinierten Kategorien („Betrugsversuch“ bzw. „Kein Betrugsversuch“) einzuteilen. So kann z. B. der Spam-Filter eines E-Mail-Programms eine Mail als Phishing klassifizieren und automatisch in den Spam-Ordner verschieben. Bei der Klassifizierung können dabei zwei Arten von Fehlern auftauchen. Zum einen der **falsch positive Fehler (False Positives**), bei dem fälschlicherweise ein Betrugsvorfall erkannt wird, obwohl es keiner ist. Die andere Art sind **falsch negative Fehler (False Negatives)**, bei denen ein Betrugsvorfall fälschlicherweise nicht erkannt wird.

Bei der **Rating-basierten Betrugserkennung** versucht das ML-Modell, das Risiko bzw. die Wahrscheinlichkeit anzugeben, dass es sich bei Eingabedaten um einen Betrugsversuch handelt. So kann z. B. die Betrugserkennung bei einem Onlineangebot der Verbraucher:in anzeigen, dass es sich mit 75-prozentiger Sicherheit um einen Betrugsversuch handelt.

Die algorithmische Betrugserkennung zum digitalen Verbraucherschutz wird insbesondere in den folgenden Bereichen genutzt:

- Erkennung betrügerischer E-Mails (Phishing-Mails)
- Erkennung betrügerischer Onlineangebote (Fake Shops/Fake Products)
- Erkennung betrügerischer Kundenbewertungen (Fake Reviews)

4.4.1.2.1 Phishing

E-Mails gehören zu den ältesten und bedeutendsten digitalen Kommunikationskanälen. Neben der gewünschten Nutzung gab es aber auch schon früh diverse Missbrauchsformen, einschließlich Massenwerbung, unerwünschten Nachrichten und auch Phishing-E-Mails. Dabei hat sich der Begriff „Spam“ als Metapher für massenhafte, aufdringliche und betrügerische E-Mails etabliert, die an viele Empfänger:innen gesendet werden.

Die Erkennung betrügerischer Phishing-Angriffe per E-Mail ist deshalb meist Teil sogenannter Spam-Filter. Dies sind Mechanismen, die in E-Mail-Diensten und -Servern implementiert sind, um unerwünschte E-Mails zu erkennen und herauszufiltern. Spam kann verschiedene Formen annehmen, und es gibt verschiedene Verfahren, um Spam von legitimen E-Mails zu unterscheiden. Einige der Verfahren sind

- **Blacklist-Filterung.** Dieser Ansatz verwendet schwarze Listen von bekannten Phishing-Domains, -E-Mail-Adressen und -Inhalten. Wenn eine eingehende E-Mail oder eine Webseite auf einer solchen Liste steht, wird sie blockiert oder als verdächtig markiert.
- **Sender-Authentifizierung.** Dieser Ansatz zielt darauf ab, den Absender einer E-Mail zu identifizieren und seine Berechtigung zum Verschicken der E-Mail zu prüfen. Hierzu

wurden verschiedene Protokolle entwickelt, um die Authentifizierung und Autorisierung bei E-Mails zu ermöglichen.
- **Datenbankbasierte Filterung.** Dieser Ansatz prüft, ob in der E-Mail verdächtige Wörter, URL, Telefonnummern etc. vorkommen, die als Spam eingestuft werden können.
- **Machine-Learning-basierte Filterung.** Bei diesem Ansatz dienen bekannte oder durch generative KI erzeugte Spam- und Phishing-Mails als Trainingsdaten, um durch maschinelles Lernverfahren Spam-Filter zu trainieren.

Kommerzielle Spam-Filter benutzen meist eine Kombination verschiedener Verfahren. Hierbei kommt maschinellen Lernmethoden eine zunehmend wichtige Bedeutung zu.

Neben automatisierten Verfahren gilt es, Kompetenzen von Verbraucher:innen zu stärken, um Phishing-Angriffe zu erkennen und zu verhindern. Die Hauptziele der Verbraucherbildung werden von Franz et al. (2021) wie folgt zusammengefasst:

- **Minimierung von Aufwand und Aufdringlichkeit:** Es ist wichtig, dass Schulungs- und Aufklärungsmaßnahmen für Verbraucher:innen informativ, klar und korrekt sind. Der Aufwand muss angemessen in Bezug zur Effektivität der Maßnahme sein.
- **Unterstützung kognitiver Prozesse:** Es ist wichtig, dass Verbraucher:innen für die Merkmale sensibilisiert werden, an denen sie erkennen können, dass „etwas nicht stimmt“. Hier gilt es die kognitiven Prozesse zu unterstützen, die genutzt werden, um verdächtige Aktivitäten zu erkennen.
- **Aneignung von Schutzmaßnahmen:** Es ist wichtig, dass Verbraucher:innen bei der Aneignung von Sicherheitsfunktionen sowie sicherheitsrelevanten Praktiken und Verhaltensweisen unterstützt werden.

4.4.1.2.2 Fake Shops

Betrügerische Angebote im Internet sind z. B. Fake-Produkte, d. h. gefälschte oder nachgeahmte Produkte, die oft als Imitationen von Markenprodukten oder hochwertigen Waren verkauft werden. Neben einzelnen Produkten existieren auch ganze Online-Shops, die darauf abzielen, Nutzer:innen zu täuschen oder finanziell zu schädigen. Diese sogenannten Fake-Shops bzw. Scam-Shops sind betrügerische Websites, die vorgeben, echte Produkte oder Dienstleistungen zu verkaufen, aber in Wirklichkeit betrügerisch sind.

Es gibt mehrere Ansätze zur Erkennung von Fake-Shops: Sie analysieren die Merkmale, die für das menschliche Auge kaum zu erkennen sind (Beltzung et al. 2020; Carpineto und Romano 2020; Daoud et al. 2020). Hierbei werden Informationen zu mehreren Merkmalen der Betrugserkennung herangezogen, wie z. B.:

- **Analyse der Website-URL:** Die Struktur der Website-URL wird analysiert, um verdächtige Zeichenfolgen oder Subdomains zu identifizieren.
- **Analyse des Webshop-Inhalts:** Der Inhalt der Website, einschließlich der Produktbeschreibungen und Preise, wird auf Unregelmäßigkeiten und Anomalien hin untersucht.

- **Analyse des Webshop-Aussehens:** Erstellung von Screenshots der zu prüfenden Webseiten, die mit Screenshots von bereits als betrügerisch erkannten Fake-Shops verglichen werden, um Ähnlichkeiten festzustellen.
- **Analyse des Web-Quellcodes:** Die Analyse des HTML5-Codes einer Website kann verschiedene Merkmale und Anomalien aufdecken, die auf betrügerische Absichten hinweisen können.
- **Analyse der akzeptierten Zahlungsmethoden:** Die akzeptierten Zahlungsmethoden auf der Website werden überprüft, da betrügerische Websites oft unsichere Zahlungsmethoden verwenden oder Vorauszahlungen verlangen.
- **Analyse von SSL-Zertifikaten:** Die Identifizierung von verbotenen oder risikobehafteten Anbietern auf SSL-Zertifikaten wird verwendet, um verdächtige Domains zu erkennen.
- **Analyse der Preisgestaltung:** Die Preise werden z. B. mit den Durchschnittspreisen für ähnliche Produkte oder Dienstleistungen auf anderen vertrauenswürdigen Websites verglichen. Signifikante Abweichungen können dabei auf betrügerische Absichten hinweisen.

Die Ansätze bieten eine hohe Genauigkeit bei der Identifizierung von Fake-Shops, jedoch besteht immer die Gefahr von sowohl falsch positiven als auch falsch negativen Fehlern. Des Weiteren ist die Betrugserkennung für die Nutzenden nur dann nützlich, wenn sie einen Warnhinweis richtig einordnen können und das Risiko erkennen.

Neben algorithmischen Analysemöglichkeiten gibt es auch spezielle Webseiten, wo Nutzende beliebige URLs, die sie als unsicher betrachten, eingeben können. Auf der Webseite wird ihnen dann angezeigt, ob es sich bei der URL um eine bekannte betrügerische Webseite handelt oder nicht (Beltzung et al. 2020).

4.4.1.2.3 Fake Reviews

Gefälschte Bewertungen oder Rezensionen (auch Fake Reviews oder Opinion Spam) sind unwahre bzw. manipulierte Bewertungen. Sie dienen dazu, in täuschender Absicht den Ruf eines Produkts, einer Dienstleistung, eines Unternehmens oder einer Plattform zu beeinflussen. In der Regel werden gefälschte Bewertungen in drei verschiedene Arten unterteilt: unwahre Bewertungen, Bewertungen zu bestimmten Marken und Nicht-Bewertungen (Jindal et al. 2010; Vidanagama et al. 2020).

Zur Erkennung gefälschter Rezensionen werden maschinelle Lernmethoden vor allem wegen ihrer Skalierbarkeit angewandt und auch, um Merkmale und Muster zu detektieren, die für das Auge der Nutzenden nicht leicht zu erkennen sind (Hussain et al. 2019; Ren und Ji 2019). Bei der Erkennung von gefälschten Bewertungen ziehen die verschiedenen Verfahren unter anderem folgende Merkmale und Kategorien heran:

- **Sprachliche Merkmale.** Auffälligkeiten bei der Verwendung von Adverbien, Adjektiven und Verben in den Bewertungen, die Wortanzahl, die Zeichenzahl, die Anzahl der Sätze, die Aussagekraft des Reviews, die Stimmung des Reviews (z. B. extrem positiv oder extrem negativ) etc.

- **Reviewerbezogene Merkmale.** Auffälligkeiten der Aktivität des:r Reviewer:innen, Anzahl verfasster Bewertungen, Art und Umfang des sozialen Netzwerks des:r Reviewer:innen, Anzahl der Fotos, die der:die Reviewer hochgeladen hat etc.
- **Metadaten-bezogene Merkmale**. Existenz von Duplikaten (d. h. Reviews, die gleich bzw. zu anderen sehr ähnlich sind), Abweichung der Bewertung vom Durchschnitt, Anzahl von Reviews insgesamt bzw. Anzahl der von anderen als nützlich eingestuften Reviews etc.
- **Zeitliche Merkmale.** Auffälligkeiten im zeitlichen Muster, in dem die Bewertungen erstellt wurden, wie z. B. ungewöhnlich viele in kurzer Zeit, Zeitpunkt der Erstellung des Reviews etc.
- **Produktbezogene Merkmale.** Auffälligkeiten im Preis des Produkts, der Produktbeschreibung etc.

Die Verfahren zur automatisierten Fake-Review-Erkennung werden vor allem von Onlineplattformen verwendet. Es gibt auch Webseiten wie ReviewMeta.com, FakeSpot.com oder TheReviewIndex.com, die Verbraucher:innen nutzen können, falls sie sich über zweifelhafte Bewertungen informieren wollen. Diese Webseiten sind jedoch vom Einkaufsprozess abgekoppelt und bedeuten für die Verbraucher:innen einen zusätzlichen Aufwand. Einige dieser Anbieter haben deshalb auch ein Browser-Plugin entwickelt, um Verbraucher:innen während des Online-Shoppens über fragwürdige Anbieter und manipulierte Bewertungen zu informieren. Ein aktueller Forschungszweig im Bereich erklärbare KI untersucht hierbei verschiedene Visualisierungskonzepte, wie eine Analyse der algorithmischen Betrugserkennung transparent, verständlich und vertrauenswürdig angezeigt werden kann (Mohawesh et al. 2021; Mukherjee 2015; Oh und Park 2021).

4.4.2 Digitale Resilienz

Trotz aller Präventionsmaßnahmen werden Verbraucher:innen immer wieder Opfer von Onlinebetrug und Cybercrime-Attacken. Den Zustand bzw. Prozess, wie Opfer ihre jeweilige Situation erleben, wird auch als Viktimisierung bezeichnet (Ybarra et al. 2012). In der Regel erzeugt die Viktimisierung eine stressvolle Situation, die vom Opfer irgendwie bewältigt werden muss – und zwar sowohl praktisch als auch psychisch. Deshalb gilt es, die Robustheit und Widerstandsfähigkeit von Verbraucher:innen gegenüber digitalen Bedrohungen zu stärken. Hierzu muss die Fähigkeit einer Person gefördert werden, auf einen Angriff richtig zu reagieren, die Viktimisierung zu bewältigen, sich zu erholen und sich ggf. an eine neue Situation anzupassen.

4.4.2.1 „Blaming“ und „Shaming“

Neben dem Schaden, der durch den:die Angreifer:in verursacht wurde, ist die Viktimisierung für das Opfer meist auch durch die Stigmatisierung durch andere (engl. „blaming“) und die eigene Scham (engl. „shaming“), etwas falsch gemacht zu haben, belastend.

Es gibt Belege dafür, dass die Meldequote bei Online-Vorfällen sogar noch niedriger ist als bei Betrug in einer Offline-Umgebung (Smith und Budd 2009). Die Gründe für die

Nichtmeldung, das Gefühl der Scham und der Schuld, ein Opfer zu sein, und die Angst vor der Reaktion anderer sind einige der größten Herausforderungen für die Opfer. Ein weiteres häufiges Problem in diesem Zusammenhang ist das Gefühl, dumm gewesen zu sein (Button und Cross 2017) oder nicht zu wissen, wo man sich Hilfe holen kann.

Leider erleben viele Opfer auch ein zusätzliches Trauma durch ihre Familie, Freund:innen und das Strafrechtssystem im Allgemeinen (Button und Cross 2017). Außerdem wird gerade den Opfern von Onlinebetrug sehr oft eine Mitschuld gegeben. Dies verschlimmert den bereits erlittenen Schaden zusätzlich auch noch auf der persönlichen Ebene. Solche Reaktionen können nicht nur von der Öffentlichkeit, sondern auch von den offiziellen Stellen kommen, die sich eigentlich um die Opfer kümmern sollten (Button und Cross 2017).

Des Weiteren kann es dazu kommen, dass dem Opfer explizit und implizit eine gewisse Schuld für seine Viktimisierung zugeschrieben wird (Burgess et al. 2013). So kommuniziert eine Präventionskampagne mit dem Slogan „Du kannst dich schützen“ implizit, dass die Opfer Maßnahmen hätten ergreifen können, um ihre Viktimisierung zu verhindern. Genau solche Aussagen können Schuldzuweisungen und Schamgefühle beim Opfer verstärken.

Fallbeispiel: Blaming und Shaming von Opfern

Luisa K. (Studentin, 22 Jahre) aus Dortmund hat im Juli mehrere neue Kleidungsstücke auf ihrer Lieblingswebseite gekauft und diese mit PayPal bezahlt. Die Produkte sind in zwei Paketen angekommen, und sie hat nicht weiter darüber nachgedacht. Im August bekommt Luisa K. eine E-Mail von PayPal.com, in der gesagt wird, sie müsse noch einen Teil einer Rechnung vom Juli begleichen. In der E-Mail ist ein Link hinterlegt, um zur Zahlung zu gelangen. Da ihre Klamotten in zwei Paketen angekommen sind und der offene Teil der Rechnung mit dem Inhalt des zweiten Pakets übereinstimmen könnte, klickt sie auf den Link.

Das PayPal-Fenster öffnet sich, und sie meldet sich mit Passwort und Nutzernamen an. Jetzt sieht sie, dass die Rechnung schon bezahlt ist und dass die E-Mail nur eine Erinnerung ist „für den Fall, dass man noch nicht bezahlt haben sollte“. Sie loggt sich aus und denkt sich nichts weiter dabei. Ein paar Tage später werden 200 € von PayPal von ihrem Konto abgebucht. Luisa K. setzt sich mit PayPal in Verbindung und bemerkt, dass sie auf einen Betrug hereingefallen ist. Sie sperrt alle Transaktionen und setzt sich mit ihrer Bank in Verbindung. Leider lässt sich die Transaktion nicht rückgängig machen.

Am nächsten Tag spricht sie mit ihrer Familie über den Vorfall. Während ihre Mutter sagt, sie solle zur Polizei gehen, meint ihr Bruder, dass die Polizei nicht nur nichts tun kann, sondern Luisa K. auslachen werde, da sie auf eine Phishing-E-Mail hereingefallen und selber schuld sei, da sie „so dumm ist, auf einen Link in einer E-Mail zu klicken“.

Luisa K. fühlt sich schrecklich dumm und weiß nicht, was sie tun soll und an wen sie sich wenden kann. Schließlich fängt sie an, sich zurückzuziehen, löscht ihre Online-Accounts und geht nicht mehr im Internet einkaufen.

4.4.2.2 Coping-Ansätze

Ein wichtiger Aspekt der digitalen Resilienz ist die Fähigkeit der Stressbewältigung im Falle einer Viktimisierung. Im Englischen wird dies auch als Coping bezeichnet und beschreibt die fortdauernde Auseinandersetzung mit der Situation, um das Gefühl von Stabilität und Sicherheit wiederzuerlangen (Blum et al. 2012). Dies umfasst die emotionale, kognitive und praktische Reaktion, um die stressvolle Situation zu bewältigen, zu tolerieren, zu mildern oder sie zu vermeiden (Lazarus und Launier 1981).

Es umfasst zusätzlich nicht nur den aktiven Umgang mit der Situation, sondern auch passives Verhalten, das der Tolerierung, Milderung oder dem Aushalten der Situation dient. Coping wird hierbei als eine aktive Widerstandskraft gegen stressvolle und aufreibende Situationen verstanden (Endler und Parker 1994). Neben einer mentalen Stärke stellt das finanzielle, soziale und kulturelle Kapital einer Person eine wichtige Ressource zur Bewältigung der Situation dar (Blum et al. 2012).

In der Literatur werden dabei häufig drei verschiedene Copingstrategien unterschieden (Lazarus und Folkman 1984; Stevens et al. 2023):

Problemorientiertes Coping. Diese Strategie setzt auf die aktive Auseinandersetzung mit einem Problem oder einer belastenden Situation, um die Bedrohung zu bewältigen. Sie zielt darauf ab, die Bedrohung zu verändern, sei es durch Einflussnahme auf die Umgebung, auf sich selbst oder auf beides. Dies kann auch in der Vermeidung von stressigen Situationen bestehen, z. B. durch Ablenkung, soziale Zerstreuung, aber auch Vermeidung sozialer Interaktionen. Es gibt aber auch Formen des Copings, die genau umgekehrt die aktive Konfrontation mit der Situation suchen und aktiv Unterstützung annehmen, um mit dem Stress umzugehen.

Ein wichtiger Aspekt des problemorientierten Copings besteht darin, neue Sicherheitsmaßnahmen zu erlernen. In diesem Zusammenhang überlegt die betroffene Person normalerweise, wie groß die Bedrohung ist und ob es sich lohnt, Maßnahmen zur Abwehr zu ergreifen. Deshalb sind in der Regel Personen, die direkt oder indirekt einen Cyberangriff erlebt haben, offener dafür, sich mit Präventionsmaßannahmen auseinanderzusetzen (siehe Abschn. 4.4.1). Wenn es jedoch keine geeigneten Gegenmaßnahmen gibt oder die Bedrohung als unvermeidlich eingestuft wird, kann es zu emotionsorientiertem Coping kommen.

Emotionsorientiertes Coping. Diese Strategie zielt auf die innere Verarbeitung von Emotionen, die in stressigen Situationen auftreten z. B. Angst, Wut, Scham, aber auch Wunschdenken. Die Emotionsregulierung findet meist unbewusst statt. Das emotionale Coping wird häufig durch das Gefühl ausgelöst, die Kontrolle über die Situation zu verlieren und von den eigenen Emotionen überwältigt zu werden. Dies geschieht besonders dann, wenn die Bedrohung als unvermeidlich wahrgenommen wird, entweder weil die ergriffenen Maßnahmen nicht effektiv sind oder weil das Opfer sich nicht in der Lage fühlt, diese umzusetzen.

Eine Form der Stressbewältigung, die auf den ersten Blick irrational erscheinen mag, besteht darin, unangenehme Gefühle zu verdrängen bzw. zu rechtfertigen. Indem das Opfer beispielsweise die Schuld bei sich selbst sucht, erlangt es eine gewisse Kontrolle, da es sich nicht als passives Opfer, sondern als aktive Person sieht, die grundsätzlich die Situation hätte vermeiden können.

Bedeutungstiftendendes Coping. Bei dieser dritten Form bemühen sich die betroffenen Personen, ihre Situation in einen umfassenderen Kontext zu stellen, um einen Sinn oder

etwas Positives darin zu finden. Ein Beispiel dafür beschreiben Blum et al. (2012): Eine Frau wurde mit der Tatsache konfrontiert, dass ihre Schwester an Brustkrebs erkrankt war. Um besser mit dieser Situation umzugehen, entschied sich die Frau, eine Wohltätigkeitsstiftung zu gründen. Auf diese Weise konnte sie zumindest einen Sinn im Tod ihrer Schwester finden.

Diese Erkenntnisse zur Psychologie der Stressbewältigung helfen besser zu verstehen, wie Opfer psychologisch und emotional mit den Folgen ihrer Viktimisierung umgehen. Insbesondere zeigt dieser Forschungszweig, dass Cybercrime und Onlinebetrug nicht ein technisches Problem bzw. nur finanzielle Verluste verursachen, sondern auch erheblichen Stress und emotionale Belastung bei den Betroffenen hervorrufen können (Green et al. 2010). Dieses erweiterte Verständnis ist von großer Bedeutung, da es ermöglicht, geeignete Unterstützungsangebote für Opfer zu entwickeln. Diese Angebote sollten nicht nur materielle Hilfe und praktische Maßnahmen zur Schadensbegrenzung umfassen, sondern auch psychologische Unterstützung bieten, um den Opfern bei der Bewältigung des emotionalen Stresses zu helfen. Insgesamt trägt die Berücksichtigung der psychologischen Aspekte der Viktimisierung dazu bei, Opfern von Onlinebetrug ganzheitlichere Unterstützung zukommen zu lassen.

4.5 Zusammenfassung

Dieses Kapitel hat gezeigt, dass Verbraucher:innen Spuren in nahezu allen Bereichen und Lebensräumen hinterlassen. Besonders der stetig wachsende digitale Lebensraum ist voll von Informationen und Daten. Durch die Allgegenwärtigkeit datensammelnder Dienste und Geräte, wie das Smartphone, durchdringen diese immer tiefer auch die analogen Bereiche des Lebens. Das Kapitel hat Auswirkungen auf Privatsphäre durch diese Datensammlung untersucht, sowie die resultierenden Gefahren für Cyberkriminalität. Es wurden Wege aufgezeigt, wie Verbraucher:innen sensibilisiert und befähigt werden können, um sich selbst, ihre Privatsphäre und ihre Daten zu schützen. Außerdem haben wir einen Überblick darüber gegeben, welche Arten von Cyberkriminalität es gibt und was darunter verstanden wird. Hierbei wurde auf Verbraucherschutz, Privatsphäre, und die verschiedenen Arten des Onlinebetrugs eingegangen. Nicht zuletzt gab das Kapitel einen Einblick in die „Digitale Resilienz“ von Verbraucher:innen sowie verschiedenen Präventions- und Bewältigungsstrategien, die Opfer verwenden.

4.6 Übungen

1. Begriff Privatsphäre: Was versteht man unter Privatsphäre im Allgemeinen und unter informationeller Privatheit im Speziellen?
2. Privacy by Design: Was sind die Grundsätze des Privacy-by-Design-Ansatzes? Beschreiben Sie diese kurz und erklären Sie, wie sie sich von den Methoden der Privacy Enhancing Technologies unterscheiden.
3. Verbraucherrechte und DSGVO: Was sind die vier zentralen Verbraucherrechte, die in der DSGVO festgeschrieben sind? Beschreiben Sie diese kurz.

4. Risiken Datenmissbrauch: Was sind Risiken beim digitalen Verbraucherschutz? Nennen Sie bitte fünf mögliche Risikofaktoren und beschreiben Sie diese kurz. Veranschaulichen Sie diese außerdem anhand von Beispielen aus dem Alltag.
5. Datenschutz Dritter und Unbeteiligter: Welche Herausforderungen bestehen beim Schutz der Privatsphäre von Dritten (Besuchern, Haushaltsmitgliedern, Unbeteiligte)? Welche Rechte stehen ihnen zur Verfügung?
6. Onlinebetrug: Was sind die 8 Kategorien von Onlinebetrug, und wie werden sie definiert?
7. Onlinebetrug: Warum gibt es keine All-in-one-Musterlösung für den Umgang mit Onlinebetrug?
8. Erkennung von Onlinebetrug: Welche Möglichkeiten neben technisch-algorithmischen Möglichkeiten gibt es, um „Fake Shops“ zu erkennen?
9. Social Engineering: Was genau versteht man unter Social Engineering, und wie unterscheidet es sich von klassischen Onlinebetrugsarten?
10. Verbraucherschutz: Was wird unter „Victim Blaming“ verstanden? Was unter „Shaming“?
11. Nennen und erläutern Sie drei Ziele von Social Engineering.
12. Nennen und erläutern Sie drei typische Methoden des Copings.

Literatur

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. 2015. „Keys under doormats: Mandating insecurity by requiring government access to all data and communications“. *Journal of Cybersecurity*: tyv009. https://doi.org/10.1093/cybsec/tyv009.

Ablon, Lillian. 2018. „Data thieves“. *The motivations of cyber threat actors and their use and monetization of stolen data*. Aussage vor dem House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, am 15. März 2018.

Acquisti, Alessandro, und Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine* 3(1): 26–33. https://doi.org/10.1109/MSP.2005.22.

Acquisti, Alessandro, und Jens Grossklags. 2007. What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technologies and Practices* 18:363–377.

Aldawood, Hussain, und Geoffrey Skinner. 2019. A taxonomy for social engineering attacks via personal devices. *International Journal of Computer Applications* 975:8887.

———. 2020. An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications* 177(30): 1–11.

Aldenhoff, Christian. 2019. „Legitimation von Datenverarbeitung via AGB? Wider eine Verlagerung von datenschutzrechtlichen Abwägungen in das Vertragsrecht“. In *Digitalität und Privatheit*, Christian Aldenhoff, Lukas Edeler, Martin Hennig, Jakob Kelsch, Lea Raabe, und Felix Sobala, 37–62. Bielefeld: transcript Verlag. https://doi.org/10.14361/9783839446614-004.

Algarni, Abdullah, und Yue Xu. 2013. Social engineering in social networking sites: Phase-based and source-based models. In *International Journal of E-Education, e-Business, e-Management and e-Learning*, Bd. 3, 456–462. International Association of Computer Science and Information Technology (IACSIT). https://eprints.qut.edu.au/220650/. Zugegriffen am 03.04.2023.

Alizadeh, Fatemeh, Timo Jakobi, Jens Boldt, und Gunnar Stevens. 2019. „GDPR-reality check on the right to access data: Claiming and investigating personally identifiable data from companies“.

In *Proceedings of Mensch Und Computer 2019 on – MuC'19*, 811–814. Hamburg: ACM Press. https://doi.org/10.1145/3340764.3344913.

Baumeister, Roy F., und Brad J. Bushman. 2020. *Social psychology and human nature*. Cengage Learning. Belmont, CA: Thomson Higher Education.

Beals, Michaela, Martha Deevy, Debbie Deem, Keith Anderson, und Robert Anguizola. 2015. „Framework for a taxonomy of fraud", Financial Fraud Research Center, S.40.

Beltzung, L., A. Lindley, O. Dinica, N. Hermann, und R. Lindner. 2020. „Real-time detection of fake-shops through machine learning". In *2020 IEEE International Conference on Big Data (Big Data)*, 2254–2263. https://doi.org/10.1109/BigData50022.2020.9378204.

Belz, J. 2018. *„Verbraucher-Scoring: Repräsentativbefragung zur Akzeptanz und Kenntnis über (neuartige) Scoring-Methoden". Repräsentativbefragung*. Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz. https://www.infas.de/publikationen/verbraucher-scoring-repraesentativbefragung-zur-akzeptanz-und-kenntnis-ueber-neuartige-scoring-methoden/. Zugegriffen am 03.04.2023.

Bezuidenhout, Monique, Francois Mouton, und H. S. Venter. 2010. „Social engineering attack detection model: SEADM". *2010 Information Security for South Africa*: 1–8. https://doi.org/10.1109/ISSA.2010.5588500.

Bhagyavati, B. 2007. „Social engineering". Chapter. In *Cyber warfare and cyber terrorism*. IGI Global. https://doi.org/10.4018/978-1-59140-991-5.ch023.

Blankertz, Aline, und Louisa Specht. 2021. „Wie eine Regulierung für Datentreuhänder aussehen sollte". Policy-Brief. Juli. Berlin: Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/sites/default/files/regulierung_fuer_datentreuhaender.pdf. Zugegriffen am 14.02.2022.

Blum, S., M. Brow, und R. Silver. 2012. „Coping". In *Encyclopedia of human behavior*, Hrsg. Vilayanur S. Ramachandran, Bd. 2, 596–601. Elsevier. https://books.google.nl/books?hl=nl&lr=&id=yASuxMCuhKkC&oi=fnd&pg=PT218&dq=ramachandran+encyclopedia&ots=7nI39WAy7n&sig=WPdK9qd7uxJPQ9Pn0vGagCHc2Ks&redir_esc=y#v=onepage&q=ramachandran%20encyclopedia&f=false. Zugegriffen am 03.04.2023.

BMUV. 2023. „Digitaler Verbraucherschutz". Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz. 2023. https://www.bmuv.de/WS6914. Zugegriffen am 03.04.2023.

Boehmer, Jan, Robert LaRose, Nora Rifon, Saleem Alhabash, und Shelia Cotten. 2015. Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology* 34(10): 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448.

Brignull, Harry. 2023. *Deceptive patterns: Exposing the tricks tech companies use to control you*. Testimonium Ltd.

Bundesamt für Sicherheit in der Informationstechnik. 2021. „Bericht zum Digitalen Verbraucherschutz 2020". Bundesamt für Sicherheit in der Informationstechnik (BSI).

Burgess, A., C. Regehr, und A. Roberts. 2013. *Victimology theories and applications*, 2. Aufl. Burlington: Jones and Bartlett Learning.

Button, Mark, und Cassandra Cross. 2017. *Cyber frauds, scams and their victims*. London: Routledge. https://doi.org/10.4324/9781315679877.

Carpineto, Claudio, und Giovanni Romano. 2020. An experimental study of automatic detection and measurement of counterfeit in brand search results. *ACM Transactions on the Web* 14(2): 1–35. https://doi.org/10.1145/3378443.

Cavoukian, Ann. 2009. „The 7 foundational principles". https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Zugegriffen am 03.04.2023.

———. 2011. „Privacy by Design – Die 7 Grundprinzipien". Ontario. Https://web.archive.org/web/20130617053037/; https:/www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-german.pdf. Wayback Machine. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-german.pdf. Zugegriffen am 03.04.2023.

Cena, Federica, Silvia Likavec, Amon Rapp, und Alessandro Marcengo. 2016. „An ontology for quantified self: Capturing the concepts behind the numbers“. In *Proceedings of the 2016 ACM international joint conference on pervasive and ubiquitous computing: Adjunct*, 602–4. Heidelberg: ACM. https://doi.org/10.1145/2968219.2968329.

Cialdini, Robert B. 2021. *Influence, new and expanded: The psychology of persuasion*. HarperCollins.

Cross, Cassandra. 2020a. Romance Fraud. In *The Palgrave handbook of international cybercrime and cyberdeviance*, Hrsg. Thomas J. Holt und Adam M. Bossler, 917–937. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_41.

———. 2020b. ‘Oh, we can’t actually do anything about that’: The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice* 20(3): 358–375. https://doi.org/10.1177/1748895819835910.

Cross, Cassandra, Russell G. Smith, und Kelly Richards. 2014. Challenges of responding to online fraud victimisation in Australia. *Trends and Issues in Crime and Criminal Justice* 474:1.

Daoud, Eduard, Vu Dang, Hung Nguyen, und Martin Gaedke. 2020. Improving fake product detection using AI-based technology. In *Proceedings of the 18th international conference on E-society (ES 2020)*, 119–125. IADIS Press. https://doi.org/10.33965/es2020_202005L015.

Davies, B. 2010. „Why privacy by design is the next crucial step for privacy protection“. https://www.semanticscholar.org/paper/Why-Privacy-by-Design-is-the-next-crucial-step-for-Davies/7ffc32552027757110ad60b3ae701148b702f706. Zugegriffen am 03.04.2023.

Deges, Frank. 2021. Juristische Aspekte der Artikulation und Publikation von Bewertungen. In *Bewertungssysteme im E-Commerce: Mit authentischen Kundenbewertungen Reputation und Umsatz steigern*, Hrsg. Frank Deges, 121–143. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-34493-1_4.

Diercks, Nina. 2016. Big Data-Analysen & Scoring in der (HR-)Praxis. *PinG Privacy in Germany* 1:11. https://doi.org/10.37307/j.2196-9817.2016.01.11.

Dinev, Tamara, und Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17(1): 61–80.

Djeffal, Christian. 2019. ‚Privatheit 4.0‘ im Spiegel von Recht und künstlicher Intelligenz. Das Recht als (Re)aktion und der status activus technicus. In *Privatsphäre 4.0, Eine Neuverortung des Privaten im Zeitalter der Digitalisierung*, 177–197. https://doi.org/10.1007/978-3-476-04860-8_11.

Dogruel, Leyla, und Sven Joeckel. 2019. Risk perception and privacy regulation preferences from a cross-cultural perspective. A qualitative study among German and U.S. smartphone users. *International Journal of Communication* 13(0): 20.

Endler, Norman S., und James D. A. Parker. 1994. Assessment of multidimensional coping: Task, emotion, and avoidance strategies. *Psychological Assessment* 6(1): 50.

Endres, Johannes. 2013. „Dienste und Software zum Verbergen der IP-Adresse“. *c’t Security 2013*, Juli, 120–22.

European Network and Information Security Agency. 2014. *Privacy and data protection by design: From policy to engineering*. LU: Publications Office. https://data.europa.eu/doi/10.2824/38623. Zugegriffen am 03.04.2023.

Fogg, B. J. 2002. Persuasive technology: Using computers to change what we think and do. *Ubiquity* 2002(December): 2. https://doi.org/10.1145/764008.763957.

Fox, Dirk. 2014. Social Engineering im Online-Banking und E-Commerce. *Datenschutz und Datensicherheit – DuD* 38(5): 325–328.

Franz, Anjuli, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, und Joachim Vogt. 2021. „SoK: Still plenty of Phish in the sea – A taxonomy of user-oriented phishing interventions and avenues for future research“. In Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021), S. 339–358.

Fuchs-Heinritz, Werner, Hrsg. 2013. *Lexikon zur Soziologie*, 5., überarb. Aufl. 2011. Wiesbaden: Springer VS.

Garfinkel, Simson, und Heather Richter Lipford. 2014. *Usable security: History, themes, and challenges*, Synthesis lectures on information security, privacy and trust 11. San Rafael: Morgan & Claypool Publishers.

Geeng, Christine, und Franziska Roesner. 2019. „Who's in control?: Interactions in multi-user smart homes". In *Proceedings of the 2019 CHI conference on human factors in computing systems – CHI '19*, 1–13. Glasgow: ACM Press. https://doi.org/10.1145/3290605.3300498.

Gerber, Paul, Melanie Volkamer, und Karen Renaud. 2015. Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *ACM SIGCAS Computers and Society* 45(1): 16–21. https://doi.org/10.1145/2738210.2738214.

Gerber, Paul, Melanie Volkamer, und Nina Gerber. 2017. Das Privacy-Paradoxon – Ein Erklärungsversuch und Handlungsempfehlungen. In *Dialogmarketing Perspektiven 2016/2017*, Hrsg. DDV Deutscher Dialogmarketing Verband e.V., 139–167. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-16835-3_8.

Ghaiumy Anaraky, Reza, Kaileigh Angela Byrne, Pamela J. Wisniewski, Xinru Page, und Bart Knijnenburg. 2021. „To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults". In *Proceedings of the 2021 CHI conference on human factors in computing systems*, 1–14. Yokohama, Japan: ACM. https://doi.org/10.1145/3411764.3445204.

Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt, und Austin L. Toombs. 2018. The dark (patterns) side of UX Design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, 1–14. Montreal: ACM. https://doi.org/10.1145/3173574.3174108.

Gray, Colin M., Cristiana Santos, Nataliia Bielova, Michael Toth, und Damian Clifford. 2021. Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI conference on human factors in computing systems*, 1–18. Yokohama: ACM. https://doi.org/10.1145/3411764.3445779.

Gray, Colin M., Cristiana Santos, und Nataliia Bielova. 2023. Towards a preliminary ontology of dark patterns knowledge. In *Extended abstracts of the 2023 CHI conference on human factors in computing systems*, 1–9. Hamburg: ACM. https://doi.org/10.1145/3544549.3585676.

Green, Diane L., Jung Jin Choi, und Michael N. Kane. 2010. Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behavior in the Social Environment* 20(6): 732–743.

Gunawan, Johanna, Cristiana Santos, und Irene Kamara. 2022. Redress for dark patterns privacy harms? A case study on consent interactions. In *Proceedings of the 2022 symposium on computer science and law*, 181–194. Washington: ACM. https://doi.org/10.1145/3511265.3550448.

Habermas, Jürgen. 2015. *Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft; mit einem Vorwort zur Neuauflage 1990*, Suhrkamp-Taschenbuch Wissenschaft 891, 14. Aufl. Frankfurt a. M.: Suhrkamp.

Hafiz, Munawar. 2006. A collection of privacy design patterns. In *Proceedings of the 2006 conference on pattern languages of programs*, 1–13. Portland: ACM. https://doi.org/10.1145/1415472.1415481.

Harbers, Maaike, Mortaza Bargh, Ronald Pool, Jasper Van Berkel, Susan Van den Braak, und Sunil Choenni. 2018. *A conceptual framework for addressing IoT threats: Challenges in meeting challenges*. http://hdl.handle.net/10125/50166. Zugegriffen am 03.04.2023.

Hatfield, Joseph M. 2019. Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security* 83(Juni): 354–366. https://doi.org/10.1016/j.cose.2019.02.012.

Helm, Paula, und Sandra Seubert. 2020. Normative paradoxes of privacy: Literacy and choice in platform societies. *Surveillance and Society* 18(2): 185–198. https://doi.org/10.24908/ss.v18i2.13356.

Hornung, Gerrit. 2014. „Datenverarbeitung der Mächtigen bleibt intransparent". *Legal Tribune Online* (blog). https://www.lto.de/recht/hintergruende/h/bgh-urteil-vizr15613-schufa-scoring-ermittlung-kreditwuerdigkeit-algorithmus-geschaeftsgeheimnis-auskunft/. Zugegriffen am 29.01.2014.

Hussain, Naveed, Hamid Turab Mirza, Ghulam Rasool, Ibrar Hussain, und Mohammad Kaleem. 2019. Spam review detection techniques: A systematic literature review. *Applied Sciences* 9(5): 987. https://doi.org/10.3390/app9050987.

ISO. 2018. „DIN EN ISO 9241-11:2018-11, Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte". Beuth Verlag GmbH. https://doi.org/10.31030/2757945.

Jahankhani, Hossein, Thulasirajh Jayaraveendran, und William Kapuku-Bwabw. 2012. Improved awareness on fake websites and detecting techniques. In *Global security, safety and sustainability & e-democracy*. Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering, Hrsg. Christos K. Georgiadis, Hamid Jahankhani, Elias Pimenidis, Rabih Bashroush, und Ameer Al-Nemrat, 271–279. Berlin: Springer. https://doi.org/10.1007/978-3-642-33448-1_36.

Jakobi, Timo, Sameer Patil, Dave Randall, Gunnar Stevens, und Volker Wulf. 2019. It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26(1): 1–44.

Jakobi, Timo, Gunnar Stevens, Maximilian von Grafenstein, Dominik Pins, und Alexander Boden. 2020. User-friendly formulation of data processing purposes of voice assistants: A user perspective on the principle of purpose limitation. In *Proceedings of the Conference on Mensch Und Computer*, 361–372. Magdeburg: ACM. https://doi.org/10.1145/3404983.3405588.

Jindal, Nitin, Bing Liu, und Ee-Peng Lim. 2010. Finding unusual review patterns using unexpected rules. In *Proceedings of the 19th ACM international conference on information and knowledge management–CIKM'10*, Bd. 1549. Toronto: ACM Press. https://doi.org/10.1145/1871437.1871669.

Junger, Marianne, Lorena Montoya, und F.-J. Overink. 2017. Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior* 66:75–87.

Karaboga, Murat, Philipp K. Masur, Tobias Matzner, Cornelia Mothes, Maxi Nebel, Carsten Ochs, Philip Schütz, und Hervais Simo Fhom. 2014. „Selbstdatenschutz". White Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Karlsruhe: Forum Privatheit. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/White_Paper_Selbstdatenschutz_Forum_Privatheit.pdf?_=1421924480. Zugegriffen am 03.04.2023.

Keber, Tobias O. 2018. Stützen der Informationsgesellschaft – zur Rolle von Datenschutz und Datensicherheit im Mediensystem. In *Privatheit in der digitalen Gesellschaft*, Hrsg. Steffen Burk, Martin Hennig, Benjamin Heurich, Tatiana Klepikova, Miriam Piegsa, Manuela Sixt, und Erik Trost, 261–288. Berlin: Duncker & Humblot.

Kerwin, Jason T. 2012. „"Rational fatalism": Non-monotonic choices in response to risk". *Working Paper*, Nr. WGAPE Spring 2012: 70.

Kokolakis, Spyros. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64(Januar): 122–134. https://doi.org/10.1016/j.cose.2015.07.002.

Krasnova, Hanna, und Natasha F. Veltri. 2010. Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii international conference on system sciences*, 1–10. IEEE.

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, und Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and Applications* 22:113–122.

Kuhn, Axel. 2019. Reader Analytics: Vom privaten zum öffentlichen Lesen? In *Digitalität und Privatheit*, Hrsg. Christian Aldenhoff, Lukas Edeler, Martin Hennig, Jakob Kelsch, Lea Raabe, und Felix Sobala, 263–282. Bielefeld: transcript Verlag. https://doi.org/10.14361/9783839446614-014.

Kumar, Anshul, Mansi Chaudhary, und Nagresh Kumar. 2015. Social engineering threats and awareness: A survey. *European Journal of Advances in Engineering and Technology* 2(11): 15–19.

KunstUrhG. 1907. *Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie*. *KunstUrhG*. https://www.gesetze-im-internet.de/kunsturhg/index.html. Zugegriffen am 03.04.2023.

Lazarus, Richard S., und Susan Folkman. 1984. *Stress, appraisal, and coping*. New York, NY: Springer

Lazarus, Richard S., und Raymond Launier. 1981. Stressbezogene Transaktionen zwischen Person und Umwelt. In *Stress: Theorien, Untersuchungen, Maßnahmen. Bern:* Huber 213:259.

Leonard, Thomas C. 2008. Richard H. Thaler, Cass R. Sunstein, Nudge: Improving decisions about health, wealth, and happiness. *Constitutional Political Economy* 19(4): 356–360. https://doi.org/10.1007/s10602-008-9056-2.

Li, Ming, Wenjing Lou, und Kui Ren. 2010. Data security and privacy in wireless body area networks. *IEEE Wireless Communications* 17(1): 51–58. https://doi.org/10.1109/MWC.2010.5416350.

Limerick, Hannah, David Coyle, und James W. Moore. 2014. The experience of agency in human-computer interactions: A review. *Frontiers in Human Neuroscience* 8(August). https://doi.org/10.3389/fnhum.2014.00643.

Mainzer, Klaus. 2018. Digitale Würde? Sensoren, Roboter und Big Data zwischen Selbstorganisation und Selbstbestimmung. In *Privatheit in der digitalen Gesellschaft*. Duncker & Humblot. https://mediatum.ub.tum.de/node?id=1481122. Zugegriffen am 05.08.2023.

Manske, Kurt. 2000. An introduction to social engineering. *Information Systems Security* 9(5): 1–7. https://doi.org/10.1201/1086/43312.9.5.20001112/31378.10.

Marschall, Timm, David Morawitzky, Marco Reutter, Raphaele Schwartz, und Henning Baars. 2015. „Netzwerkanalysen für die Betrugserkennung im Online-Handel“. *Wirtschaftsinformatik Proceedings 2015*, März. https://aisel.aisnet.org/wi2015/124

Masur, Philipp K., Doris Teutsch, und Tobias Dienlin. 2018. Privatheit in der Online-Kommunikation. In *Handbuch Online-Kommunikation*, Hrsg. Wolfgang Schweiger und Klaus Beck, 1–29. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-18017-1_16-1.

Mathur, Arunesh, Mihir Kshirsagar, und Jonathan Mayer. 2021. What makes a dark pattern … dark?: Design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI conference on human factors in computing systems*, 1–18. Yokohama: ACM. https://doi.org/10.1145/3411764.3445610.

Matzner, Tobias. 2018. Der Wert informationeller Privatheit jenseits von Autonomie. In *Privatheit in der digitalen Gesellschaft*, Hrsg. Steffej Burk, Martin Hennig, Benjamin Heurich, Tatiana Klepikova, Miriam Piegsa, Manuela Sixt, und Erik Trost, 75–94. Berlin: Duncker & Humblot.

Mause, Karsten. 2019. „Schutz der (digitalen) Privatsphäre als Staatsaufgabe? Eine politökonomische Analyse“. https://doi.org/10.25969/MEDIAREP/13277.

McDonald, Aleecia M., und Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *A Journal of Law and Policy for the Information Society 4(3): 540–565*.

Meng, Nicole, Dilara Keküllüoğlu, und Kami Vaniea. 2021. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction* 5(CSCW1): 1–29. https://doi.org/10.1145/3449119.

Millham, Mary Helen, und David Atkin. 2018. Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society* 20(1): 50–67. https://doi.org/10.1177/1461444816654465.

Mitnick, Kevin D., und William L. Simon. 2003. *The art of deception: Controlling the human element of security*. Indianapolis, Ind.: John Wiley & Sons.

Mohawesh, Rami, Xu Shuxiang, Son N. Tran, Robert Ollington, Matthew Springer, Yaser Jararweh, und Sumbal Maqsood. 2021. Fake reviews detection: A survey. *IEEE Access* 9:65771–65802. https://doi.org/10.1109/ACCESS.2021.3075573.

Mouton, Francois. 2018. *Social engineering attack detection model*. University of Pretoria (South Africa) ProQuest Dissertations Publishing, 2018. 30709891.

Mouton, Francois, Louise Leenen, und Hein S. Venter. 2016. Social engineering attack examples, templates and scenarios. *Computers & Security* 59:186–209.

Mühlhoff, Rainer. 2021. Predictive privacy: Towards an applied ethics of data analytics. *Ethics and Information Technology* 23(4): 675–690.

Mujkanovic, Samir. 2009. *Kreditkartenbetrug aus soziologischer Sicht: Erscheinungsformen, Trends und Ursachen*. diplom.de. https://books.google.com/books?hl=de&lr=&id=JSlrAQAAQBAJ&oi=fnd&pg=PA6&dq=T%C3%A4uschenden++nicht+darin,+dem+Get%C3%A4uschten+in+irgendeiner+Weise+zu+schaden&ots=WEXiGP0txc&sig=z46eJfQ1LhycChSUegHiPy6YT00. Zugegriffen am 05.08.2023.

Mukherjee, Arjun. 2015. Detecting deceptive opinion spam using linguistics, behavioral and statistical modeling. In *Proceedings of the 53rd annual meeting of the association for computational linguistics and the 7th international joint conference on natural language processing: Tutorial abstracts*, 21–22. Beijing: Association for Computational Linguistics. https://doi.org/10.3115/v1/P15-5007.

Muscanell, Nicole L., Rosanna E. Guadagno, und Shannon Murphy. 2014. Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass* 8(7): 388–396.

Niksirat, Salehzadeh, Evanne Anthoine-Milhomme Kavous, Samuel Randin, Kévin Huguenin, und Mauro Cherubini. 2021. 'I thought you were okay': Participatory design with young adults to fight multiparty privacy conflicts in online social networks. In *Designing Interactive Systems Conference 2021*, 104–124. Virtual Event: ACM. https://doi.org/10.1145/3461778.3462040.

Nohlberg, Marcus. 2008. „Securing information assets: Understanding, measuring and protecting against social engineering attacks". PhD Thesis, Institutionen för data-och systemvetenskap.

Nohlberg, Marcus, und Stewart Kowalski. 2008. „The cycle of deception: A model of social engineering attacks, defenses and victims". In: Proceedings of the Second International Symposium on Human Aspects of Information Security and Assurance (HAISA 2008), S. 1–11

Norberg, Patricia A., Daniel R. Horne, und David A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41(1): 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x.

Norman, Paul, Henk Boer, und Erwin R. Seydel. 2015. Protection motivation theory. In *Predicting and changing health behaviour: Research and practice with social cognition models*, Hrsg. Mark von Conner und Paul Norman, 81–126. Maidenhead: Open University Press.

Oh, Yu Won, und Chong Hyun Park. 2021. Machine cleaning of online opinion spam: Developing a machine-learning algorithm for detecting deceptive comments. *American Behavioral Scientist* 65(2): 389–403. https://doi.org/10.1177/0002764219878238.

Petrlic, Ronald, Christoph Sorge, und Wolfgang Ziebarth. 2023. Einführung in den Technischen Datenschutz. In *Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie*, 9–27. Wiesbaden: Springer.

Pins, Dominik, Alexander Boden, Britta Essing, und Gunnar Stevens. 2020. ‚Miss Understandable': A study on how users appropriate voice assistants and deal with misunderstandings. In *MuC '20: Proceedings of the Conference on Mensch und Computer*, 349–359. Magdeburg: Association for Computing Machinery. https://doi.org/10.1145/3404983.3405511.

Pins, Dominik, Timo Jakobi, Alexander Boden, Fatemeh Alizadeh, und Volker Wulf. 2021. Alexa, we need to talk: A data literacy approach on voice assistants. In *Designing interactive systems conference 2021*. DIS '21, 495–507. New York: Association for Computing Machinery. https://doi.org/10.1145/3461778.3462001.

Pins, Dominik, Timo Jakobi, Gunnar Stevens, Fatemeh Alizadeh, und Jana Krüger. 2022. Finding, getting and understanding: The user journey for the GDPR'S right to access. *Behaviour & Information Technology* 41(10): 2174–2200. https://doi.org/10.1080/0144929X.2022.2074894.

Recki, Lena, Margarita Esau-Held, Dennis Lawo, und Gunnar Stevens. 2023. AI said, she said – How users perceive consumer scoring in practice. In *Mensch Und Computer 2023*, 149–160. Rapperswil: ACM. https://doi.org/10.1145/3603555.3603562.

Reiter, Julius, und Olaf Mehner. 2016. Scoring-Verfahren. Datenschutzrechtliche Grenzen und praktische Schwierigkeiten. In *Tagungsband Herbstakademie 2016*, Hrsg. Jürgen Taeger, 453–468. Edewecht.

Ren, Yafeng, und Donghong Ji. 2019. Learning to detect deceptive opinion spam: A survey. *IEEE Access* 7:42934–42945. https://doi.org/10.1109/ACCESS.2019.2908495.

Rössler, Beate. 2001. *Der Wert des Privaten*, Suhrkamp Taschenbuch Wissenschaft 1530, 1. Aufl. Frankfurt a. M.: Suhrkamp.

Rost, Martin. 2013. Zur Soziologie des Datenschutzes. *Datenschutz und Datensicherheit – DuD* 37(2): 85–91. https://doi.org/10.1007/s11623-013-0023-3.

Rost, Martin, und Kirsten Bock. 2011. Privacy by Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen. *Datenschutz und Datensicherheit – DuD* 35(1): 30–35. https://doi.org/10.1007/s11623-011-0009-y.

Sandfuchs, Barbara, und Andreas Kapsner. 2018. Privacy nudges. In *Privatheit in der digitalen Gesellschaft*, Hrsg. Steffen Burk, Martin Hennig, Benjamin Heurich, Tatiana Klepikova, Miriam Piegsa, Manuela Sixt, und Kai Erik Trost, Bd. 10, 319–338. Duncker & Humblot. http://www.jstor.org/stable/j.ctv1q69v1n.17. Zugegriffen am 05.08.2023.

Sasse, M. Angela, Matthew Smith, Cormac Herley, Heather Lipford, und Kami Vaniea. 2016. Debunking security-usability trade-off myths. *IEEE Security and Privacy* 14(5): 33–39. https://doi.org/10.1109/MSP.2016.110.

Schurz, G. 2008. Patterns of abduction. *Synthese* 164(2): 201–234. https://doi.org/10.1007/s11229-007-9223-4.

Seele, Peter, und Chr. Lucas Zapf. 2017. *Die Rückseite der Cloud*. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-54758-8.

Shillair, Ruth, Shelia R. Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, und Nora J. Rifon. 2015. Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior* 48(Juli): 199–207. https://doi.org/10.1016/j.chb.2015.01.046.

Sixt, Manuela. 2018. Scoring. Implikationen für Individuum und Gesellschaft. In *Privatheit in der digitalen Gesellschaft*, Hrsg. Steffej Burk, Martin Hennig, Benjamin Heurich, Tatiana Klepikova, Miriam Piegsa, Manuela Sixt, und Erik Trost. Berlin: Duncker & Humblot.

Smith, Russell G., und Carolyn Budd. 2009. Consumer fraud in Australia: Costs, rates and awareness of the risks in 2008. *Trends and Issues in Crime and Criminal Justice/Australian Institute of Criminology* 382:1–6. https://doi.org/10.3316/agispt.20095363.

Stevens, und Paul Bossauer. 2017. Dealing with personal data in the age of big data economies. *Zeitschrift Für Geistiges Eigentum* 9(3): 266. https://doi.org/10.1628/186723717X15069451170856.

Stevens, Gunnar, und Alexander Boden. 2022. „Warum wir parteiische Datentreuhänder brauchen", In *Zu treuen Händen (Vortragsreihe),* Verbraucherzentrale NRW e.V.. https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-06-stevens-boden-warum-wir-parteiische-datentreuhaender-brauchen.pdf. Zugegriffen am 05.06.2023.

Stevens, Gunnar, Alexander Boden, Fatemeh Alizadeh, Timo Jakobi, Michelle Walther, und Jana Krüger. 2023. Wie gehen Verbraucher:innen mit Onlinebetrug um? – Eine Literaturübersicht. In *Handbuch Cyberkriminologie 2*. Cyberkriminologie – Theorien, Methoden, Erscheinungs-

formen, Hrsg. Thomas-Gabriel Rüdiger und P. Saskia Bayerl, 533–554. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-35442-8_42.

Such, Jose M., und Natalia Criado. 2018. Multiparty privacy in social media. *Communications of the ACM* 61(8): 74–81. https://doi.org/10.1145/3208039.

Taeger, Jürgen. 2016. Scoring in Deutschland nach der EU-Datenschutzgrundverordnung. *Zeitschrift für Rechtspolitik* 49(3): 72–75.

Taib, Ronnie, Yu Kun, Shlomo Berkovsky, Mark Wiggins, und Piers Bayl-Smith. 2019. Social engineering and organisational dependencies in phishing attacks. In: *IFIP conference on human-computer interaction*, 564–584. Springer.

Titus, Richard M., Fred Heinzelmann, und John M. Boyle. 1995. Victimization of persons by fraud. *Crime & Delinquency* 41(1): 54–72. https://doi.org/10.1177/0011128795041001004.

UK Fraud Act. 2006. „Fraud Act 2006“. Text. Statute Law Database. 2006. https://www.legislation.gov.uk/ukpga/2006/35/contents. Zugegriffen am 05.08.2023.

Universität Oldenburg. 2018. „Social Scoring“. Gehalten auf der Informatik und Gesellschaft 2018/19 Social Scoring. http://www.informatik.uni-oldenburg.de/~iug18/soc/China.html#fn1. Zugegriffen am 05.08.2023.

Van de Merwe, Johan, und Francois Mouton. 2017. Mapping the anatomy of social engineering attacks to the systems engineering life cycle. In *Proceedings of the eleventh international symposium on human aspects of information security & assurance (HAISA 2017)*. CSCAN.

Verbraucherzentrale Bundesverband e.V. 2020. „Neue Datenintermediäre – Anforderungen des vzbv an ‚Personal Information Management Systems‘ (PIMS) und Datentreuhänder“. Positionspapier. Berlin. https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf. Zugegriffen am 05.08.2023.

Vidanagama, Dushyanthi U., Thushari P. Silva, und Asoka S. Karunananda. 2020. Deceptive consumer review detection: A survey. *Artificial Intelligence Review* 53(2): 1323–1352. https://doi.org/10.1007/s10462-019-09697-5.

Wang, Zuoguang, Hongsong Zhu, und Limin Sun. 2021. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access* 9:11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633.

Warren, Samuel D., und Louis D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4(5): 193–220. https://doi.org/10.2307/1321160.

Westin, Alan Furman. 2015. *Privacy and freedom*. New York: IG Publishing.

Whitten, Alma, und J. Doug Tygar. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *USENIX security symposium* 348:169–184.

Wiele, Johannes, und Bettina Weßelmann. 2017. Anonymität als soziokulturelle Inszenierung. In *Informationelle Selbstbestimmung im digitalen Wandel*, Hrsg. Michael Friedewald, Jörn Lamla, und Alexander Roßnagel, 109–130. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-17662-4_8.

Wiesner, Barbara. 2021. *Private Daten: Unsere Spuren in der digitalen Welt*, Digitale Gesellschaft, Bd. 35, 1. Aufl. Bielefeld: transcript Verlag. https://doi.org/10.14361/9783839456057.

Witt, Bernhard C. 2010. *Datenschutz kompakt und verständlich*. Wiesbaden: Vieweg+Teubner Verlag.

Xie, Wenjing, Amy Fowler-Dawson, und Anita Tvauri. 2019. Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology* 38(7): 742–759. https://doi.org/10.1080/0144929X.2018.1552717.

Ybarra, Michele L., Danah Boyd, Josephine D. Korchmaros, und Jay (Koby) Oppenheim. 2012. Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health* 51(1): 53–58. https://doi.org/10.1016/j.jadohealth.2011.12.031.

Zimmermann, Verena, und Karen Renaud. 2021. The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction* 28(1): 1–45. https://doi.org/10.1145/3429888.

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (http://creativecommons.org/licenses/by/4.0/deed.de) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.