Kapitel 1
Grundlagen

I. Begriff der Identität

Für eine Untersuchung der Problematik des Identitätsdiebstahls und Identitätsmissbrauchs sind die Begriffe der „Identität“ sowie des „Diebstahls“ und des „Missbrauchs“ einer Identität grundlegend. Daher werden diese Begriffe nachfolgend kurz erörtert und für die Zwecke dieser Untersuchung definiert.

1. Divergierende Begriffe der Identität

Der Begriff der Identität ist schillernd[1] und hat in den verschiedenen Disziplinen unterschiedliche Bedeutung. Die ersten Überlegungen zum Identitätsbegriff entstammen der Philosophie, auch hier wurden und werden unterschiedliche Begriffe verwendet.[2]

Auch im Hinblick auf Identitäten im Internet divergieren die Beschreibungen von „Identität“. Einige aktuelle Zitate aus verschiedenen Bereichen zeigen, dass mit dem Begriff der Identität jeweils ein ähnliches Anliegen verfolgt wird, aber diesem durchaus unterschiedliche, disziplinspezifische Verständnisse des Begriffs zugrunde liegen.

- „An identity is any subset of attributes of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as ‚the identity‘, but several of them.“[3]
- „Eine Identität ist eine in ihrem Verwendungskontext eindeutige, wiedererkennbare Beschreibung einer natürlichen oder juristischen Person oder eines Objektes, die sich aus Attributen und einem Identitätsbezeichner zusammensetzt.“[4]

---

[1] *J. Meyer*, S. 9.

[2] Siehe einen kurzen Überblick bei *Höffe*, S. 2 ff.

[3] *Pfitzmann/Hansen*, S. 29.

[4] BITKOM-Leitfaden zu Web-Identitäten, Oktober 2005.

G. Borges et al., *Identitätsdiebstahl und Identitätsmissbrauch im Internet,*
DOI 10.1007/978-3-642-15833-9_1, © Springer-Verlag Berlin Heidelberg 2011

- „Identität ist die Summe derjenigen Merkmale, anhand derer ein Individuum von anderen unterschieden werden kann.“[5]
- „Bei der Identität, die im Fokus steht, geht es um die kommunikativ zugängliche Repräsentanz einer Person.“[6]
- „Der Begriff Identität bezeichnet eigentlich nur die Zuordnung eines Bezeichners […] zu einer Entität (Person), die […] bei der Geburt der Person festgelegt wird und dann als definiertes Bündel von Eigenschaften gilt, mit dem verglichen wird.“[7]
- „In der Begriffswelt des Identitätsmanagements werden mit einer Person verkettete Identifier wie Namen, Adressen, Bitfolgen etc. als deren partielle Identitäten verstanden. Die partiellen Identitäten […] bestimmen in wesentlichen Teilen und unmittelbar die Identität dieser Person.“[8]
- „Ein Individuum kann in den Augen anderer nur dann Einheitlichkeit und Kontinuität besitzen, wenn es von diesen wiedererkannt wird; je nach der Form des Wiedererkennens und der Informationen, über die die Anderen bereits verfügen, verändert sich auch die Identität des Individuums. Identität ist damit der Weg, auf dem der Einzelne mit der Gesellschaft interagiert.“[9]
- „Rechtlich bezeichnet Identität die Übereinstimmung personenbezogener Daten mit einer natürlichen Person.“[10]

In Bezug auf die technische Darstellung von Identitäten oder in Bezug auf das Internet wird häufig der Begriff der „digitalen Identität“ verwendet. Auch hier sind die Definitionen nicht einheitlich, wie nachfolgende Beispiele zeigen:

- „Eine digitale Identität ist definiert als ein eindeutiger, digitaler Identifikator, dem personifizierende Attribute zugeordnet sein können.“[11]
- „Geht man von der Identität eines Menschen mit all ihren Facetten aus, ist dessen digitale Identität die Untermenge dessen, was technisch abgebildet wird.“[12]
- „Eine digitale Identität ist eine Identität, die von einem Rechner verstanden und verarbeitet werden kann.“[13]
- „Digital identity denotes attribution of attributes to an individual person, which are immediately operationally accessible by technical means.“[14]

Die Beispiele zeigen, dass die Untersuchung nicht auf ein interdisziplinär einheitliches Verständnis der Identität zurückgreifen kann.

---

[5] *Mezler-Andelberg*, S. 9.

[6] *Hansen/Krasemann/Rost/Genghini*, DuD 2003, 551.

[7] *Bräuer*, DuD 2005, 24.

[8] *Rost/Meints*, DuD 2005, 216, 217.

[9] *Hornung*, S. 31.

[10] *Meints*, DuD 2006, 576.

[11] *Baier*, S. 39.

[12] *Hansen/Meissner*, S. 22.

[13] BITKOM-Leitfaden zu Web-Identitäten, Oktober 2005.

[14] *Pfitzmann/Hansen*, S. 30.

2. *Begriff der Identität im rechtlichen Sinne*

Ein einheitlicher Begriff der Identität im rechtlichen Sinn existiert nicht.[15] Das Gesetz verwendet den Begriff meist im Sinne von Identifizierung.[16] Ein strafrechtliches Beispiel ist etwa § 163b StPO, der von der „Feststellung der Identität" spricht. Ein Beispiel aus dem Zivilrecht ist § 312c Abs. 1 S. 2 BGB. Danach hat der Unternehmer dem Verbraucher bei der Kontaktaufnahme „seine Identität […] offen zu legen". Das Gesetz geht aber auch teilweise von einem anderen Verständnis aus. So wird in einer Reihe von Normen von der „sexuellen Identität" gesprochen,[17] womit die sexuelle Orientierung gemeint ist.[18]

Der Begriff der Identität wurde aus rechtlicher Sicht bisher nur selten untersucht. Die erste umfassende Untersuchung des Begriffs der Identität und ihres rechtlichen Schutzes in Bezug auf die elektronische Kommunikation liegt nunmehr in Form einer aktuellen Bochumer Dissertation von *Julia Meyer* zur Identität und ihrem Schutz im Internet[19] vor. *J. Meyer* unterscheidet auf der Grundlage einer Auseinandersetzung mit den in der Psychologie und Soziologie verwendeten Identitätsbegriffen aus rechtlicher Sicht in Bezug auf die Identität natürlicher Personen im Internet drei Begriffe: die numerische Identität, die soziale Identität und die virtuelle Identität.

Numerische Identität einer natürlichen Person ist die „erkennbare Übereinstimmung von Dateien mit einer einzigen Person".[20] Der Sache nach wird dieser Begriff auch in anderen Definitionen in diesem Sinne verstanden, etwa in den oben genannten Definitionen von *Bräuer* und *Meints*.[21] Diejenigen Daten, die geeignet sind, eine Person von allen anderen zu unterscheiden (zu identifizieren), bezeichnet *J. Meyer* als „Identitätsdaten".[22]

Der Begriff der sozialen Identität, der vor allem in der Psychologie und in den Sozialwissenschaften Bedeutung hat,[23] wird danach als „Übereinstimmung von subjektivem Inneren, der Selbstwahrnehmung, und gesellschaftlichem Außen, der Wahrnehmung durch Andere", definiert.[24]

---

[15] *J. Meyer*, S. 12.

[16] *J. Meyer*, S. 12.

[17] Etwa in §§ 1, 19 Abs. 1, 20 Abs. 1 S. 1 und Abs. 2, 33 Abs. 3 S. 1 AGG, § 8 Abs. 1 S. 1 BBG, § 75 Abs. 1 BetrVG, § 19a S. 1 SGB IV, § 1 Abs. 1 SoldGG.

[18] *J. Meyer*, S. 12; *Roloff*, in Rolfs/Giesen/Kreikebohm/Udsching, § 1 AGG Rz. 9; *Schlachter*, in ErfKomm, § 1 AGG Rz. 13.

[19] *Julia Meyer*, Identität und virtuelle Identität natürlicher Personen im Internet. Schutz durch besondere Persönlichkeitsrechte und das Allgemeine Persönlichkeitsrecht, Diss. Bochum 2010.

[20] *J. Meyer*, S. 15.

[21] Siehe oben Fn. 7 u. 10.

[22] *J. Meyer*, S. 16.

[23] *J. Meyer*, S. 43 ff.

[24] *J. Meyer*, S. 45 m. w. Nachw.; vgl. auch *Gerhard*, S. 43; *Henrich*, in Marquard/Stierle, S. 134; *Oerter/Dreher*, in Oerter/Montada, S. 291; *Peifer*, S. 7; *Teichert*, S. 4; Brockhaus Band 13, "Ich-Identität".

Der Begriff der virtuellen Identität wird vor allem in den Sozialwissenschaften verwendet.[25] Aus rechtlicher Sicht definiert *J. Meyer* diesen Begriff als „ein Nutzerprofil einer Person, das auf Dauer angelegt ist, konsistent genutzt wird und daher für andere Nutzer wiedererkennbar ist, ohne dass die dahinterstehende natürliche Person erkennbar ist."[26]

Für die vorliegende Untersuchung ist vor allem der Begriff der numerischen Identität von Interesse, der in gleicher Weise auch auf juristische Personen und sonstige Rechtsträger anwendbar ist.

3. Identitätsbegriff der Studie

Der Identitätsbegriff der Studie sollte sich nach dem Zweck der Studie richten. Gegenstand der Analyse sind das Sichverschaffen und das missbräuchliche Verwenden von Bezeichnungen im Rechtsverkehr, die zur eindeutigen Unterscheidung und Adressierung von Personen benutzt werden. Dies sind klassischerweise Namen sowie heute deren moderne technische Äquivalente; im allgemeinsten Sinn: personenbezogene (aber das ist hier selbstverständlich) Daten.

Die Studie verwendet – als Arbeitsgrundlage, ohne Anspruch auf abschließende wissenschaftliche Klärung der Begrifflichkeiten – folgende Begriffe:

- Identifizierung einer Person: eindeutige Bestimmung einer Person i. S. einer numerischen Abgrenzung von anderen Personen,
- Identität einer Person: Menge an Daten, durch die eine Person in einem bestimmten Zusammenhang eindeutig bezeichnet und von anderen unterschieden werden kann.

Beispiel:
Person: der Mensch Erich Mustermann; Identität mit beispielsweise den Merkmalen = Daten „Name" Erich Mustermann, „Geburtsdatum" 15.3.1954, „Augenfarbe" grau/blau, „Körpergröße" 182 cm, „Wohnanschrift" Hauptstraße 5, 6755 Heusenstamm.

Diese Identität wird der konkreten Person zugewiesen. Die Person wird mit der Identität „Erich Mustermann" bestimmt und von anderen Personen unterschieden.

Mit diesem Verständnis ist die „Identität" zunächst nur ein Datensatz. Diese Daten können als Identitätsdaten bezeichnet werden.

- Definition: Identitätsdaten sind Daten, anhand derer eine Person in einem bestimmten Zusammenhang bezeichnet wird.

Dieser Datensatz muss einer Person zugeordnet werden, um diese zu bestimmen. Damit hat diese Zuordnung entscheidende Bedeutung. Die Zuordnung findet nach sehr unterschiedlichen Kriterien durch unterschiedliche Institutionen statt, oft durch Behörden (z. B. Personalausweisnummer, in Streitfällen letztlich durch gerichtliche Feststellung).

---

[25] Siehe dazu den Überblick bei *J. Meyer*, S. 47 ff.

[26] *J. Meyer*, S. 50.

Die Identifizierung ist die nachvollziehende Feststellung dieser Zuordnung.

Ausgangspunkt dieser Begrifflichkeit ist die Person im Sinne einer „realen" Entität. Personen sind danach vor allem natürliche Personen (Menschen) sowie juristische Personen, ebenso weitere Entitäten mit Rechtsfähigkeit.

Die Definition lässt aber auch zu, einer fiktiven Person eine Identität zuzuordnen. Auch eine Romanfigur beispielsweise hat danach eine Identität.

4. Begriff der Identität im technischen Sinne

Im Bereich der IT existiert eine Vielzahl von Datensätzen, die in einem bestimmten Kontext die obige Definition einer Identität erfüllen. Als „soziale Identität" bezeichnen wir im Folgenden Daten, die auch ohne Verwendung von IT mit einer natürlichen oder juristischen Person in Verbindung gebracht werden können. Hierzu zählen unter anderem

- Privatpersonen (Name, Adresse, Geburtsdatum, Personalausweisnummer, Passnummer, Geburtsurkunde) und
- juristische Personen (Handelsregistereintrag).

An diese soziale Identität können weitere Datensätze (in Software oder Hardware) gebunden werden. Dies kann durch einen Vertrag oder durch eine technische Maßnahme erfolgen.

Beispiele für eine Bindung durch Vertrag sind

- Benutzername/Passwort: Akzeptieren der AGB einer Webapplikation, Eingabe der Adresse, Auswahl von Nutzername/Passwort.
- E-Mail-Adresse (keine anonymen E-Mail-Adressen): Vertrag mit dem Internet Service Provider; hierdurch wird die E-Mail-Adresse an eine Rechnungsadresse gebunden.
- Telefonnummer: Vertrag mit dem Telekommunikationsunternehmen.
- Mobilfunknummer und International Mobile Subscriber Identity (IMSI), gespeichert in einer SIM-Karte: Vertrag mit einem Mobilfunkanbieter.
- Personalnummer: Arbeitsvertrag.
- Domainname: Vertrag mit einem Domainregistrar.
- Chipkarte: Eine personalisierte Chipkarte wird nach Abschluss eines Vertrages an den Kunden ausgegeben.

Beispiele für eine Bindung durch eine technische Maßnahme sind

- Bestätigungsmail: Eine E-Mail mit einem Passwort oder sonstigen Sicherheitstoken wird an die angegebene E-Mail-Adresse gesandt.
- Zertifikat: Eine juristische oder technische Adresse wird an einen öffentlichen Schlüssel gebunden. Diese Bindung wird durch eine digitale Signatur gegen Fälschung geschützt.
- Single-Sign-On-Token: Eine Aussage über eine Identität wird vom Authentifizierungsserver an den Dienstserver übermittelt (SAML).

Schutz von Identitätsdaten
Da diese weiteren Identitäten, die wir im Folgenden zur Abgrenzung als „technische Identitäten“ bezeichnen wollen, nur Datensätze sind, können sie kopiert und von unbefugten Dritten verwendet werden. Jede technische Identität sollte also im Idealfall mit einer Methode verknüpft sein, mit der sich der eigentliche Besitzer gegenüber unbefugten Dritten abgrenzen kann. Diese Methoden können auf Wissen, Besitz oder Sein beruhen und stark oder schwach sein. (Als vierte Methode wird in der Literatur noch der Ort genannt.)

Oft wird auch argumentiert, dass allgemein „Technik“ eine Identität schützen könne. Dieser Schutz ist aber in der Regel sehr schwach und nur schwer zu quantifizieren.

Schutz durch „Technik“
Für viele technische Identitäten ist ein gewisser Schutz durch die sie definierende technische Infrastruktur gegeben. Diese Infrastruktur verhindert nur gewisse Missbrauchsszenarien, sie verhindert nicht Identitätsmissbrauch im Allgemeinen.

- Beispiel IP-Adressen[27]: Jeder Angreifer kann in die von ihm gesendeten IP-Pakete eine beliebige Absenderadresse schreiben (vgl. Abschnitt zu IP-Spoofing, S. 17 ff.). Allerdings wird er in den meisten Fällen keine Antwort auf dieses IP-Paket empfangen können, da diese von der Routing-Infrastruktur an das Gerät gesendet wird, das diese technische Identität tatsächlich besitzt.
- Beispiel E-Mail-Adressen: Hier gilt ein analoger Sachverhalt, der z. B. zum Ausstellen von E-Mail-Zertifikaten oder zur Erstanmeldung in einem Internetportal ausgenutzt wird: Eine Bestätigungsmail mit einem Passwort oder einer zufälligen Zahl wird an die angegebene E-Mail-Adresse geschickt. Um diese E-Mail abzufangen, müsste ein Angreifer Zugriff auf die E-Mail-Infrastruktur haben.

Nachteil dieses „Schutzes durch Technik“ ist, dass dieser Schutz nicht genau quantifiziert werden kann. In den meisten Fällen ist dieser Schutz relativ leicht zu umgehen, wie die in dieser Studie genannten Beispiele zu Routing-Protokollen und DNS-Angriffen zeigen.

Schutz durch Wissen
Schutz durch Wissen ist die immer noch am häufigsten eingesetzte Schutzmethode. Beispiele hierfür sind

- Passwörter: In der Regel bieten sie nur einen schwachen Schutz, da die meisten Passwörter eine niedrige Entropie haben und daher leicht geraten werden können. Datenbanken, die alle häufig verwendeten Passwörter enthalten, stehen zur freien oder kommerziellen Nutzung bereit. Darüber hinaus sind Passwörter, da sie in der Regel in ein Eingabefenster einer unsicheren grafischen Nutzeroberfläche eingegeben werden müssen, anfällig für Phishingangriffe.
- Kryptografischer Schlüssel: Am anderen Ende der Entropieskala stehen kryptografische Schlüssel. Sie haben eine sehr hohe Entropie, sind aber sehr schwer

[27] http://www.heise.de/meldung/Beweismittel-IP-Adresse-fragwuerdig-980685.html.

zu memorieren. Viele Verschlüsselungstools erlauben eine direkte Eingabe des Schlüssels oder von Werten, aus denen dieser Schlüssel direkt abgeleitet wird. Daher können auch kryptografische Passwörter unter der Rubrik „Schutz durch Wissen" aufgelistet werden.

Schutz durch Wiedererkennen
Einige interessante neue Ansätze lassen sich zwischen „Wissen" und „Sein" einordnen, da sie versuchen, die Entropie beim Authentifizierungsvorgang zu erhöhen, indem Besonderheiten des menschlichen Geistes berücksichtigt werden.

So wurde z. B. von der Firma Passmark Security, die mittlerweile von RSA aufgekauft wurde, eine Methode entwickelt, Nutzer teilweise durch ihre Fähigkeit zum Wiedererkennen von Bildern gegen Phishingangriffe zu schützen. Hierzu wurde im Eingabefenster für die Passworteingabe ein persönliches Foto angezeigt, das der Nutzer vorher auf den Server geladen hatte. Die Idee war, dass ein Angreifer dieses Foto, das in der Menge aller Fotos eine große Entropie besitzt, raten müsste, um den Nutzer zur Eingabe seines Passwortes zu verleiten.

Dieses Verfahren könnte man auch direkt für das Log-in verwenden, indem man den Nutzer bittet, aus einer Menge von zufällig angeordneten Bildern gezielt seine persönlichen Bilder herauszusuchen.

Schutz durch Sein
In der Regel versteht man hierunter den Schutz durch den Abgleich biometrischer Merkmale (z. B. Fingerabdruck, Gesicht, Iris etc.). Die Sicherheit dieser Methoden ist wiederum schwer einzuschätzen, da hier viel von der konkreten technischen Ausführung des Erfassungsgeräts abhängt. So konnte z. B. die erste Generation von Fingerabdruckscannern relativ leicht durch nachmodellierte Plastikfinger getäuscht werden.

Schutz durch Besitz
Die heute sicherste Methode, eine Identität nachzuweisen, ist der Nachweis durch Besitz, oft gekoppelt mit einem (lokalen) Nachweis von Wissen. In diesem Fall benötigt man ein Hardware-Sicherheitstoken, etwa eine Chipkarte (SIM, nPA, Gesundheitskarte, EC-Karte), einen Einmal-Passwortgenerator oder ein komplexeres USB-Sicherheitstoken.

Oft werden diese Geräte erst durch Nachweis des Wissens einer PIN aktiviert.

Verkettung von Identitäten
Eine Verkettung bei der Ausstellung von Identitäten ist möglich und in der Praxis üblich. In der Regel dient dabei eine soziale Identität als Ausgangspunkt. An diese wird durch einen juristischen Vertrag eine erste technische Identität gebunden. An diese erste technische Identität können dann mithilfe rein technischer Maßnahmen, die aber juristisch abgebildet werden können, weitere technische Identitäten gebunden werden.

Folgendes Beispiel soll zur Erläuterung dieser Sachlage dienen:

- Ein durch Nutzername/Passwort geschütztes Nutzerkonto wird durch Vertrag mit dem Internet Service Provider an die Rechnungsadresse des Kunden gebunden (oft ist hiermit auch eine initiale Vergabe einer E-Mail-Adresse sowie eine temporäre Vergabe einer IP-Adresse an den jeweiligen Kunden verknüpft).

- Das Nutzerkonto stellt die erste technische Identität dar. Der Kunde kann sich mit dem Nutzernamen/Passwort einwählen. Er erhält temporär eine IP-Adresse zugeordnet und kann in der Regel über ein Webinterface neue E-Mail-Adressen erzeugen.
- Über die E-Mail-Adresse als technische Identität der zweiten Stufe kann der Kunde nun bei einem anderen Anbieter ein Nutzerkonto eröffnen oder auch ein Clientzertifikat beantragen. Beides wird durch eine Bestätigungsmail an die angegebene Adresse verifiziert.
- Mit dem Clientzertifikat kann er sich ggf. im Rahmen der SSL-Client-Authentifizierung identifizieren.

Als weiteres Beispiel soll ein zukünftiger Einsatzbereich des neuen Personalausweises skizziert werden.

- Die Ausgabe eines neuen Personalausweises erfolgt nach persönlichem Erscheinen und persönlicher Identifikation auf einem Amt. Damit wurde durch diese Amtshandlung der nPA als erste technische Identität an die Identität des Nutzers gebunden.
- Im Rahmen des elektronischen Identitätsnachweises kann der Nutzer sich nun gegenüber Anbietern identifizieren. Hier ist die Kette aber noch nicht zu Ende.
- Der Betreiber eines eID-Dienstes kann durch Ausstellung eines SAML-Token die durch den nPA verifizierte Identifikation gegenüber einem dritten Webdienst nachweisen. Dieses SAML-Token ist vom eID-Dienst elektronisch signiert.

Transaktionsidentitäten/Einmalidentitäten
Im Bereich des Identitätsmissbrauchs sind noch Transaktionsidentitäten/Einmalidentitäten wichtig. Diese Identitäten dürfen nur einmal verwendet werden und sind an eine andere, dauerhafte Identität gebunden. Beispielhaft seien genannt:

- TAN, iTAN: Diese Einmalidentitäten sind an ein Bankkonto gebunden, sie sind zeitlich unbegrenzt verwendbar.
- eTAN: Diese Einmalidentität ist ebenfalls an ein Bankkonto gebunden und zeitlich nur befristet verwendbar.
- eTAN+, mTAN: Diese Einmalidentitäten sind an ein Konto und eine bestimmte Transaktion gebunden.

Authentifizierung einer Sitzung/Authentifizierung einer Transaktion
Generell können Identitäten im Internet eingesetzt werden, um eine komplette Sitzung zu authentifizieren oder um einzelne Transaktionen zu authentifizieren. Während einer Sitzung können mehrere Transaktionen initiiert werden. Eine Sitzung kann nach Ablauf einer bestimmten Zeitspanne (alternativ: Zeitspanne der Untätigkeit) beendet werden, oder durch aktives Beenden der Sitzung vonseiten des Clients („Log-out“) oder des Servers („Termination“). Um die Authentifizierung einer Identität über die gesamte Dauer der Sitzung aufrechtzuerhalten, werden verschiedene technische Hilfskonstrukte (z. B. http Sessioncookies, SSL state) eingesetzt.

- Einsatz von Identitäten zur Authentifizierung von Sitzungen:
  - Nutzername/Passwort, PIN

  - Clientzertifikate in SSL
  - eID-Funktion des nPA
- Einsatz von Identitäten zur Authentifizierung von Transaktionen:
  - TAN, iTAN, eTAN, eTAN+, mTAN
  - digitale Signatur von Datensätzen (HBCI, Signaturgesetz)

Markenrecht
Ein sehr interessanter Fall von Identitätsmissbrauch tritt dann auf, wenn der Angreifer eine technisch verschiedene, aber „ähnliche" technische Identität verwendet.

- Firmenlogo und Firmendesign: In vielen Phishing-E-Mails und auf vielen Phishingwebsites wurde das Firmendesign einschließlich der Logos nachgeahmt. Design und Logo sind keine technischen Identitäten im engeren Sinn, da sich ein Logo, von dem viele Varianten (Größe, Format) existieren können, nicht durch einen einzigen Zahlenwert beschreiben lässt.
- „Ähnliche" Domainnamen: Da die Namensgebung im Domain Name System psychologisch wenig aussagekräftig ist, können sehr einfach Namen verwendet werden, die technisch völlig verschieden sind, aber psychologisch ähnlich wirken („banking.bank.de" vs. „bank.banking.de"). Auch homografische Attacken, bei denen ein internationaler Zeichensatz zur Nachahmung eines anderen verwendet wird, sind hier zu nennen.

II. Identitätsmissbrauch und Identitätsdiebstahl

Identitätsmissbrauch und Identitätsdiebstahl sind in Rechtsprechung und Literatur gebräuchliche Begriffe. Allerdings wird ein Verständnis der Begriffe regelmäßig vorausgesetzt, einheitliche Definitionen fehlen bislang.

1. Der Begriff des Identitätsmissbrauchs

Definitionen des Identitätsmissbrauchs sind nur selten zu finden. In der Literatur wird der Begriff etwa als „Nutzung des Identitätsdiebstahls zum Schaden der betroffenen Person" definiert.[28] Von dieser Definition, die von der Definition des „Identitätsdiebstahls" abhängig ist, werden etwa Fälle nicht erfasst, bei denen zunächst legal erlangte Personendaten später missbraucht werden.

In dieser Untersuchung wird der Begriff wie folgt definiert:

- Identitätsmissbrauch: unbefugtes Agieren unter einer Identität.

Dieses Verständnis des Identitätsmissbrauchs deckt nahezu alle Fallgruppen des missbräuchlichen Handelns unter Verwendung einer bestimmten Identität ab.

[28] *Busch*, DuD 2009, 317.

Erfasst wird etwa das klassische Handeln unter falscher Identität, d. h. das Handeln gegenüber einem Dritten unter einer anderen als einer eigenen Identität. Erfasst wird auch das unbefugte Handeln unter einer eigenen Identität, bei der eine eigene Identität verwendet wird, die aber in dem jeweiligen Kontext nicht zugelassen ist, z. B. der Kauf von Waren unter einer abweichenden Wohnanschrift, um vom Verkäufer nicht als der (kreditunwürdige) Käufer unter der bisher genannten Wohnanschrift identifiziert zu werden. Nicht erfasst sind sonstige unbefugte Verwendungen fremder Identität (z. B. Datenhandel).

Identitätsmissbrauch ist danach auch nicht das befugte Handeln unter einer fremden Identität (z. B. Handeln auf fremdem eBay-Account mit Billigung des Accountinhabers). Dies schließt Handeln unter einer fiktiven Identität ein.

Gefahren: Schädigung von Dritten, Schädigung des Inhabers der vorgetäuschten Identität.

2. Der Begriff des Identitätsdiebstahls

Der Begriff des Identitätsdiebstahls wird in sehr unterschiedlichen Bedeutungen verwendet. Dabei lassen sich in der juristischen Literatur zwei Grundauffassungen unterscheiden. Zum Teil wird er als missbräuchliche Nutzung personenbezogener Daten verstanden.[29] Eine solche Fallkonstellation wurde auch in der Rechtsprechung schon als Identitätsdiebstahl (in Anführungszeichen) betitelt.[30] Die Bundesregierung bezeichnet ebenfalls den „Missbrauch ausgespähter Daten" als Identitätsdiebstahl.[31] Auch findet sich dieses Verständnis außerhalb der juristischen Literatur wieder.[32]

Nach einer anderen Auffassung soll Identitätsdiebstahl als die Aneignung von Daten verstanden werden, mit denen man sich im Rechtsverkehr identifizieren kann.[33] Danach soll nur die Aneignung der Daten selbst, nicht hingegen auch die nachfolgende Verwendung Bestandteil des Identitätsdiebstahls sein. Nach *Spindler* etwa soll ein Identitätsdiebstahl vorliegen, wenn der Handelnde „in den Besitz von Identitäten gelangt".[34] *Schaar* spricht im Zusammenhang mit dem Kopieren und

---

[29] So etwa bei *Gercke*, CR 2005, 233; *Hoeren*, in Hoeren/Sieber, Rz. 206.

[30] OLG Brandenburg, 16. 11. 2005, 4 U 5/05, NJW-RR 2006, 1193, 1195; der BGH verwendet diesen Begriff im Revisionsurteil nicht, siehe BGH, 10. 4. 2008, I ZR 227/05, NJW 2008, 3714 – Namensklau im Internet.

[31] BT-Drs. 16/9160, S. 7.

[32] http://de.wikipedia.org/wiki/Identit%C3%A4tsdiebstahl; http://www.boerse-online.de/wissen/lexikon/boersenlexikon/index.html?action=descript&buchstabe=I&begriff=Identit%E4tsdiebstahl#eintrag; vgl. auch den PayPal-Leitfaden zum Identitätsdiebstahl unter https://www.paypal.com/de/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/general/UnderstandIdTheft-outside.

[33] *Junker*, in jurisPK-BGB, § 126b Rz. 42; *Schneider*, EDV-Recht, B. Rz. 981; von einer Entwendung der Daten ist die Rede unter http://lexexakt.de/glossar/identitaetsdiebstahl.php.

[34] *Spindler*, in Spindler/Wiebe, Kap. 5, Rz. 98.

Fälschen von Fingerabdrücken von Identitätsdiebstahl.[35] Teilweise werden sehr enge Begriffe verwendet, etwa Identitätsdiebstahl und Phishing gleichgesetzt.[36]

Das erstgenannte Verständnis des Identitätsdiebstahls verwendet den Begriff offenbar als Oberbegriff, der jedwede unbefugte Verwendung personenbezogener Daten abdeckt, oder als Synonym zum Identitätsmissbrauch im oben genannten Sinne. Um die Begriffe auseinanderzuhalten und eine synonyme Verwendung zu vermeiden, erscheint es sinnvoll, zwischen der Erlangung und dem späteren Agieren unter einer fremden Identität zu differenzieren.

In dieser Untersuchung wird der Begriff des Identitätsdiebstahls wie folgt definiert:

- Identitätsdiebstahl: unbefugtes Sichverschaffen einer Identität.

Ein Identitätsdiebstahl liegt danach vor, wenn der Täter sich die Identität einer Person, also eine Menge an Daten verschafft, durch die die betreffende Person in einem bestimmten Zusammenhang eindeutig bezeichnet wird. Beispiele sind etwa das Beschaffen von Name und Kreditkartendaten oder von Name und Anschrift oder von Name und Geburtsdatum.

Von dem Identitätsdiebstahl in diesem Sinne ist das Beschaffen personenbezogener Daten abzugrenzen, die für eine Identifizierung nicht ausreichen. Dies ist etwa bei einer ungeordneten Mehrheit von Identifizierungsdaten (z. B. Kreditkartennummer ohne zugehörigen Namen) der Fall oder wenn nur einzelne Daten (z. B. nur der Name) bekannt sind.

3. Schutz von Identitäten (Überblick)

Identitäten sind in vielfältiger Weise geschützt. Insbesondere werden Identitäten durch technische und organisatorische Schutzmaßnahmen sowie durch verschiedene rechtliche Schutzinstrumente gegen unbefugte Verwendung durch Dritte gesichert.

Zu den technischen und organisatorischen Schutzinstrumenten (dazu oben S. 6 ff.) gehören etwa der Schutz durch „Wissen“, durch „Besitz“ oder durch „Sein“.

Die rechtlichen Schutzinstrumente sind vielfältig und haben unterschiedliche Zielrichtungen. Zunächst ist die Identität durch die Grundrechte der Verfassung geschützt. Im Vordergrund steht das Persönlichkeitsrecht der Person, das auch die eigene Identität umfasst (dazu unten S. 200). Es können aber auch weitere Grundrechte betroffen sein.

Die Identität von Personen steht unter dem Schutz des Datenschutzrechts, das die Verwendung personenbezogener Daten, zu denen die Identitätsdaten gehören, grundsätzlich an die Einwilligung des Berechtigten bindet (dazu unten S. 204).

---

[35] *Schaar*, MMR 2008, 137, 138.

[36] So *Löhnig/Würdinger*, WM 2007, 961; ähnlich *Gercke*, CR 2005, 606, 607.

Dem Schutz der Identität dient ferner eine Vielzahl strafrechtlicher Verbote. Schon die unbefugte Erlangung identitätsrelevanter Daten ist umfassend unter Strafe gestellt (dazu unten S. 196 und S. 233 ff.). So können beim Erlangen der bloßen Daten die Straftatbestände der §§ 202a, 202b, 202c, 303a StGB erfüllt sein, bei Entwendung von Datenträgern die §§ 242, 246, 263, 249, 253, 255 StGB. Der Identitätsmissbrauch ist ebenfalls umfassend strafbar (dazu unten S. 197 f. und S. 244 ff.). So ist jeweils § 44 BDSG i. V. m. § 43 Abs. 2 BDSG erfüllt, je nach Kontext auch weitere Straftatbestände, etwa §§ 263, 263a, 267, 269, 270 StGB.

Schließlich kann der Identitätsinhaber durch verschiedene zivilrechtliche Schutzmechanismen gegen die unbefugte Verwendung seiner Identität vorgehen (dazu unten S. 211 ff. und S. 277 ff.). Das klassische Schutzinstrumentarium enthält folgende Instrumente:

- Beseitigungsanspruch, d. h. Anspruch auf Beseitigung, d. h. Beendigung und ggf. Rückgängigmachung einer unbefugten Verwendung,
- Unterlassungsanspruch, d. h. Anspruch auf Unterlassung künftiger unbefugter Verwendung,
- Schadensersatzanspruch, d. h. Anspruch auf Ersatz des durch die Verwendung entstandenen Schadens.

Diese gesetzlichen Schutzansprüche stehen bei unbefugter Verwendung von Identitäten grundsätzlich zur Verfügung.

Hinzu können vertragliche Schutzpflichten mit der Sanktion des Schadensersatzanspruchs bei Pflichtverletzung und weitere Instrumente kommen (dazu unten S. 290 ff.).

III. Fallgruppen des Identitätsdiebstahls und -missbrauchs

1. Identitätsdiebstahl und -missbrauch ohne IT-Bezug (Überblick)

Identitätsdiebstahl bzw. -missbrauch kann auch ohne die Zuhilfenahme von IT stattfinden. Die Szenarien lassen sich dabei grob in zwei Klassen unterteilen:

- Identitätsdiebstahl bzw. -missbrauch im „*hoheitlichen*“ Bereich. Darunter fallen die Fälle der Fälschung bzw. des Missbrauchs von hoheitlichen Dokumenten (etwa Reisepass, Personalausweis, Geburtsurkunde etc.).
- Identitätsdiebstahl bzw. -missbrauch im „*privaten*“ Bereich, bspw. Heiratsschwindelei, Kreditkartenmissbrauch oder auch das Entwenden von persönlichen Informationen aus der häuslichen Umgebung.

Im hoheitlichen Bereich liegt die Zielsetzung meist darin, mithilfe einer falschen Identität unterzutauchen, Grenzkontrollen zu passieren oder auch generell einer Strafverfolgung zu entgehen. Dazu gehören in erster Linie alle Formen des

Ausweis-/Passbetrugs, ggf. unter Einschluss der Verwendung von Tarnidentitäten, die dazu benutzt werden sollen, kriminelle Aktivitäten vorzubereiten bzw. auszuführen. Des Weiteren gehören in diese Fallkategorie auch das Untertauchen mit falscher Identität i. V. m. der Eröffnung von Bankkonten etc., die unerlaubte Einreise und der unerlaubte Aufenthalt sowie die Nutzung von Decknamen und Ähnlichem, häufig ebenfalls mit der Zielsetzung verbunden, einer Strafverfolgung zu entgehen.

Im privaten Bereich wird neben der Fälschung von (nichtamtlichen) Ausweispapieren das Annehmen einer falschen Identität betrachtet. Meist geschieht dies in betrügerischer Absicht. In diesem Zusammenhang sind insbesondere die Hochstapelei und der Heiratsschwindel zu erwähnen, ebenso die Urkundenfälschung im weitesten Sinne, etwa in Form der Erlangung von Titeln etc., und schließlich der Scheckbetrug.

Dabei kann sich der Angreifer verschiedener Methoden bedienen, um sich die notwendigen Informationen zu beschaffen. Diese reichen von der simplen Durchforstung eines Papierkorbs bzw. Mülleimers und dem Einbruch und Diebstahl von entsprechenden Gegenständen, beispielsweise aus dem Auto, bis zur heimlichen Entleerung eines Briefkastens, der z. B. den Brief mit der neuen Kreditkarte enthält. Papierkörbe spielen dabei auch in Bankfilialen eine nicht zu unterschätzende Rolle: Werden dort Kontoauszüge oder fehlerhaft ausgefüllte Überweisungsträger unachtsam entsorgt, findet der Angreifer alle benötigten Informationen wie Kontonummer, Bankleitzahl, Name und häufig auch die Adresse des potenziellen Opfers. Auch der Anruf bei der Bank zur Erhöhung des Kreditkartenlimits oder die unbefugte Einrichtung eines Nachsendeauftrags gehören dazu. Darüber hinaus besteht für einen Angreifer die Möglichkeit, sich durch *Skimming*[37] oder *Shoulder surfing*[38] weitere Informationen zu beschaffen. Beide Angriffsverfahren sind diesbezüglich hauptsächlich im Zusammenhang mit Identitätsdiebstahl bzw. -missbrauch von Kreditkarten und Kontodaten interessant. Während beim Skimming die Einordnung als Identitätsdiebstahl bzw. -missbrauch ohne IT-Bezug fraglich ist, da hier in den meisten Fällen Informationstechnologie in Form von Auslesegeräten für Magnetstreifen zum Einsatz kommt, ist der Sachverhalt in Bezug auf Shoulder surfing eindeutig. Hier nutzt der Angreifer den Umstand aus, dass viele Opfer unvorsichtig bei der Eingabe persönlicher Daten sind und keine Vorkehrung gegen ein „Ausspähen über die Schulter“ treffen.

Die Zielsetzung liegt für den Angreifer meistens darin, sich einen wie auch immer gearteten Vorteil zu verschaffen. Hiermit kann er sich z. B. illegale Substanzen (bspw. Drogen) beschaffen oder etwa die Erstellung gefälschter Einreisedokumente finanzieren.

Wichtiger Punkt bei der Bekämpfung des Identitätsdiebstahls bzw. -missbrauchs ohne IT-Bezug ist – wie im Übrigen bei allen Szenarien mit IT-Bezug – das schnellstmögliche Melden des Vorfalls. Nur dadurch lassen sich die möglichen Auswirkungen eines Identitätsdiebstahls bzw. -missbrauchs wirkungsvoll minimieren. Entwendet der Angreifer aber bspw. einen Brief aus dem Briefkasten

[37] Vgl. hierzu auch: http://de.wikipedia.org/wiki/Skimming_%28Betrug%29.

[38] Vgl. hierzu auch: http://en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29.

des Opfers und wurde dieser darüber hinaus auch vom Angreifer – und nicht vom Opfer – angefordert, so entsteht die Schwierigkeit, dass das Opfer gar nicht mit dem Erhalt eines Briefes rechnet und somit den Verlust des Briefes auch nicht bemerkt. Erst wenn der Angreifer – ggf. unter Zuhilfenahme weiterer Maßnahmen – den eigentlichen Identitätsdiebstahl bzw. -missbrauch in einen finanziellen Vorteil verwandelt, hat das Opfer, bspw. durch Kontrolle der Kreditkartenabrechnungen, überhaupt eine Chance, den Identitätsdiebstahl bzw. -missbrauch zu bemerken. Benutzt der Angreifer darüber hinaus weitere Methoden wie etwa die Erstellung eines Nachsendeauftrags zu seinen Gunsten, so bekommt das Opfer auch keine Kreditkartenabrechnung mehr. In einem solchen Fall ist lediglich das Ausbleiben der Kreditkartenabrechnung das auffällige Merkmal, das dem Opfer einen Hinweis auf einen möglichen Identitätsdiebstahl bzw. -missbrauch geben kann. Um das Risiko für das Opfer einzuschränken, ist daher eine regelmäßige Kontrolle des Briefkastens und der Kreditkartenabrechnungen – ggf. auf einem alternativen Wege, etwa durch Überprüfung des Onlinekreditkartenauszuges – dringend zu empfehlen. Selbiges gilt natürlich auch im Zusammenhang mit Kontoauszügen und während einer Urlaubsabwesenheit. Im letztgenannten Fall sollten weitere vertrauenswürdige Personen (etwa Freunde oder Nachbarn) mit der regelmäßigen Kontrolle und Leerung des Briefkastens betraut werden. Um dem Datendiebstahl im Zusammenhang mit Papierkörben und Mülleimern zu begegnen, sollten alle sensitiven Dokumente sicher vernichtet werden. Anzuraten ist dabei, die entsprechenden Dokumente mittels eines Aktenvernichters mit Partikelschnitt[39] zu zerstören.

2. Identitätsdiebstahl und -missbrauch mit IT-Bezug (Überblick)

An dieser Stelle soll ein erster Überblick über die Erscheinungsformen von Identitätsdiebstahl und Identitätsmissbrauch gegeben werden, ohne Anspruch auf eine etwaige Systematik zu erheben. Die Beispiele betreffen dabei *technische* Identitäten, wie sie auf S. 6 ff. beschrieben sind.

Nutzung fremder Adressdaten (Spaßbestellungen)
Adressdaten können als technische Identität aufgefasst werden. Sie sind jedoch leicht zu ermitteln und zunächst durch keinerlei technische Maßnahmen geschützt. Der „Inhaber" dieser Daten kann sich nur durch Geheimhaltung der Daten schützen, was in der Praxis schwer durchzuhalten ist, da Adressdaten in Telefonbüchern und Adresssammlungen von Unternehmen vorgehalten werden.

Ein Anbieter von Waren oder Dienstleistungen kann sich jedoch organisatorisch gegen den Missbrauch fremder Adressdaten (z. B. für „Spaßbestellungen") schützen, indem er die Adressdaten an einen geheimen Wert (z. B. Nutzername/Passwort) bindet und die erste Bestellung nur gegen Vorkasse oder per Nachnahme durchführt.

[39] Hierzu siehe auch: http://de.wikipedia.org/wiki/Aktenvernichter#Funktionsweise.

Kreditkartenmissbrauch
Die Kreditkartennummer ist keine geheime Information. Da sie sehr oft weitergegeben wird (Eingabe in Webformulare, Weitergabe in Hotels), ist sie anfällig für Phishingangriffe. Vollständige Datensätze von Kreditkarten (Nummer, Prüfziffer, Gültigkeitszeitraum, Name) werden daher im Internet für wenig Geld gehandelt. Überprüfungen der einzelnen Zahlungsvorgänge durch die Kreditkartenfirmen halten die Schäden hier in Grenzen.

Nutzung fremder E-Mail-Accounts
Der Zugang zu E-Mail-Accounts ist in der Regel durch Nutzername/Passwort geschützt. Durch Phishingangriffe kann sich somit ein Unbefugter Zugang zu diesen Accounts verschaffen und sie z. B. zum Versenden von SPAM-E-Mails benutzen.

Spoofing
Technische Identitäten, die nur durch eine technische Infrastruktur geschützt sind, können über diverse Spoofing-Angriffe kompromittiert werden. Die im Rahmen der Angriffe auf Onlinebanking bekanntesten Spoofing-Varianten sind Phishing (E-Mail-Spoofing, Web-Spoofing) und Pharming (DNS-Spoofing).

Nutzung fremder Transaktionsidentitäten
Im deutschen Onlinebanking werden Einmal- oder Transaktionsidentitäten verwendet, um einzelne Transaktionen abzusichern. Diese müssen von einem Angreifer abgefangen werden, und ihre Einlösung bei der Bank muss verhindert werden. Hierzu ist eine aktive Kontrolle des Netzwerks erforderlich.

Man-in-the-Middle-Angriffe
Insbesondere bei Identitätsdaten, die durch Besitz geschützt sind, ist ein Identitätsdiebstahl im Internet praktisch nicht zu realisieren, da hierzu ein realer Diebstahl des verwendeten Hardwaretokens erforderlich wäre. In diesem Fall werden in der Praxis sogenannte Man-in-the-Middle-Angriffe durchgeführt, bei denen der Angreifer den Kommunikationskanal kontrolliert, die Identifikation durch Besitz ungehindert passieren lässt, aber anschließend die ausgetauschten Daten verändert.

Die Kontrolle des Kommunikationskanals kann hierbei im Endgerät (PC) des Nutzers (z. B. über ein eingeschleustes Trojanisches Pferd) oder im Internet selbst durch Umleitung des Datenverkehrs erfolgen.

IV. Ähnliche Phänomene

Eine Reihe von Phänomenen ist den hier interessierenden Angriffen ähnlich, hat aber für die Problematik des Identitätsdiebstahls und -missbrauchs keine Bedeutung. Dazu zählen etwa

- DDos-Angriffe ohne Verwendung fremder Identitäten.
- Unbefugte Speicherung und Verwendung, Handel mit Identitätsdaten.
  Der Datenhandel mit persönlichen Daten (Adressdaten, Bankdaten), die durch Datenschutzbestimmungen geschützt sind, hat in jüngster Vergangenheit in der

Presse große Aufmerksamkeit erfahren. Für diese Studie ist er nicht relevant, da diese Daten in der Regel freiwillig von den Nutzern preisgegeben wurden (wenn auch zu einem eingeschränkten Verwendungszweck), also kein Identitätsdiebstahl vorliegt. Diese Datensätze enthalten in der Regel auch keine geheimen Daten wie Passwörter. Dieser Datenhandel ist in großem Maßstab möglich, da er IT-gestützt ist. Dies verdeutlicht bereits die Problematik von Identitäten, die in IT-Systemen eingesetzt werden: Ein Missbrauch in großem Maßstab ist einfach und mit geringen Kosten durchzuführen.

- Unbefugte Speicherung und Verwendung sonstiger Daten.

http://www.springer.com/978-3-642-15832-2

Identitätsdiebstahl und Identitätsmissbrauch im Internet
Rechtliche und technische Aspekte
Borges, G.; Schwenk, J.; Stuckenberg, C.-F.; Wegener, C.
2011, XIX, 405 S. 50 Abb. in Farbe., Hardcover
ISBN: 978-3-642-15832-2