Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2018

geleitet durch Prof. Dr. Paul Molitor

Digitale Identität und ihre Gefahren

Christian Figul & Julia Gruhl

Inhaltsverzeichnis

Gender-Hinweis: Die weibliche Form ist der männlichen Form in dieser Arbeit gleichgestellt; lediglich aus Gründen der Vereinfachung wurde die männliche Form gewählt.

Überarbeitung durch den Dozenten: Der vorliegende Text entspricht im Wesentlichen dem ursprünglichen durch Herrn Christian Figul und Frau Julia Gruhl erstellten Bericht. Der Dozent hat lediglich (die sehr wenigen) Schreib- und Kommatafehler korrigiert.

1 Der Identitätsbegriff im soziologischen und psychologischen Kontext

Wenn man über die Gefahren von digitaler Identität sprechen will, muss unseres Erachtens vorher geklärt werden, auf welchen Identitätsbegriff wir uns beziehen, denn es gibt keine über alle wissenschaftlichen Disziplinen hinweg einheitliche Definition von Identität.

1.1 Lothar Krappmann

Der deutsche Soziologe setzt seinen Identitätsbegriff aus einer These von George H. Mead und einer von Erik H. Erikson zusammen: zum einen kann Identität nur auf dem Umweg über den Anderen gewonnen werden und zum anderen hat Identität einerseits eine personale Seite, die sich über die unverwechselbare Biographie und ihre typischen Krisenlösungen definiert, und eine soziale Seite, die über die Anerkennung des Selbstbildes durch die Anderen gewonnen wird (Abels, 2009, S.376).
Daraus ergibt sich nach Krappmann das Problem der Balance zwischen dem Individuum und der Gesellschaft in der Adoleszenzphase. Heranwachsende können in dieser Phase, sichere Rahmen, in denen richtige Entscheidungen getroffen werden können, nur schwer erkennen. Denn die Bezugsgruppen, von denen das Individuum Legitimationen für eigene Entscheidungen erhält, sind diffus und widersprüchlich. Diese Umstände resultieren in der „balancierenden Identität“ eines Individuums; sie beschreibt das Ergebnis der Bemühungen, Unklarheiten, Unstimmigkeiten und Widersprüche zu bearbeiten (ebd. S. 377).
Um die Identität zu schützen, ist es für die Heranwachsenden notwendig, ihren Identitätsentwurf immer wieder verständlich zu machen, zu verteidigen und ggf. umzukonstruieren. Dadurch soll vermieden werden, sich außerhalb sozialer Erwartungen zu bewegen und dabei die eigenen Wünsche nicht ausreichend zu respektieren. Außerdem besteht für jedes Individuum die Notwendigkeit, seinen eigenen Platz in einer widersprüchlichen, sich ständig wandelnden Gesellschaft zu bestimmen; auch das dient dem Schutz der eigenen Identität (ebd. S. 377).

1.2 David Riesman

Der amerikanische Soziologe David Riesman konzentriert sich in seiner Theorie deutlicher auf die äußeren Umstände insbesondere im Bezug auf den Menschen der Moderne. Das „außengeleitete“ Individuum handelt so, wie alle, die ihm wichtig sind, handeln. Das können enge Freunde, die nächsten Nachbarn, aber auch Fans der gleichen Musik oder anonyme Trendsetter weltweit sein (Abels, 2009, S. 341). Aktuell ist für letzteres der Begriff *Influencer* wahrscheinlich zeitgemäßer.
Ständig in Konkurrenz miteinander stehende Verhaltensmuster für die gleiche Situation, permanent mit Neuem und Anderem durch immer mehr Kontakt mit fremden Kulturen konfrontiert zu werden und das im Menschen verankerte Überflussbewusstsein, das durch den ansteigend breiten Wohlstand und mehr Freizeit ein Bedürfnis entwickelt, diese Ressourcen um jeden Preis zu verbrauchen, konstituiert den Menschen der Moderne. Unterstützt werden diese Faktoren durch die Massenmedien, die dem Individuum trotz geografisch großer Entfernung die fremden Kulturen direkt nach Hause liefern, sodass sich jedes Individuum, insbesondere Heranwachsende, irgendwann fragt, ob diese Informationen nicht eine realistische Alternative zum eingelebten Verhalten darstellen können (ebd. S. 343f.).
Das Problem für die eigene Identität erklärt Riesman über eine Sender-Empfänger-Metapher: Das Individuum hat viele verschiedene Sender zur Verfügung und unterliegt einem häufigen Programmwechsel. Durch das Verbrauchsbedürfnis ist der Wunsch groß, alle Signale zu empfangen, was für den Menschen bedeutet, dass er das Empfangsgerät komplett verinnerlichen muss (ebd. S. 345). Somit zeigt das Individuum nicht mehr, wer es ist, sondern was es kann. Es gibt also eine passende Identität für jede Situation und nicht mehr eine Identität für alle Situationen, in die das Individuum gerät (ebd. S. 346).
Abschließend stellt Riesman fest:

> „Bei Jugendlichen schütteln wir den Kopf, wenn sie heute das und morgen das für wahnsinnig wichtig halten, und den *anderen* Erwachsenen kreiden wir es als Charakterschwäche an, wenn sie ‚ihr Fähnchen nach dem Wind hängen‘. Doch Außenleitung macht sich nicht nur *vor* unserer Haustür breit, sondern ist in die Bedingungen der Moderne eingewoben.“
> (ebd. S. 347, Hervorhebungen im Original)

1.3 Identität-Lexikon der Psychologie

Identität beantwortet in einer universellen und kulturell-spezifischen Dimension die Frage, wer man selbst ist oder wer jemand anderer ist. Die Antwort sind Bedingungen, die eine biographische und situationsübergreifende Gleichheit in der Wahrnehmung der eigenen Person möglich machen. So konstruiert sich innere Einheitlichkeit trotz äußerer Veränderungen (Keupp, 2000).
Außerdem ist Identität ein Akt sozialer Konstruktion, d.h. das Individuum versucht die eigene oder eine andere Person in einem Kontext zu erfassen. Somit wird eine individuelle soziale Verortung, basierend auf dem menschlichen Grundbedürfnis nach Anerkennung und Zugehörigkeit, produziert (ebd.).
Identität hat zudem auch immer einen sogenannten „Doppelcharakter“: auf einer Seite geht des um die Darstellung des unverwechselbaren Individuellem und auf der anderen Seite um die des sozial Akzeptablen. Für das Individuum geht es dabei darum, einen Kompromiss zwischen Eigensinn und Anpassung zu finden (ebd.).

2 Gesetzliche Aspekte

Nachdem wir den Begriff Identität formal eingegrenzt haben, ist zu klären, wie Identität in Gefahr geraten kann. Die Kernfragen hierbei sind, wie sieht Identitätsdiebstahl aus und wie versucht das Gesetz unsere Identität zu schützen. So mag es vielleicht überraschen, dass der Identitätsdiebstahl an sich keinen eigenen Straftatbestand im deutschen Recht erfüllt, sondern nur die daraus resultierenden Delikte strafrechtlich verfolgt werden.
Grundlegend können wir Identitätsdiebstahl in der digitalen Welt aus zwei Richtungen betrachten: Zum einen vertrauen wir täglich Unternehmen unsere Daten an, seien es Banken, Onlineshops oder der Google-Account. Uns wird höchste Datensicherheit versprochen und wir gehen davon aus, dass niemand ohne Legitimation diese Daten verarbeitet. Zum anderen geben wir einen wesentlichen Teil unserer Persönlichkeit und damit auch unserer Identität im Internet preis, z. B. in sozialen Netzwerken wie Facebook. Vielen Menschen ist nicht bewusst, was für eine sensible Information allein das Geburtsdatum ist. Kaum hat man Vor-, Nachnamen und das Geburtsdatum, lassen sich hinterlegte Passwörter am Telefon mal eben ändern. Noch vor gar nicht allzu langer Zeit wurden bei bekannten Telekommunikationsunternehmen die persönlichen Daten lediglich mit dem Geburtsdatum bestätigt, wenn man das Passwort nicht zur Hand hatte.

So konnten neue Verträge bereits über das Telefon mit dem vermeintlich verifizierten Vertragspartner geschlossen oder auch Adressänderungen vollzogen werden.

2.1 Datendiebstahl und -weitergabe durch Dritte

2014 stahl eine Hacker-Organisation 145 Millionen Datensätze der Plattform Ebay (Juraforum, 2018). Wer einen Ebay-Account hat, weiß, welche Daten dabei in die Hände Dritter gelangt sind: E-Mail-Adressen, Postadressen, Geburtsdaten, Telefonnummern und Passwörter. Doch nicht nur solche Fälle sollten den Nutzer beunruhigen.
Datenhandel ist ein lukratives Geschäftsmodell (Datenschutz, 2018). Datensätze werden dabei in Massen von Unternehmen an andere verkauft, meist zum Zweck des Direktmarketings. Der ein oder andere hat vielleicht schon mal Werbepost, E-Mails oder Anrufe von Unternehmen erhalten, mit denen er im Vorfeld nichts zu tun hatte. Diejenigen können sich sicher sein, dass ihre Daten verkauft wurden. Das Geschäft an sich ist nicht neu, doch wurde es durch die Digitalisierung enorm beschleunigt. Während in den 50er Jahren Adresshändler lediglich Stammdatensätze (Vor-, Nachname, Adresse, Geburtsdatum) besaßen, horten Unternehmen heutzutage Millionen von Privatadressen zusammen mit Merkmalen, Wohnumfeld, Neigungen, Hobbys und Interessen, sehr detailliert und für jeden zum Kauf erhältlich (Keller, 2017).

2.2 Datenschutzgrundverordnung (DSGVO)

Die neue Datenschutzgrundverordnung, kurz DSGVO, zielt darauf ab, zumindest der illegalen Datenweitergabe einen Riegel vorzuschieben und Unternehmen mehr in die Verantwortung zu nehmen, personenbezogene Daten zu schützen.
Innerhalb der EU gilt die DSGVO. Jedes Unternehmen, das personenbezogene Daten auf irgendeine Art und Weise erhebt oder verarbeitet, darf das nur noch mit Erfüllung eines durch die DSGVO bestimmten Grunds. Es gilt das Verbotsprinzip, d. h. die Erhebung und Verarbeitung personenbezogener Daten ist grundsätzlich verboten, wenn sie nicht durch einen Erlaubnistatbestand gedeckt ist (EU Datenschutzgrundverordnung, 2018). Dazu gehören u.a. die Notwendigkeit zur Vertragserfüllung gemäß Art. 6 I b DSGVO und besonders die Zustimmung des Betroffenen gemäß Art. 6 I a DSGVO. Gleichzeitig darf das Unternehmen die Daten nur so lange speichern, wie der Grund zur Datenerhebung besteht (ebd.).
Den Betroffenen werden besondere Rechte zugesprochen. Allen voran muss die Einwilligung gemäß Art.7 I, IV DSGVO freiwillig erbracht worden sein. Die Betroffenen haben

darüber hinaus jederzeit das Recht, Daten einzusehen, zu berichtigen und vollständig löschen zu lassen. Das Unternehmen hat dafür Sorge zu tragen, dass es im Falle einer notwendigen Weitergabe von Daten diese nur DSGVO-konforme Unternehmen überträgt.
Daraus ergibt sich eine besondere Anforderung an internationale Unternehmen und solche, die mit nicht in der EU ansässigen Unternehmen zusammenarbeiten. Diese müssen nämlich zumindest einen vergleichbar strikten Datenschutz verfolgen wie die EU, so z.B. das EU-US Privacy Shield Übereinkommen, das dem Nutzer einen ähnlich starken Datenschutz bieten soll wie die DSGVO (Bohl, 2018).
Hier zeichnet sich direkt die nächste große Hürde des digitalen Zeitalters ab. Das Internet ist quasi grenzenlos und während sich Rechtsvorschriften und Sitten auf Staatsgrenzen und Gemeinschaften beschränken, war es nie einfacher diese Grenzen zu überschreiten. Man denke alleine an unzählige Cloud-Lösungen, die täglich Milliarden Daten um die Welt schicken. Im Zuge der DSGVO ist jedes Unternehmen nun auch dazu verpflichtet, jedwede Verarbeitung und Erhebung zu dokumentieren und auf Verlangen die Prozesse nachvollziehbar und transparent offenzulegen. Indirekt geht daraus auch hervor, dass Daten so gesichert werden müssen, dass sie im Falle eines Datenlecks unbrauchbar sind, sprich verschlüsselt.

2.2.1 Was droht Unternehmen bei Verstoß?

Neben empfindlich höheren Strafen hat die DSGVO den Betroffenen ein starkes Recht eingeräumt: nunmehr kann allein auf Verdacht jeder Betroffene ein Unternehmen bei der zuständigen Aufsichtsbehörde melden. Diese sind dazu angehalten, jedem Verdacht nachzugehen. Bei bestätigten Fällen drohen Unternehmen Bußgelder von bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes (Kirsch, 2016).
Vor der DSGVO galt eine Höchststrafe von 300 000 Euro.

2.2.2 Diskussion: Kann uns die DSGVO schützen?

Die DSGVO hat kurz vor der Umsetzung eine Panikwelle unter Unternehmern entfacht. Das Thema war besonders in kleinen Unternehmen ständig präsent, externe Datenschutzbeauftragte und Weiterbildungskurse waren ausgebucht.
Dieses Phänomen lässt sich unseres Erachtens auf zwei Weisen deuten: Zum einen scheint die DSGVO einen wesentlichen Teil dazu beigetragen zu haben, dass zumindest

in Deutschland der Datenschutz auf eine neue Ebene gehoben wurde, allein aus der Angst vieler kleiner Unternehmen resultierend, Abmahnungen zu erhalten. Auf der anderen Seite ist es kaum vorstellbar, dass die zuständigen Aufsichtsbehörden mit allen durch Verdachtsfälle ausgelösten Ermittlungen Herr der Lage werden. Somit bleibt die Frage, wie viel Schutz ein System bieten kann, welches sich nicht verfolgen lässt.
Bei den Seminarteilnehmern war der Konsens groß, dass die DSGVO schützen kann, solange jeder auch selbst darauf achtet, welche Daten man von sich im Internet preisgibt.

2.3 Datendiebstahl durch frei verfügbare Daten

Täglich posten Milliarden von Menschen sensible Daten, wie z.B. Urlaubsfotos, Posts über die ausgeartete Party der letzten Nacht, Informationen zum persönlichen Beziehungsstatus oder auch Fotos der eigenen Kinder. Jeder Post, aber auch jeder ‚Like' gibt ein Stück Persönlichkeit im Internet preis. Nach und nach formt sich das Bild einer Person, welches leicht kopiert werden kann. Dabei verfolgen Täter in der Regel eines von zwei Zielen: sie wollen sich entweder einen finanziellen Vorteil verschaffen oder dem Opfer persönlich schaden (Computerbetrug, 2018).

2.3.1 Finanzieller Schaden

Wie bereits erwähnt, reichen Stammdaten oft schon aus, um Verträge abzuschließen oder sie zu den eigenen Gunsten ändern zu lassen. Je umfangreicher der Datensatz, umso leichter wird es für den Täter mit den Daten Missbrauch zu betreiben.
Eine beliebte Methode ist es, mit dem geklauten E-Mail-Konto und ein paar persönlichen Informationen ausgedachte Szenarien an die Kontaktliste zu versenden und darin Familie und Freunde des Opfers um Geld zu bitten. Die Täter tun so, als wären die vermeintlichen Opfer im Urlaub beklaut worden und benötigten Geld für die Rückreise (Feil, 2017). Je mehr Informationen der Täter hat, umso glaubwürdiger kann er seine Geschichte formulieren.
Neben solchen gezielten Aktionen nutzen Täter E-Mail-Adressen auch, um massenweise Spam-Mails zu versenden. Dabei werden die Vorlagen immer trickreicher. Während wir uns heute noch über den nigerianischen Prinzen amüsieren, der uns sein Vermögen schenken möchte, wenn wir ihm nur die Transaktionsgebühr bezahlen, hört beim täuschend echtem Schreiben von PayPal, man möge seine Zugangsdaten verifizieren, der Spaß auf.

Das Bundeskriminalamt hat 2014 knapp 50.000 Fälle im Bereich Internetkriminalität registriert. Dabei liegt die Dunkelziffer jedoch bei ca. 90 Prozent (Ilex-Recht, 2015). Eine Studie von 2015 geht dabei sogar von jährlich 14,7 Millionen Fällen von Internetkriminalität aus, wobei alleine 84 Prozent im Bereich Phishing, Identitätsbetrug und Angriffe mittels Schadsoftware liegen (ebd.). Aus dieser Annahme ergebe sich nun ein Schaden von ca. 3,4 Milliarden Euro in Deutschland (ebd.).
Anders als bei üblichen Straftaten steht ein Aspekt im Vordergrund, der durch das Internet an Bedeutung gewinnt: der Täter braucht keine persönliche Nähe zum Opfer haben. Der Täter muss nicht einmal im selben Land leben. Daraus ergibt sich für die Opfer und Strafverfolgungsbehörden eine immense Hürde im Bezug auf die Verfolgbarkeit der Täter. Nicht umsonst rangiert Internetkriminalität auf Platz 10 der Hauptaktivitätsfelder der organisierten Kriminalität (Schulte am Hülse, 2015).

2.3.2 Persönlicher Schaden

Doch mit gestohlenen Identitäten lassen sich auch Schäden anrichten, die über das Maß finanzieller Interessen hinausgehen.
Ein Beispiel: Klaus möchte Petra näherkommen und kopiert ihr Profil auf Facebook, um mit ihren Freunden in Kontakt zu treten. Klaus hat es einfach, denn Petra hat ein sehr ausgeprägtes Profil. Klaus kopiert dieses sehr penibel und erhält dadurch Zugang zu ihrem Freundeskreis. Er erfährt noch mehr intime Details aus Petras Leben und dem Leben ihrer Freunde. Klaus kopiert nun auch Profile von Petras Freunden und verabredet sich letztendlich mit ihr unter einem der falschen Profile. Als sich Petra mit einem vermeintlichen Freund treffen möchte, steht plötzlich Klaus vor ihr.
Klaus hat sich in unserem Fall der Nachstellung gemäß ğ238 I Nr.2 StGB, dem sogenannten Stalking, strafbar gemacht. Doch nicht nur Stalking steht auf der Liste möglicher Folgestraftaten des Identitätsdiebstahls. Ebenso sind Mobbing, Verstöße gegen die Persönlichkeitsrechte und gegen Bildrechte denkbar. Das deutsche Strafgesetz kennt viele Tatbestände, die sich aus der Folge ergeben können, doch noch keinen für den Identitätsdiebstahl als solchen.

2.3.3 Diskussion: Brauchen wir einen neuen Straftatbestand?

Ein Gesetz schützt nicht davor, dass Straftaten begangen werden. Gesetze sind die Manifestation der Moralvorstellungen der Menschen, die sie festlegen. Ein moralisch gesunder Mensch würde die Persönlichkeitsrechte einer anderen Person auch wahren, wenn es kein gesondertes Recht gibt. Das Gesetz dient lediglich als Grundlage für die Verfolgbarkeit, denn in Deutschland gilt der Grundsatz „keine Strafe ohne Gesetz“ gemäß ğ1 StGB.
Da jedoch jede Folge, die aus Identitätsdiebstahl resultieren könnte, bereits durch einen Tatbestand gedeckt ist, scheint uns ein übergeordneter Tatbestand nicht erforderlich. Zumal die Verfolgbarkeit der Tat in Frage gestellt ist, so lange keine auf dem Identitätsdiebstahl aufbauende Straftat, wie z.B. Stalking, ausgeübt wird. Somit hätte zwar ein Identitätsdiebstahl-Tatbestand eine befriedigende Wirkung auf unser moralisches Empfinden, würde sich unseres Erachtens aber in der Praxis als nutzlos erweisen, da er ohnehin hinter schwereren Folgestraftaten zurücktreten würde.
Denkbar wäre es den Identitätsdiebstahl als qualifizierenden Tatbestand in Strafgesetze einzuführen, um den Persönlichkeitsrechten Rechnung zu tragen. Unangetastet davon bleiben für aggressives Vorgehen, wie die Manipulation von Programmen, um an Daten gewaltsam heranzukommen, ohnehin Tatbestände, wie z. B. das Abfangen von Daten, Computerbetrug. Diese bestehen und bilden eine solide juristische Grundlage zur Verfolgung der Internetkriminalität.
Die Meinungen der Zuhörer gingen bei dieser Diskussion auseinander: Ein Teil der Wortmeldungen befürwortete die Einführung eines solchen Tatbestands, da daraus die Schwere des Vergehens deutlicher zum Tragen käme, als es bei der strafrechtlichen Verfolgung der Auswirkungen von Identitätsdiebstahl der Fall wäre. Der andere Teil hielt die Straftatbestände, z. B. für Stalking, Mobbing oder finanziell entstandene Schäden, für ausreichend. Leider driftete die Diskussion an dieser Stelle etwas in den Bereich ab, in welcher Verbindung Moral und Gesetz zueinanderstehen (Henne-Ei-Problem: was war eher da, das Gesetz oder die Moral?).
Eine weitere Frage der Seminarteilnehmer lautete: ist die DSGVO nicht die rechtliche Grundlage für Identitätsdiebstahl als Straftatbestand? Unseres Erachtens erfüllt die DSGVO nicht den Charakter eines klassischen Straftatbestandes. Das liegt vor allem schon am äußeren Rahmen der Gesetzesverordnung, denn die Schwelle der Verfolgbarkeit ist bei der DSGVO deutlich niedriger angesetzt, hier genügt allein schon die Vermutung eines Verstoßes, als das im strafrechtlichen Kontext der Fall ist, wo ein

hinreichender Tatverdacht bestehen muss. Außerdem liegt die Zuständigkeit der Verfolgung bei Verstößen gegen die DSGVO bei den landesweiten Datenschutzbehörden im Gegensatz zur Staatsanwaltschaft, wie es im Strafrecht der Fall wäre (Art. 51ff. DSGVO). Auch die Art der Strafe bei DSGVO-Verstößen muss von Straftatbeständen abgegrenzt werden, denn Geldbußen werden im Gegensatz zu Geldstrafen nicht im Bundeszentralregister erfasst (Art. 84 DSGVO, Juraforum, 2018). Damit kann die DSGVO allein aus Formalitätsgründen nicht als Straftatbestand angesehen werden, da sie zum öffentlichen Recht gehört und nicht zum Strafrecht.

3 Schutzmaßnahmen

3.1 Optimaler Schutz

> Daten, die man nicht preisgibt, können auch nicht gestohlen werden.

Folgt man diesem Leitsatz bedeutet das für die digitale Identität folgendes:

- keine Online-Bestellungen, -Reservierungen, o.ä.
- keine online zugänglichen Kundenkonten (z.B. bei Mobilfunkanbietern)
- kein Online-Banking
- keine eigenen Aktivitäten in sozialen Netzwerken und im Optimalfall auch keine von Familien/Freunden/Bekannten
- keine E-Mail Korrespondenz bzw. Accounts
- keine Smartphones
- keine beruflichen oder ausbildungsbezogenen Accounts (z.B. Stud.IP, Löwenportal, u.ä.)

Gerade im Bezug auf die drei zuletzt aufgeführten Punkte stellt sich in der heutigen Zeit die Frage: ist das überhaupt realistisch?
Es ist zwar bspw. möglich, ohne Online-Zugang zu studieren, allerdings erkennt man schnell, dass das nicht ohne erheblichen Aufwand und entstehende Nachteile realisierbar ist. Einige universitären Veranstaltungen haben eine begrenzte Teilnehmerzahl, die ihm Fall der Martin-Luther-Universität Halle-Wittenberg durch die Anmeldungen zu der

Veranstaltung über die Onlineplattform Stud.IP eingehalten wird. Wie komme ich an die Information, wann und von wem diese Veranstaltung angeboten wird, wenn ich sie online nicht einsehen kann und selbst wenn ich das herausfinde, wie kann ich Kontakt zum Dozenten aufnehmen, um mich rechtzeitig anzumelden, wenn ich seine Kontaktdaten nicht online suchen kann?
An diesem Beispiel zeigt sich, dass der optimale Schutz heutzutage kaum praktikabel ist.

3.2 Zeitgemäße Schutzstrategien

Um bei allgemeinen Onlineaktivitäten den eigenen Schutz gewährleisten zu können, ist die Einhaltung folgender Maßnahmen ratsam (Wragge und Pachiali, 2015):

- Datensparsamkeit:
  - Die Freigabe von personenbezogenen Daten sollte nur nach genauer Prüfung der Website, die sie anfordert, und mit entsprechender Vorsicht erfolgen.
- Wahl sicherer Passwörter:
  - Passwörter sollten nicht aus Familiennamen, Haustieren, Geburtsdaten o.ä. bestehen und regelmäßig geändert werden.
- regelmäßige Updates von Geräten, Systemen und Software
- Kontrolle und Überblick behalten:
  - Kontoauszüge sollten regelmäßig überprüft werden.
  - Ratsam ist es auch, ab und an zu überprüfen, welche Daten über die eigene Person im Netz kursieren.
- Prüfen von Apps und Diensten:
  - Welche Berechtigungen wollen Apps und Dienste erhalten?
  - Benötigt eine Taschenlampen-App bspw. Zugriff auf meine Kontakte?
- Nutzen von WLAN und fremden Geräten nur mit Bedacht:
  - Websites sollte man nur über sichere Verbindungen aufrufen.
  - In E-Mail-Programmen sollte man verschlüsselte Verbindungen nutzen.

  - VPN-Dienste sind in fremden Netzwerken ebenfalls von Vorteil.

Bei Onlineaktivitäten in sozialen Netzwerken sollte man sich regelmäßig immer wieder die folgenden Fragen stellen (ebd.):

- Welche Informationen sind wirklich notwendig, um diesen Dienst zu benutzen?
- Könnten mir meine hochgeladenen Inhalte später peinlich sein oder unangenehme Konsequenzen haben? Könnten dadurch Andere geschädigt werden?
- Wer kann die Informationen sehen und welche Einstellungsmöglichkeiten gibt es dafür?
- Welche Rechte und Befugnisse beanspruchen die Anbieter für sich?

Um sich explizit auch gegen Identitätsdiebstahl zu schützen, können folgende Maßnahmen helfen (ebd.):

- Zwei-Faktor-Authentifizierung
  - Prinzip: man erhält beim Einloggen einen Code (z.B. per SMS) und erst mit diesem kann die Anmeldung durchgeführt werden.
  - Außerdem gibt es mittlerweile Apps, die speziell solche Codes erzeugen.
  - Damit ist der Login in ein Onlinekonto durch Angreifer nicht möglich, selbst wenn sie die Zugangskennung und das Passwort besitzen.
- Erkennen von verdächtigen Datensammlern:
  - Wie seriös ist die gerade besuchte Website?
  - Wer ist überhaupt Anbieter und Betreiber laut Impressum?
  - Welche Daten fordert ein Onlineformular und ist es zwingend erforderlich diese einzugeben?

3.3 Diskussion: Wie geht man als Lehrer/in mit Datenfahrlässigkeit von Schülern um?

Die Mehrheit der Seminarteilnehmer fühlt sich nicht für den Einzelfall verantwortlich, plädiert aber für die Aufarbeitung von Daten- und damit Identitätsschutz im Unterricht.
Anschließend wurde über die Art und Weise der Vermittlung dieses Lernstoffs diskutiert. Eine Wortmeldung schlug zum einen die Einführung eines neuen Fachs ‚Medienkompetenz' vor, zum anderen sollten regelmäßig auch Negativbeispiele im Unterrichtskonzept Anklang finden. Letzteres lehnten einige Wortmeldungen ab und machten andere Vorschläge. So könnte man eine Kennenlernrunde mithilfe der Facebook-Profile der Schüler/innen gestalten, um für Preisgabe personenbezogener Informationen zu sensibilisieren. Außerdem könnten Datenschutzprogramme oder -routinen genauso in den Schulalltag integriert werden wie die Benutzung von Office-Programmen. Damit wird das Thema Daten- und Identitätsschutz nicht einfach abgehandelt, sondern in den Schulalltag integriert.

4 Vom Opfer zum Täter

Digitale Identität birgt nicht nur eine Gefahr für uns, sondern bietet ungeahnte kriminologische Aspekte, die Straftaten begünstigen. Warum die Zahl computerkrimineller Betätigung ansteigt und inwiefern die digitale Identität diese Entwicklung begünstigt, soll der nächste Abschnitt erörtern. Zur Veranschaulichung wollen wir dabei eng am Beispiel illegaler Raubkopien arbeiten, da dieses Delikt besonders jüngere Menschen betrifft, alle Qualitäten der Anonymität im Netz demonstriert und trotz des Entstehens von immensen Schaden immer noch als Bagatelle in den Köpfen der Öffentlichkeit steckt. Des Weiteren lassen sich Parallelen zu ähnlichen Delikten in der realen Welt ziehen, um so den Kernunterschied zur digitalen Identität zu verdeutlichen.

4.1 Einführung in den Begriff der Urheberrechtsverletzung

Beschränkt man sich auf die subjektive Sicht, so ist das Urheberrecht das Herrschaftsrecht des Urhebers an seinem Werk (Rehbinder, 2010, Rn. 2; Loewenheim, 2010, ğ1 Rn. 1). Geschützt wird eine bestimmte kulturelle Geistesschöpfung (Rehbinder, 2010, Rn. 2). In der Kontrolle darüber liegt das Problem und die Gefahr, welche das Urhe-

berrecht zu verhüten versucht.
Besonderes Augenmerk wollen wir hierbei auf das Filesharing legen. Das Urheberrecht bestimmt in ğ12 I UrhG, dass allein der Urheber das Recht besitzt zu bestimmen, wie und ob sein Werk veröffentlicht wird. Mit der Weiterentwicklung im Feld der digitalen Welt mussten auch weitere Vervielfältigungstechniken aufgenommen werden. So gilt als Vervielfältigung auch die Digitalisierung und Speicherung auf der Festplatte oder gar dem bloßen Arbeitsspeicher, der besonders im Streaming-Bereich von Bedeutung ist (Schulze, 2013, ğ16 Rn.7). Das Herunterladen aus dem Internet ist folglich eine Vervielfältigung (ebd. ğ16 Rn. 13; Loewenheim, 2010, ğ16 Rn. 16ff.). Der User macht sich demnach mit dem Herunterladen einer Datei ohne Genehmigung des Urhebers strafbar.

4.2 Verbreitung durch Organisationen

Neben der Möglichkeit privater User, die legal erworbenen Kopien illegal zu vervielfältigen und über Filesharing zu verbreiten, stehen an oberster Stelle in sich strukturierte Organisationen. Diese Gruppen werden als Release-Groups bezeichnet (GVU, 2015). Sie bestehen aus unterschiedlichen Personen, von denen jede einen klaren Aufgabenbereich zu erfüllen hat. Vom ersten Beschaffen bis zur kopierschutzfreien Version verletzen diese Organisationen immer wieder den Tatbestand des ğ106 I UrhG, indem sie ohne Genehmigung urheberrechtlich geschütztes Material vervielfältigen oder öffentlich wiedergeben im Sinne von ğğ15 II, 19a UrhG.

4.3 Tätermotivation

Das Internet bietet Kriminalität aufgrund seiner Losgelöstheit von der physischen Welt nicht nur neue Spielräume, sondern es bedarf auch einer anderen Sichtweise auf die Tätermotivation. Das Wesen des Internets ist insoweit anarchisch geprägt, als dass der Austausch von Informationen ursprünglich frei war (Hoeren, 1995, S. 3298). Als Kommunikationsmittel war es von Kindesbeinen an nicht auf eine kommerzielle Nutzung des Datenflusses ausgerichtet (Peukert, 2014, S. 78).
Die Täter sehen sich nicht in der Täterrolle. Sie halten an der Informationsfreiheit, für die das Internet geschaffen wurde, fest und fügen sich nicht der Kommerzialisierung (Wiese, 2006, S. 698). Die Tätergruppen sind sich der Freiheit des Internets, die sich besonders durch Anonymität und erschwerter Verfolgbarkeit auszeichnet, stets bewusst (Rau, 2004, S. 71). Im Rahmen der nicht gewinnorientierten Release-Groups geht es

bei den Taten um Anerkennung und Ruhm innerhalb der Szene, wobei Profit sogar verachtet wird (ebd. S. 72).
Eine Reihe kriminologischer Theorien lassen sich zur Tätermotivation ableiten. Darunter zählen Gedanken, wie z.B. die Bagatellisierung oder die Ablehnung des Opfers, da große Musiker oder Softwareunternehmen doch genug Profit erzielen würden. Doch auch hierbei spielt die Anonymität eines jeden Täters für sich und die Chancen digitaler Identitäten eine tragende Rolle.
Nach der Theorie von Cohen bestehen innerhalb unserer Gesellschaft Subkulturen, die eigene ausgeprägte Werte und Normen besitzen, meist in Gegenwehr zu denen der Gesellschaft (Cohen und Short, 1979, S. 372f.). In diesen Kreisen finden vor allem Jugendliche Status und Anerkennung, die sie in unserer Gesellschaft auf anderem Wege nicht erlangen können (Kunz, 2008, Kapitel 2 Rn. 27). Bei einem Teil der Täter handelt es sich um weniger sozial integrierte Personen, die im Kreis ihrer Computeraffinität den Ausgleich an Anerkennung und sozialer Integration suchen. Aber auch Personen, die ein geregeltes Sozialleben pflegen, finden sich unter den Tätern wieder. Die digitale Identität ermöglicht es, solchen Subkulturen beizuwohnen, ohne die wahre Identität preisgeben zu müssen. Die Moral eines Menschen ist nicht abhängig von Gesetzen. Diese bieten lediglich einen Rahmen, in dem sich die Moral entfalten kann. Moral wird jedoch von der Gesellschaft geformt. So lernt der Täter in den Subkulturen eine eigene Moral.
Das Internet bietet aber auch hier ein neuartiges Problem: während wir in der realen Welt auf den direkten Kontakt mit Menschen angewiesen sind, herrscht in der digitalen Welt die Anonymität. Hinzu kommt die Losgelöstheit von physischen Grenzen. Eine soziale Interaktion ist begrenzt durch den Raum, in dem wir uns bewegen. Im Gegensatz dazu können sich soziale Netze im Internet weltweit erstrecken. Betrachtet man bspw. Facebook, so wird man feststellen, dass sich hier unzählige Netzwerke aufgebaut haben. Dadurch erhöht sich die Chance für den Delinquenten auf Gleichgesinnte zu stoßen signifikant und frei von Äußerlichkeiten. Der Mensch ist nicht mehr abhängig von dem Wohlwollen seiner Mitmenschen.
Die Tatgelegenheiten sind vermutlich so offensichtlich wie in keinem anderen Kriminalitätsbereich. Die Anonymität und Distanz, die das Internet bietet, geben dem Täter Spielraum und Sicherheit und senken die Kosten, wie z.B. das Entdeckungsrisiko. Das größte Problem dabei ist die Identifizierung des Nutzers. Dies geschieht in aller Regel über die IP-Adresse des Client oder des Servers. Heute ist es auch ohne großes technisches Know-How möglich, eine IP-Adresse zu verbergen bzw. auf eine andere

umzuleiten. Die Möglichkeiten reichen von Programmen, die eine zufällige IP-Adresse generieren, bis zu Browsern, die mit allen anderen Nutzern die IP-Adressen tauschen, was eine Ermittlung des Täters unmöglich macht (Lang, 2009, S. 129). Eine Studie der University of Washington hat gezeigt, wie IP-Adressen manipuliert werden können, sodass Mahnschreiben bspw. an die IP-Adresse eines Druckers gehen (Piatek, Kohno und Krishnamurthy, 2015, S. 1ff.). Demzufolge kann jeder Nutzer Opfer einer solchen Manipulation werden.

5 Hat die Informatik/die Informatikerin/der Informatiker im Bezug auf diese Thematik eine Verantwortung?

Unseres Erachtens bildet die Informatik mit ihren Berufsgruppen die Schnittstelle zwischen Endanwender und Unternehmen, die Daten in irgendeiner Form erheben und verarbeiten. Demzufolge liegt ein großer Teil der Verantwortung bzgl. des Datenschutzes beim Informatiker, denn die Unternehmen müssen rein formal die rechtlichen Verordnungen einhalten, die Umsetzung dieser liegt aber in den Händen unserer Berufsgruppe. Wie wir in unseren Betrachtungen unter dem Punkt Schutzmaßnahmen bereits gesehen haben, ist es heutzutage nicht mehr möglich, sich von jeglicher Online-Aktivität fernzuhalten, ohne dadurch auch ein Stück Lebensqualität abzugeben. Damit sind die Endanwender auf eine konsequente und korrekte Umsetzung der Datenschutzrichtlinien durch unsere Arbeit angewiesen.

6 Quellen und weiterführende Literatur

ABELS, Heinz, 2009. *Einführung in die Soziologie. Band 2: Die Individuen in ihrer Gesellschaft.* 4. Auflage. Wiesbaden: VS Verlag. ISBN 3-531-16634-4.

BOHL, 2018. Privacy Shield vs. DSGVO: Rechtslage beachten. In: *sc-networks.de* [online]. Zugriff am 28.07.2018. Verfügbar unter: https://www.sc-networks.de/blog/privacy-shield-vs-dsgvo-rechtslage-beachten/.

GESELLSCHAFT ZUR VERFOLGUNG VON URHEBERRECHTSVERLETZUNGEN e.V., 2015. Verbreitungsweg illegaler Kopien. In: *gvu.de* [online]. Zugriff am 18.05.2015. Verfügbar unter: http://www.gvu.de/26_Illegale_Kopien.htm.

HOEREN, Thomas, 1995. Das Internet für Juristen - eine Einführung. In: *NJW.* 1995, S. 3295-3298

KELLER, Gabriela, 2017. Datenhandel: Die Vermessung des deutschen Volkes. In: *Berliner Zeitung* [online]. 29.09.2017 [Zugriff am 28.07.2018]. Verfügbar unter: https://www.berliner-zeitung.de/politik/datenhandel-die-vermessung-des-deutschen-volkes-28509076.

KEUPP, Heiner, 2000. Identität. In: *Spektrum* [online]. Zugriff am: 28.07.2018. Verfügbar unter: https://www.spektrum.de/lexikon/psychologie/identitaet/6968.

KIRSCH, Marcus, 2016. Datenschutz-Grundverordnung: Bußgelder und Sanktionen. In: *datenschutzbeauftragter-info* [online]. 17.03.2016 [Zugriff am 28.07.2018]. Verfügbar unter: https://www.datenschutzbeauftragter-info.de/datenschutz-grundverordnung-bussgelder-und-sanktionen/.

KUNZ, Karl-Ludwig, 2008. *Kriminologie: eine Grundlegung.* 5. Auflage. Bern: Haupt Verlag. ISBN 978-3-8252-1758-7.

LANG, Alexander, 2009. *Filesharing und Strafrecht.* 1. Auflage. Berlin: Logos. ISBN 978-3-8325-2020-5.

LOEWENHEIM, Ulrich, 2010. *Urheberrecht: Kommentar.* 4. Auflage. München: C.H. Beck. ISBN 978-3-406-59033-7.

o. V., 2018. Datenhandel: Alle wollen den Datenschatz heben. In: *datenschutz.org* [online]. Zugriff am 28.07.2018. Verfügbar unter: https://www.datenschutz.org/datenhandel/.

o. V., 2018. Identitätsdiebstahl. In: *computerbetrug.de* [online]. Zugriff am 28.07.2018. Verfügbar unter: https://www.computerbetrug.de/sicherheit-im-internet/identitaetsdiebstahl.

o. V., 2018. Identitätsdiebstahl. In: *juraforum.de* [online]. Zugriff am 28.07.2018. Verfügbar unter: https://www.juraforum.de/lexikon/identitaetsdiebstahl.

PEUKERT, Alexander, 2014. Das Urheberrecht und die zwei Kulturen der Online-Kommunikation. In: *GRUR-Beilage*. 2014, S. 77-93.

PAITEK, Michael, Tadayoshi KOHNO und Arvind KRISHNAMURTHY, 2015. Challenges and Directions for Monitoring P2P File Sharing Networks - or - Why My Printer Received a DMCA Takedown Notice. In: *University Washington* [online]. Zugriff am 28.07.2018. Verfügbar unter: http://dmca.cs.washington.edu/dmca_hotsec08.pdf.

RAU, Lars, 2004. *Phänomenologie und Bekämpfung von Cyberpiraterie.* 1. Auflage. Göttingen: Cuvillier. ISBN 3-86537-246-5.

REHBINDER, Manfred, 2010. *Urheberrecht: ein Studienbuch.* 16. Auflage. München: C.H. Beck. ISBN 978-3-406-59768-8.

SCHULTE AM HÜLSE, Dr. Ulrich, 2015. Nehmen Phishing-Fälle zu? Der Anstieg im Bereich Cybercrime. in: *anwalt.de* [online]. 26.11.2015 [Zugriff am 28.07.2018]. Verfügbar unter: https://www.anwalt.de/rechtstipps/nehmen-phishing-faelle-zu-der-anstieg-im-bereich-cybercrime_075868.html.

SCHULTE AM HÜLSE, Dr. Ulrich, 2015. Zunehmende Fälle beim Phishing? Cybercrime erfährt laut BKA deutlichen Anstieg. In: *ilex-recht.de* [online]. 08.10.2015 [Zugriff am 28.07.2018]. Verfügbar unter: https://www.ilex-recht.de/nachricht-im-detail/fallsteigerung-beim-phishing-cybercrime-erfaehrt-laut-bka-deutlichen-anstieg.html.

SCHULZE, Gernot, 2013. *Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz, Kommentar.* 4. Auflage. München: C.H. Beck. ISBN 978-3-406-62747-7.

FEIL, Thomas, 2017. Rechtsanwalt gegen Identitätsdiebstahl. In: *recht-freundlich.de* [online]. 24.01.2017 [Zugriff am 28.07.2018]. Verfügbar unter: https://www.recht-freundlich.de/identitaetsdiebstahl/rechtsanwalt-identitaetsdiebstahl.

WIESE, Heiko, 2006. Aufspüren von Pirateriefällen im Netz. In: *ZUM*. 2006, S. 696-701.

WRAGGE, Alexander und David PACHALI, 2015. In: *iRights.info* [online]. 02.02.2015 [Zugriff am 28.07.2018]. Verfügbar unter: https://irights.info/artikel/identittsdiebstahl-im-internet/7227.