Wie können wir digital unsichtbar werden?

Julia Podlipensky
Matrikelnummer: 765550

Researchprojekt Interactive Media Design
Wintersemester 2023/24
Referent: Prof. Tsunemitsu Tanaka

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Abstract

Die Arbeit verfolgt das Ziel der Untersuchung unserer digitalen Unsichtbarkeit. Es wird sich der konzeptionellen Ergründung, wie wir digital unsichtbar werden können, angenommen. Das digitale Sichtbarkeitsverhältnis lässt sich auf der ersten Stufe der digitalen Sichtbarkeit über Zugänglichkeit von Informationen über uns beschreiben. Gesellschaftliche Praktiken in der digitalisierten Gesellschaft hinterlassen eine digitale Spur aus Daten. Da ohne Daten oder die digitale Spur, das Digitale unsichtbar bleibt, müssten Prozesse wie Datenminimierung, Datenumgangskontrolle und Datenlöschung eingeleitet werden. Die digitale Unsichtbarkeit wird dem Grad 0 einer Unbeobachtbarkeit zugeschrieben. Diese besteht aus der Anonymität einer Person, der Unverkettbarkeit zu Handlungen und Charakteristiken mit der Person, und der Unentdeckbarkeit von Informationen aus dieser digitalen Spur. Eine Person kann mehrere digitale Teilidentitäten besitzen, die abhängig von Bedingungen im Sichtbarkeitsverhältnis für den Beobachter jeweils unsichtbar sind. Die Arbeit kommt zur Auslegung einer absoluten und relativen digitalen Unsichtbarkeit. Bei Ersterem wird das Risiko eines möglichen Beobachters minimiert und legt den Fokus auf die maximale Datenminimierung und Datenlöschung. Zweiteres ist abhängig vom Sichtbarkeitsverhältnis und legt den Fokus auf die Anonymität und die Unentdeckbarkeit. Die Erörterung der Motivation hinter der Frage unserer digitalen Unsichtbarkeit, kommt zum Schluss, dass die Förderung der Autonomie, bzw. die Befähigung zum selbstständigen Handeln in einem potenziellen Sichtbarkeitsverhältnis, die zentrale Erkenntnis dieser Arbeit ist.

Inhaltsverzeichnis

Inhalt

1. Konventionen

1.1 Zitierstil

Die in dieser Forschungsarbeit zitierten Inhalte entsprechen den Vorgaben der 7. Auflage der American Psychological Association. Bei indirekten Zitaten werden im Textverweis der Autor, das Erscheinungsjahr des Werkes und bei direkten Zitaten die Seitenzahl zusätzlich angegeben. Die vollständigen Quellenangaben sind im alphabetisch nach Nachnamen sortierten Literaturverzeichnis zu finden.

1.2 Methodik

Für die Bearbeitung der Forschungsfrage wurde in dieser Arbeit die Methode der Literaturrecherche durchgeführt. Zur Durchführung der Recherche wurden Bücher, wissenschaftliche Paper und Fachartikel sowie Fachbeiträge hinzugezogen. In Ausnahmefällen wurden Blog-Beiträge als auch Websiteartikel von Experten zum Heranziehen eines Sachverhaltes verwendet. Die Rechercheergebnisse basieren hauptsächlich auf Quellen aus den Wissenschaftsbereichen der Computerwissenschaft, Soziologie, Philosophie und der Rechtswissenschaft. Zunächst wurden Aspekte des digitalen Sichtbarkeitsverhältnisses und des Sichtbarkeitsprozesses von Daten ergründet. Anschließend wurden die Zusammenhänge und Definitionen der Begriffe der Forschungsfrage anhand der Unbeobachtbarkeit und der Identität analysiert, um das Ergebnis unserer digitalen Unsichtbarkeit feststellen zu können. Darauf aufbauend wurde die Recherche auf die Motivation hinter der Forderung nach digitaler Unsichtbarkeit ausgeweitet, um ein umfassenderes Verständnis der Beobachtungsverhältnisse und den dahinterliegende Bedürfnissen zu erreichen. Die Ergebnisse der jeweiligen Kapitel wurden anschließend in der Diskussion zur Bearbeitung der Frage zusammengeführt, als auch die Limitationen der Bearbeitung geschildert.

2. Einführung digitale Sichtbarkeit

Die allgemeine Definition der Sichtbarkeit setzt den menschlichen Wahrnehmungssinn des Sehens voraus. Die Sichtbarkeit eines Objekts in der Natur bezieht sich grundsätzlich auf absorbiertes und reflektierendes Licht, welches von diesem Objekt in unser Auge fällt und dieses somit visuell wahrgenommen werden kann. In der analogen Welt ist die Möglichkeit der Sichtbarkeit sehr eng an unseren Wahrnehmungsraum geknüpft, welcher sowohl räumliche als zeitliche Grenzen aufweist (Thompson, 2005).

Bleibt man beim Sehsinn und betrachtet zusätzlich das Sichtbarwerden einer Person, muss sich diese Person im Wahrnehmungsraum des Beobachters befinden. Dadurch befindet sich der Beobachter auch im Wahrnehmungsraum der Person und könnte somit auch von dieser gesehen werden – vorausgesetzt er hat keine Tarnung oder Hilfen. Der Beobachter kann zum Beobachteten werden und die Sichtbarkeit wäre damit aufeinander bezogen [1] .

Im Digitalen ist diese Verbindung zur räumlich-zeitlichen Nähe zueinander fast vollständig aufgelöst. Sichtbar oder Unsichtbar zu werden ist damit eine Frage der verfügbaren Information über eine Person, dem Zugang zu dieser über Räume und Zeiten hinweg, als auch dem Wissen oder Nichtwissen, ob man beobachtet wird oder nicht (Thompson, 2005). Deswegen spricht man im Digitalen nicht mehr von Un/Sichtbarkeit im Wahrnehmungssinn des Sehens, sondern erweitert diesen auf die allgemeine Wahrnehmbarkeit und dem Engagement des Beobachters. Dabei unterscheidet man im Digitalen in drei Stufen der Sichtbarkeit [2] : „being noticable“, „being heard or noticed“ und „being recognized or respected“ (Brantner & Stehle, 2021).

Die erste Stufe „being noticable“ , oder zu Deutsch bemerkbar zu sein, bedeutet, dass die soziomaterielle Darstellung des Verhaltens von Menschen, Kollektiven, technischen Geräten oder der Natur in einer Form existiert, die von Dritten beobachtet werden kann. Dabei können die Akteure absichtlich oder unabsichtlich ihre Sichtbarkeit durch die Verfügbarkeit von Informationen, die Genehmigung zur Weitergabe von Informationen und die Zugänglichkeit von Informationen für Dritte beeinflussen (Stohl et al., 2016; Branter & Stehle, 2021).

Die zweite Stufe bezieht sich auf „being heard or noticed“, also gehört oder bemerkt zu werden. Diese Möglichkeit ergibt sich, wenn etwas in einem Medium präsent ist und die Aufmerksamkeit anderer erregt (Branter & Stehle, 2021).

Die dritte Stufe „being respected or recognized“, übersetzt respektiert und anerkannt zu werden, wird meist in der Forschung zur Diversität und Ungleichbehandlung herangezogen. Dabei wird Sichtbarkeit als Kernelement für die Mitbestimmung im öffentlichen Raum betrachtet, die entweder zu gegenseitiger Anerkennung oder mehr Kontrolle führen kann. Das erreichen der ersten zwei Stufen garantiert jedoch nicht die Sichtbarkeit auf dritter Stufe. Man kann sozusagen übersehen und damit unsichtbar werden (Branter & Stehle, 2021).

Diese Stufen verhalten sich vom Einfluss ähnlich wie der Aufbau von Einflusssphären, welche sich konzentrisch um uns als Individuum, die Familie und Freunde, weitere äußere soziale Kreise bis hin zu Regierungen und weltweiten Unternehmen spannen. Dabei vermindert sich das Vertraute als auch der Einfluss auf die Sphäre, je weiter man aus dem konzentrischen Modell herausgeht. Den meisten Einfluss besitzen Menschen somit innerhalb der bekannteren inneren sozialen Sphäre (Stasch, o.J.).

1: *“What we see is that which lies within our field of vision, where the boundaries of this field are shaped by the spatial and temporal properties of the here and now. Visibility is situated: the others who are visible to us, are those who share the same spatial-temporal locale. Visibility is also reciprocal (at least in principle): we can see others who are within our field of vision, but they can also see us (provided that we are not concealed in some way). It is the situated visibility of co-presence.”* (Thompson, 2005, S.35)

2: *“Digital visibility” refers to perceptibility as the likelihood of being ‘seen’ in the sense of being noticeable (this understanding is closest to the original understanding), in being heard or noticed, or in the sense of being respected or recognized.”* (Brantner & Stehle, 2021, S. 1)

Dies ist auch nicht verwunderlich, da das Sichtbarkeitsverhältnis zwischen zwei Parteien auch ein Machtverhältnis beschreibt. Mit dem sinkenden Einfluss im Sphärenmodell nach außen hin, steigt auch die Wahrscheinlichkeit einer Machtungleichheit im Sichtbarkeitsverhältnis. Michel Focault nutzt für die Beschreibung dieser Ungleichheit das Modell des "Panoptikons" [1] , wo Machtbeziehungen asymmetrisch verflochten sind (Focault, 1977). Ein Akteur kann dabei sehen (informiert werden) und der andere Akteur wird gesehen, obwohl er keine Kontrolle über das wie und wann hat (Kvakic & Wærdahl, 2022). Der Soziologieprofessor Brighenti kommt hierbei zum Fazit, dass die Sichtbarkeit ein zweischneidiges Schwert ist, welches gleichzeitig befähigend und entmündigend ist [2] .

Nach diesem Modell würde damit die Frage von Bedeutung sein, wer überhaupt darüber entscheiden sollte was sichtbar werden soll und was unsichtbar bleibt. Sollte es nicht für das Individuum zu einem gewissen Grad möglich sein, Kontrolle über die Sichtbarkeit des wie und wann zu erlangen? Zu bestimmen wann man digital sichtbar - und speziell für diese Arbeit - wann man digital unsichtbar sein möchte?

Um über die digitale Unsichtbarkeit zu bestimmen, muss diese zu Beginn der Weiterarbeit genauer definiert werden. Hierfür kann die erwähnte erste Stufe der digitalen Sichtbarkeit herangezogen werden, um zu untersuchen, inwieweit man sich der Bemerkbarkeit bzw. der Beobachtbarkeit Dritter entziehen kann.

1: Panoptikon ist ein Begriff vom Philosoph Jeremy Bentham und beschreibt den Entwurf eines perfekten Gefängnisses, welches die durchgehende Beobachtung der Inhaftierten gewährleistet (Foucault, 1977).

2: *"visibility is a double-edged sword: it can be empowering as well as disempowering."*
(Brighenti, 2007, S. 334)

3. Digitale Unsichtbarkeit

3.1 Daten und deren Unsichtbarkeiten

Wenn wir in der digitalen Welt unterwegs sind, erzeugen wir Daten. Sei es beispielsweise bei Teilnahme an Social Media, hören von Musik über Streaming Anbieter, Eingaben in Suchmaschinen, Self-Tracking auf Gesundheitsapps, Speichern von Bilderalben in Clouds, Ausführung elektronischer Zahlungen mit der EC- oder Kreditkarte oder das Reisen mit dem Reisepass in andere Länder. Es kann aus fast allem Daten erzeugt werden, wenn maschinenlesbare Merkmale vorhanden sind. Dies geht drauf zurück, dass gesellschaftliche Praktiken in der digitalisierten Gesellschaft Spuren erzeugen (Nassehi, 2019).

Bruno Latour spricht dabei auch vom Hinterlassen einer digitalen Spur (2013). Jedoch muss diese digitale Spur aufgenommen, aufbereitet und vor allem in Informationen interpretiert werden, um einen Mehrwert für jemanden zu erzeugen (Nassehi, 2019). Der Soziologe Armin Nassehi beschreibt weiter wie digitale Spuren erst rekombiniert werden müssen:

> *„Die Welt wird durch eine Realitätsebene verdoppelt, die nicht einfach diese Welt abbildet, sondern mit den Spuren umgeht, die an Schnittstellen zwischen Datensätzen und ihrer Umwelt anfallen – durch Sensorik aller Art, aber auch durch die Kombinatorik von Datensätzen. In solchen Datensätzen werden jene Muster errechnet, mit denen sich etwas anfangen lässt "(Nassehi, 2019, S.147)*

Daten sind auch erstmal nichts anderes als Kombinationen von 1 und 0, die zu etwas verarbeitet werden müssen. Man kann auch von einer anfänglichen Daten-Unsichtbarkeit bzw. eines nötigen Sichtbarkeitsprozesses für Daten reden (Neumayer et al., 2021). Die Autoren Neumayer et al. beziehen sich dabei genauer auf die Unsichtbarkeit in Daten aus sozialen Medien für Forscher, die diese auf soziale Phänomene und gesellschaftliche Muster untersuchen. Diese sind aber zum großen Teil verborgen oder nur für die Unternehmen, welche die Daten speichern, sichtbar. In letzter Zeit wurde den Sichtbarkeitsverfahren viel Aufmerksamkeit gewidmet, da Unternehmen Zugang zu diesen Daten gewähren oder den Zugang für Forscher beschränken (Neumayer et al., 2021). In diesem Fall müsste man weiter ergründen, inwieweit unzugängliche Daten von beispielsweise Unternehmen überhaupt als unsichtbar gelten können.

In dieser Quelle bezieht sich der Sichtbarkeitsprozess von Daten eher auf das „zugänglich machen" von Daten für Forscher: Das erarbeitete Modell des Sichtbarkeitsverfahrens kann jedoch auch für diese Arbeit von Bedeutung sein, um zu wissen an welchen Punkt man ansetzen könnte, um digital unsichtbar zu werden.

Das Sichtbarkeitsverfahren lässt sich in vier sozio-technischen Dimensionen beschreiben (Neumayer et al., 2021):

- Menschen und Intentionalität: Diese Dimension konzentriert sich darauf, wie Personen Datenspuren erstellen oder hinterlassen, mit dem Ziel diese sichtbar zu machen oder zu verschleiern. Zum einen erzeugen Personen absichtlich Daten mit dem Wunsch nach Selbstdarstellung, sozialer Verbindung, Informationsaustausch, persönlichem Branding oder sogar strategischer Manipulation der eigenen Online-Präsenz. Zum anderen können Personen durch ihre Online-Aktivitäten unwissentlich Daten erstellen, z. B. wenn ihre Aktionen automatisch von der Plattform aufgezeichnet werden oder wenn ihre Interaktionen

ohne ihre ausdrückliche Absicht von Algorithmen verfolgt werden.

- Zugänglichkeit und Form: Die Sichtbarkeit von Daten wird dadurch beeinflusst, wie Daten in verschiedenen Formen zugänglich gemacht werden können, beispielsweise durch Datenschutzeinstellungen die von Nutzern vorgenommen wurden, Vereinbarungen zur gemeinsamen Nutzung von Daten, Datenanalysemethoden oder rechtliche Rahmenbedingungen zur Speicherung und Herausgabe von Daten.
- Technologien und Tools: Diese Dimension enthält die Speicherung und Beobachtung von Daten als Sammlungen durch verschiedene Technologien wie Dateninfrastrukturen, APIs und Analysesoftware. Datenverarbeitung durch künstliche Intelligenz kann hierbei mittlerweile auch dazugezählt werden.
- Bedeutung und Vorstellungskraft: In dieser Dimension wird untersucht, inwiefern Daten die Fähigkeit zugeschrieben werden, soziale Phänomene zu messen, darzustellen oder zu enthüllen, und wie Forscher und Analysten den Daten auf der Grundlage ihrer eigenen Vorstellungen und Interpretationen eine Bedeutung zuschreiben. Hierbei spielt die Verkettbarkeit von Daten zu Informationen eine große Rolle.

Während die Dimension der Menschen und Intentionalität sich in der Nähe zum Bereich der Unsichtbarkeit befindet, liegt die Dimension der Bedeutung und Vorstellungskraft mit dem Ziel Informationen zu erschließen in der Nähe zum Bereich des Sichtbaren. Neumayer et al. bringen hierbei den Bereich des Quasi-Sichtbaren mit ein, welcher Visualisierungsprozesse von Daten sowohl ins Sichtbare als auch ins Unsichtbare erlaubt. Entweder können Daten vom Quasi-Sichtbaren durch Herausgabe der Daten von Unternehmen und Methoden der Interpretationen zu Informationen sichtbar gemacht werden. Oder Daten können vom Quasi-Sichtbaren durch die permanente Löschung von Unternehmen unsichtbar gemacht werden (Neumayer et al., 2021).

Die ersten Dimensionen des Visualisierungsprozesses decken sich mit der Beschreibung der ersten Ebene der digitalen Sichtbarkeit, welche die Verfügbarkeit, Genehmigung der Weitergabe und Zugänglichkeit erläutert (Stohl et al., 2016). In der ersten Ebene wird jedoch schon direkt von Informationen gesprochen, wobei im Sichtbarkeitsprozess noch von Daten die Rede ist. Die Vermutung liegt hierbei, dass sobald Daten erzeugt und erhoben werden, die Zugänglichkeit als auch die Interpretation in Informationen sehr nahe liegt. Der Prozess von quasi-sichtbaren Daten zu sichtbaren Informationen ist entweder ab der Zugänglichkeits-Dimension erlaubt worden oder kann beispielsweise durch externe Umstände wie Änderungen der Datenschutzrichtlinien, Plattformaktualisierungen oder auch Datenschutzverletzungen eingeleitet werden (Neumayer et al., 2021).

Um die Frage nach der digitalen Unsichtbarkeit aufzugreifen, bleiben ab der Stufe der Datenerzeugung zwei Möglichkeiten:

Man reguliert ständig die Dimension im Stadium des Quasi-Sichtbaren, um die Daten in diesem Bereich zu belassen: der Dimensionen der Zugänglichkeit und Form und die Dimension der Technologien und Tools – also der Zugänglichkeit, Speicherung und Verarbeitung von Daten. Man könnte hierbei von einem Prozess der Daten-Umgangskontrolle sprechen.

Man leitet den Sichtbarkeitsprozess vom Quasi-Sichtbaren ins Unsichtbare ein und lässt eine permanente Löschung veranlassen. Man könnte hierbei von einem Prozess der Dateneliminierung sprechen.

In beiden dieser Möglichkeiten ist der eigene Einfluss auf die Daten nicht so hoch, da man stark von der jeweiligen Institution oder dem geltenden Recht abhängig ist. Der meiste eigene Einfluss besteht in der Dimension der Menschen und Intentionalität, also der Regulierung von der eigenen digitale Spur und dem Einschränken der Möglichkeiten für Datenerzeugung. Denn wenn man die absolute digitale Unsichtbarkeit anstrebt, bleibt ohne Daten oder Datenspuren das Digitale unsichtbar (Hui, 2013). Der Ansatz dafür nennt sich Datenminimierung und liefert eine standhaftere Annäherung für die Definition der digitalen Unsichtbarkeit.

3.2 Unbeobachtbarkeit als digitale Unsichtbarkeit

Die Annäherung zur digitalen Unsichtbarkeit erfolgt über die Begriffe wie „Anonymität", „Unentdeckbarkeit", „Unverkettbarkeit" und „Unbeobachtbarkeit" (Pfitzmann et al., 2010). Die Datenschutzforscher Marit Hansen und Andreas Pfitzmann haben sich über 10 Jahre hinweg angenommen, eine allgemeine und mehrsprachige Terminologie für Diskussionen über Privatheit und Datenschutz durch Datenminimierung zu entwickeln [1] .

Privatheit bezieht sich dabei auf den Anspruch von Individuen, Gruppen oder Institutionen selbst zu bestimmen, zu welchem Grad Informationen über sie mit anderen geteilt werden können [2] .Dieser Anspruch ist dementsprechend sehr individuell, da jeder für sich den Grad, die Art und die Zeit der Informationsteilung festlegen muss. Die derzeitiger Erkenntnis der Arbeit über digitale Unsichtbarkeit ist dagegen der absolute Anspruch, keine Daten oder digitale Spur zu erzeugen, welche durch Sichtbarkeitsprozesse Informationen sichtbar machen kann. Die Terminologie aus diesem Bereich kann jedoch auch dabei helfen, die digitale Unsichtbarkeit zu verstehen.

Die Begriffe werden innerhalb eines speziellen Settings eines Systems definiert, in welchem Sender Nachrichten an Empfänger innerhalb eines abgeschlossenen Kommunikations-Netzwerk senden. Laut den Forschern sind diese Begriffe aber auch für eine Diskussion in einem breiteren Kontext anwendbar. Dabei wird allgemeiner von Subjekten gesprochen, bei denen es sich um Akteure handelt, die eine Aktion ausführen (z. B. Sender) oder Akteure, die auf die Aktion reagieren (z. B. Empfänger). Der Raum zwischen den Akteuren, ist der Raum, indem digitale Spuren der Aktionen durch Daten entstehen können (Pfitzmann et al., 2010). Im weiteren wird sich jedoch anhand der Quelle auf das spezielle Setting fokussiert.

Die „Beobachtbarkeit" wird aus der Perspektive eines Angreifers definiert. Dieser kann daran interessiert sein zu überwachen, wer die Subjekte sind, welche Kommunikation stattfindet, welche Kommunikationsmuster es gibt, oder sogar die Kommunikation zu manipulieren. Woran der Angreifer interessiert ist, wird „item of interest" oder kurz IOI genannt. Der Angreifer kann ein Außenstehender sein, der Kommunikationsleitungen des Netzwerks anzapft oder ein Insider, der an der Kommunikation teilnehmen kann und zumindest einige Endknoten oder Endgeräte kontrolliert (Pfitzmann et al., 2010).

Die **Unverkettbarkei**t bedeutet, dass der Angreifer bei zwei oder mehrerer IOIs (z. B. Subjekte, Nachrichten, Aktionen, ...) innerhalb des Systems nicht ausreichend unterscheiden kann, ob diese IOIs zusammenhängen oder nicht. Eine userzentrierte Definition sagt zusammenfassend aus, dass die Unverkettbarkeit gewährleistet, dass der Nutzer nicht mit der Tatsache der Nutzung oder seinen Nutzungsmustern eines Services in Verbindung gebracht werden kann.

1: Die Quelle ist in englischer Sprache verfasst worden, enthält aber für alle definierten Begriffe eine geprüfte deutsche Übersetzung (Pfitzman et al., 2010)

2: *"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."* (Westin, 1967, S.7)

Die **Anonymität** eines Subjektes bedeutet, dass ein Subjekt für den Angreifer nicht identifizierbar innerhalb einer beobachteten Anonymitätsmenge an Subjekten ist. Erweitert mit der Unverkettbarkeit bezieht sich Anonymität auf einen Zustand, bei dem die Identität eines Subjekts nicht bekannt ist oder nicht mit einem IOI, bspw. ihren Aktionen in Verbindung gebracht werden kann.

Die **Unentdeckbarkeit** von IOIs bedeutet, dass der Angreifer nicht ausreichend unterscheiden kann, ob dieses IOI existiert oder nicht. Die Unentdeckbarkeit bezieht sich auf den Zustand eines IOIs, nicht beobachtbar oder nicht leicht nachweisbar zu sein, in dem die Handlungen oder Daten eines Subjektes nicht beobachtet oder überwacht werden können. Meist ist damit im Anwendungsfall gemeint, dass das IOI nicht ausreichend von anderen Daten oder Rauschen unterschieden werden kann [1] .

Die **Unbeobachtbarkeit** ist der Begriff, der der digitalen Unsichtbarkeit am nächsten kommt. Die Definition schließt sich aus der Anonymität und der Unentdeckbarkeit zusammen. Dies bedeutet, dass ein IOI für daran unbeteiligte Subjekte unentdeckbar ist und die am IOI beteiligten Subjekte Anonymität (auch vor anderen am IOI beteiligten Subjekten) genießen [2] .Die Unbeobachtbarkeit impliziert Anonymität als auch Unentdeckbarkeit.

Der Begriff „Unbeobachtbarkeitsdelta“ bezeichnet einen Grad dafür, inwieweit ein IOI unentdeckt von unbeteiligten Subjekten ist und inwieweit die Anonymität der am IOI beteiligten Personen auch voneinander bewahrt wird. Eine perfekte Unbeobachtbarkeit eines IOIs hat ein Delta von 0 und nimmt mit fallender Unbeobachtbarkeit stetig ab. Beträgt das Unbeobachtbarkeitsdelta einen bestimmten negativen Wert, so kann laut Pfitzman et al. dieser nicht mehr steigen, da der Angreifer keine Information vergisst. Ob eine Unbeobachtbarkeit vom Grad 0 tatsächlich möglich ist, wird nicht erwähnt.

In diesen Definitionen ist anhand des konstruierten Systems von einem Angreifer die Rede, der den Wunsch nach der Erkennbarkeit eines IOI oder der Identifikation eines Subjekts hat. Dem liegt zugrunde, dass der Angreifer zu allererst ein dritter Beobachter ist, welcher die Intention hat, das was ihn interessiert, einzusehen. Die Motivation als Angreifer dahinter, die interpretierte Information aus dem Gesichteten zum Angriff auf ein mögliches Subjekt zu verwenden, wird nicht näher erläutert. Mögliche Gründe werden in einem späteren Kapitel aufgefasst. Die Definitionen beschreiben primär, wie ein Subjekt sich der Beobachtung eines Angreifers entziehen kann.

Transferierend auf die digitale Unsichtbarkeit lässt sich für das Erreichen einer Unbeobachtbarkeit feststellen, dass die Beeinflussung der Identifikation des Subjektes durch Rückschlüsse auf die Identität durch die hinterlassene digitale Spur als auch die Entdeckbarkeit einer digitalen Spur selbst von Bedeutung ist.

Aus diesem Grund folgt der meist verwendete Mechanismus, der zu einem Grad an Unbeobachtbarkeit beiträgt, einem Mechanismus zur Anonymisierung des Subjektes (bspw. durch Datenminimierung identifizierbarer Daten [3])in Kombination mit dem erzeugen von „Dummy-Traffic“ (bspw. Datenverwässerung durch Rauschen oder Menge an Desinformation [4]).

Heutzutage ist es jedoch schwer oder fast unmöglich geworden keine identifizierbare digitale Spur zu erzeugen, da immer mehr Anwendungen personenbezogene Daten benötigen. Aus diesem Grund ist es wichtig auch die Verwertung, Speicherung und Nutzung der erhobenen Daten zu kontrollieren (Pfitzmann et al., 2010).

Zur Methode der Datenlöschung wurde noch nichts erwähnt, diese kann jedoch dem selben Ziel an Anonymisierbarkeit und

1: Unentdeckbarkeit ist eine wünschenswerte Eigenschaft in der Methode der Datenverwässerung und steganografischen Systemen. Letztere arbeiten im Wesentlichen mit dem verbergen von Inhalten innerhalb anderer Datenformen (Pfitzmann et al., 2010).

2: *“Unobservability of an item of interest (IOI) means undetectability of the IOI against all subjects uninvolved in it and anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.”* (Pfitzmann et al., 2010, S.17)

3: *“The current mainstream approach to privacy protection is to release as little personal data as possible (‘data minimisation’). To this end, Privacy Enhancing Technologies (PETs) provide anonymity on the application and network layers, support pseudonyms and help users to control access to their personal data, e.g., through identity management systems”* (Pfitzmann et al., 2010, S.10)

4: *“Misinformation and disinformation may be regarded as semantic dummy traffic, i.e., communication from which an attacker cannot decide which are real requests with real data or which are fake ones.*“ (Pfitzmann et al., 2010, S.19)

Unentdeckbarkeit für den Datenschutz folgen. Bei der Erörterung muss man beachten, dass die Daten, oder auch die daraus interpretierten Informationen, zu einem vorherigen Zeitpunkt quasi-sichtbar oder sichtbar waren und nun unsichtbar gemacht werden sollen.

> *Der Begriff „Datenlöschung" bezieht sich auf den vollständigen und dauerhaften Prozess der Entfernung von gespeicherten Daten, sodass sie nicht mehr wiederhergestellt werden können. Dieser Prozess kann auf verschiedenen Arten erfolgen, wie beispielsweise durch physische Zerstörung von Speichergeräten, Überschreiben der Daten oder Entmagnetisierung (Wilms, 2023).*

Es gibt zudem rechtliche Grundlagen in der EU mit der DSGVO seit 2018, welche in Bezug auf Datenlöschung in diesem Artikel relevant sind. Die Aussagen beider Absätze wurden im Folgenden zusammengefasst:

- **Artikel 17, Abs 1, DSGVO**: **Das Recht auf Löschung** Mit diesem Recht kann die restlose Entfernung von personenbezogenen Daten bei einem für deren Verarbeitung Verantwortlichen verlangt werden. Es müssen jedoch einige Bedingungen erfüllt sein, um dieses Recht geltend zu machen. Beispielsweise ein Nachweis, dass die Daten für die Verarbeitung nicht mehr notwendig sind und ihren Zweck erfüllt haben, nicht rechtmäßig verarbeitet worden sind oder ein geltender Widerspruch gegen die Verarbeitung eingelegt wurde. Es können jedoch auch Ausnahmen von der Löschung bestehen, wenn die Verarbeitung der Daten legitimen öffentlichen Aufgaben oder dem öffentlichen Interesse dient oder zur Ausübung des Rechts auf freie Meinungsäußerung sowie Information verwendet wird (*BfDI* ,o. J.).
- **Artikel 17, Abs2, DSGVO: Das Recht auf Vergessenwerden**. Die Verantwortlichen für die Verarbeitung der Daten haben, soweit diese Daten veröffentlicht wurden, bei einem berechtigten Löschverlangen andere Stellen, die diese Daten verarbeiten, zu informieren. Weiterhin müssen alle vertretbare Schritte von den Verantwortlichen unternommen werden, zu informieren, dass auch die Löschung aller Links auf diese Daten oder von Kopien oder Repliken verlangt wird. Dies richtet sich insbesondere an Suchmaschinenbetreiber, die beispielsweise die Betreiber weiterer Internetseiten, auf die sie verlinken, über den Löschwillen informieren müssen. Bei diesem Recht gelten dieselben Ausnahmen, wie beim Recht auf Löschung (BfDI, o.J).

Im Bezug auf die Unbeobachtbarkeit, könnte mithilfe des Abs 1. die Unentdeckbarkeit eines IOIs beeinflusst werden, während mit Abs. 2 die Unverkettbarkeit von IOIs beeinflusst werden kann. Im Falle der Löschung des IOI und seinen Verkettungen zu Person, kann man für den Fall aller gelöschten Daten dann von einer Anonymität des Subjekts reden. Inwieweit von diesem Recht im Anwendungsfall gebraucht gemacht wird und zu welchem Grad eine Unbeobachtbarkeit tatsächlich hergestellt werden kann, wird nicht weiter beleuchtet. Dies würde aber für eine genauere Überprüfung des Rechts spannend sein.

Um diesen Abschnitt abzuschließen, lassen sich folgende erstellte Erkenntnisse für die weitere Arbeit zusammenfassen:

Digitale Unsichtbarkeit steht der Unbeobachtbarkeit am nächsten, welche sich aus der Anonymität einer Person und der Unentdeckbarkeit ihrer digitale Spur zusammensetzt. Die Definition der Unbeobachtbarkeit, besonders die

Unbeobachtbarkeit mit dem Grad 0, kann damit dem Anspruch der digitalen Unsichtbarkeit gerecht werden.

Der digitalen Unsichtbarkeit kann sich durch die Prozesse der Datenminimierung, Datenumgangskontrolle (beeinflussen von Verwertung, Speicherung und Nutzung) oder Datenlöschung angenähert werden. Um die digitale Unsichtbarkeit jedoch erreichen zu können, müssten alle diese Prozesse stattfinden.

Das Konzept der Identität wurde in diesem Abschnitt nicht weiter beleuchtet, ist jedoch von Bedeutung, um zu verstehen, um welche Identität, welchen Teil von ihr oder ob es sich primär überhaupt um die Identität eines Subjekts bei der Unbeobachtbarkeit handelt. Da die Forschungsfrage sich darauf bezieht, wie wir als Menschen digital unsichtbar werden können, wird nun die Thematik der Identität ergründet.

4. Identität

4.1 Identität und Teilidentität im Digitalen

Identität lässt sich als alleinige Lebensauffassung erklären, die eine Integration in eine soziale Gruppe und Kontinuität, die an einen Körper gebunden ist, beschreibt und - zumindest bis zu einem gewissen Grad - von der Gesellschaft geprägt ist (Pfitzmann et al, 2010). Aus der Perspektive vom Philosophen George Herbert Mead, entwickelt sich Identität durch Interaktionserfahrungen, die sich im Laufe der Sozialisation anhäufen. Der Einzelne findet sich in den Reaktionen der anderen wieder, im Sinne eines leicht verzerrten Spiegels, wodurch sich die Identität bildet (Wittpahl, 2017; Mead, 1923). Mead unterscheidet im Konzept der Identität dabei in das „I“, welches nur für das individuelle „Selbst“ zugänglich ist, frei und instinktiv handelt und nicht durch soziale Normen oder Erwartungen begrenzt ist. Zum anderen in das „Me“, welches die internalisierten sozialen Rollen, Erwartungen und Normen der Gesellschaft repräsentiert und durch Bewertung und Perspektiven anderer zu einem sozialen „Selbst“ durch Reflektion geformt wird. Dieser Teil der Identität wird in der Gesellschaft offenbart - die Art und Weise wie andere einen sehen (Mead, 1934).

Der Philosoph Paul Ricoeur unterscheidet bei Identität auch in zwei ähnliche Teile – zum einen die ipse- und zum anderen in die idem-Identität (Ricoeur, 1992). Diese wurden für den Beginn einer Erörterung der digitalen Identität von Thierry Nabeth verwendet: Die ipse-Identität bezieht sich auf die eigene Perspektive, woraus sich das Ich-Gefühl (was einen selbst ausmacht) entwickelt. Dieser Teil ist grundsätzlich fluide und unbestimmt und befindet sich außerhalb der Reichweite der Informations- und Identifikationstechnologien. Die idem-Identität bezieht sich auf die Beobachter-Perspektive, aus der die Person in beschreibenden Attribut-Sammlungen charakterisiert wird. Diese können zur Unterscheidung zwischen anderen Personen, als auch als einzigartige Identifikationsmerkmale genutzt werden. Die Charakterisierung ist statisch, auch wenn sie regelmäßig aktualisiert wird. Dies ist der Identitäts-Teil, der durch Informations- und Identifikationstechnologien formatiert und verarbeitet wird (Nabeth, 2009).

Die digitale Identität bezieht sich im Allgemeinen auf die Zuordnung von Attributwerten zu einer einzelnen Person, auf die mit technischen Mitteln zugegriffen werden kann, wie beispielsweise die E-Mail, IP-Adresse oder Konten auf Social Media (Pfitzmann et al. 2010). Weiter umfasst sie all die persönliche Daten, die in ein maschinenlesbares Datenformat gebracht werden können und von computergestützten Anwendungen gespeichert und verknüpft werden können (Giannopoulou, 2023).

Das Konzept der Identität kann zudem aus verschiedenen Perspektiven betrachtet werden. Zum einen aus der strukturellen Perspektive, wobei die Identität als Repräsentation angesehen wird, in der Attribute eine Person charakterisieren. Zum anderen aus einer prozessualen Perspektive, wobei die digitale Identität zur Identifizierung herangezogen wird. Dabei wird die Identität anhand einer Reihe von Prozessen betrachtet, die sich auf die Offenlegung von Informationen über die Person und die Verwendung dieser Informationen beziehen (Nabeth, 2009). Die digitale Identität betrifft sowohl Systeme zur Identifizierung von Personen als auch Systeme zur Authentifizierung, die Zugriffsrechte regeln und die Durchführung vorher festgelegter Aktionen oder den Zugang zu bestimmten Diensten genehmigen (Nyst et al., 2016).

In Worten der Computerwissenschaft, kann die Identität als Eigenschaft einer Entität im Sinne des Gegenteils von

Anonymität und Unverkettbarkeit erklärt und definiert werden. In einer positiveren Formulierung ermöglicht Identität sowohl die Identifizierbarkeit, als auch die Verkettbarkeit von IOIs aufgrund einer gewissen Kontinuität des Lebens (Pfitzmann et al., 2010).

Eine Identität ist eine Teilmenge von Attributwerten einer individuellen Person, die diese Person innerhalb einer beliebigen Menge von Personen hinreichend identifiziert. Daher gibt es im Allgemeinen nicht nur "die Identität", sondern mehrere von ihnen (Pfitzmann et al., 2010).

Das liegt daran, dass die Identität einer Person in vielen Lebensbereichen und Kontexten eine große Rolle spielt. Die Vielfalt der Rollen, die Menschen im Leben einnehmen, führt zu verschiedenen Teilen ihrer Identität, die sowohl angeborene als auch im Laufe des Lebens erworbene Merkmale umfassen (Nabeth, 2009). Die bildliche Darstellung in Abbildung 1 fasst dies besser zusammen.

An manchen Stellen überschneiden sich die Charakteristiken und Attribute. Zwischen einigen Bereichen ist es aber von hohem Interesse, Charakteristiken voneinander getrennt zu halten. Die Kontrolle über den Zugang zu diesen Informationen und deren Nutzung beeinflusst die Handlungsfreiheit einer Person und kann sowohl positive als auch negative Auswirkungen haben [1] .

In diesem Fall spricht man von einer partiellen Identität. Es ist ein Begriff, der verwendet wird, um eine Form der Identität zu beschreiben, die eine einzelne Person möglicherweise nicht vollständig identifiziert, wodurch ein unterschiedliches Maß an Anonymität ermöglicht wird. Im Kontext des Identitätsmanagements und aus Sicht der Datenminimierung ist eine Teilidentität eine Teilmenge der Gesamtidentität einer Person, die nur bestimmte Attribute oder Informationen enthält, die für einen bestimmten Kontext oder eine bestimmte

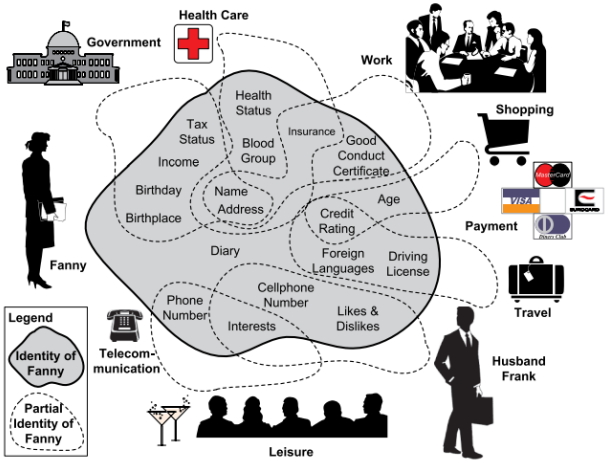

Abbildung 1: Partielle Identitäten

Rolle relevant sind. Dies bedeutet, dass eine Person je nach Kontext oder Gruppe von Personen, die berücksichtigt werden, unterschiedliche Identitäten haben kann. Beispielsweise kann eine Person eine Identität haben, die auf ihrem legalen Namen basiert, und eine andere Identität, die auf ihrem Online-Benutzernamen oder -Pseudonym basiert. (Pfitzmann et. al, 2010)

Das Konzept der Teilidentität ermöglicht mehr Flexibilität und Kontrolle bei der Offenlegung persönliche Daten und bietet Einzelpersonen die Möglichkeit, ihre Identität in unterschiedlichen Situationen zu verwalten. (Pfitzmann et. al, 2010).

Für das Einordnen einer digitalen Teilidentität wird sich des Modells von Mead grob bedient und dies erweitert. Die Identität bleibt in „I“ und „Me “ aufgeteilt, wobei eine digitale (Teil-)Identität innerhalb des expliziten „Me“ eingeordnet wird. Das „I“ bleibt dabei die unbestimmte Ich-Perspektive, vergleichbar mit der ipse-Identität. Das implizite „Me“

1: “*The management of access to the information and of the control (by the person, by institutional bodies, by organisations, or by commercial entities) is critical since it relates to the liberty of action of a person. Thus the disclosure of information about the political opinion of a person (this person can be an activist or a Unionist) can seriously impact on the degrees of liberty of action of that person (in ‘the worst case’ the person may be sent to prison, in other cases it may put the continued employment of that person in jeopardy). In particular, making the information too transparent can cause people to not act at all for fear of retaliation (from other people, from groups or from society). This can have negative consequences (people may fear denouncing unacceptable situations) or positive ones (preventing people from hiding revenues and paying less taxes or making people liable for a damage for which they are responsible). A more mundane aspect relates to the shameless exploitation of this information by third parties who consider it as a public resource.*”
(Nabeth, 2009, S. 38)

beschreibt die Perspektive, wie eine Person sich selbst sieht, während das explizite „Me“ sich rein auf die Perspektive der Anderen auf diese Person, wie diese von Anderen mit ihren Aktionen in einem gewissen Kontext wahrgenommen und repräsentiert wird, beschränkt [1] .Hier spricht man von auch von einem Image, dass die Person den anderen vermittelt (Nabeth, 2009).

Diese Aspekte stellen die Verbindung zwischen der lebenden Person („I“) und ihrer Beziehung zur der äußeren Umgebung (explizite „Me“) her, wobei diese beiden Aspekte durch die (un)bewussten Wahrnehmungen, die eine Person von sich selbst hat (implizite „Me“), reguliert werden. Konflikte und Probleme entstehen typischerweise dann, wenn eine Diskrepanz zwischen der Art und Weise, wie eine Person sich selbst wahrnimmt und der ihr zugeschriebene Identität durch das Image besteht (Nabeth, 2009). Das Image kann somit auf einer realen Identität basieren, wird jedoch auch durch die Art und Weise beeinflusst, wie eine Person über diese digitale Identität online agiert und wie andere sie dadurch wahrnehmen und bewerten.

4.2. Identitätskontrolle

Wenn es also um die Frage nach der eigenen Kontrolle einer digitalen Identität geht, mit dem Ziel Charakteristiken oder Attribute, die zur persönlichen Identität verketten, unsichtbar zu machen, müsste man an der Stelle des impliziten „Me“ regulieren – eine Art Selbstkontrolle darüber, wie viel man über seine reale Person in einer digitalen Identität preisgibt. Jedoch ist dies schwierig umzusetzen, da eine Person nur einen begrenzten Teil ihrer Identitätsinformationen selbst kontrolliert. Ein großer Teil dieser Informationen wird von außen kontrolliert: von Regierungen oder Institutionen, wie dem Finanzamt, den Gesundheitsorganisationen, von Unternehmen, z. B. von der Firma, die diese Person beschäftigt, oder von ihrer Bank; von kommerziellen Unternehmen, wie Internet- und Marketingfirmen; oder durch die "öffentliche Meinung", wie Zeitungen oder informelle und soziale Netzwerke (Nabeth, 2009, S.40).

Deswegen müssen neben der Selbstkontrolle auch immer besser Möglichkeiten gefunden werden, um eine externe Entität an der Speicherung, Manipulation und Nutzung erhobener persönlicher Daten zu beschränken, beispielsweise durch rechtliche oder technische Mechanismen (Nabeth 2009; Giannopoulou, 2023). So kann beispielsweise die partielle Identität durch Daten im Gesundheitsbereich für Beobachter aus der Institution Bank unsichtbar sein, da für diese solch klassifizierten Daten rechtlich nicht eingesehen werden dürfen (Nabeth, 2009).

Ob dies heutzutage immer noch gilt, ist für viele Menschen fragwürdig (Nassehi, 2019). Es werden immer mehr Datenspuren erzeugt als auch personenbeziehbare Attribute in Form von Daten wissentlich und unwissentlich zur Verfügung gestellt. Größere Internetfirmen, deren Geschäftsmodell auf den Daten basiert, sind besonders daran interessiert in vielen verschiedenen Lebensbereichen Services anzubieten (Nassehi, 2019). Mit dem Verständnis der partiellen Identität macht dies auch Sinn, da durch mehr gesammelte Daten aus Lebensbereichen mehrere Eigenschaften von partiellen Identitäten zu einer digitale Identität, beispielsweise zuordnungsbar zu einer E-Mail-Adresse, kombiniert werden können. Die Rekombination von anfänglich unzusammenhängenden Daten ist jedoch auch in der Lage, Annahmen zur Zugehörigkeit einer statistischen Gruppe mit den jeweiligen Interessen, Eigenschaften und Handlungsweisen zu treffen (Nassehi, 2019). Hierbei ist es auch interessant, welches digitale Image über diese externe Rekombination von einem erzeugt wird und vor allem, ob

1:

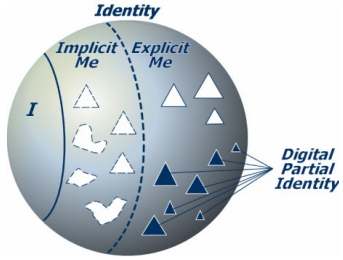

Abbildung 2: I, implizites Me und explizites Me

dieses Bild wahrhaftig mit der persönlichen Identität ist oder nicht.

Wenn es sich also um unsere digitale Unsichtbarkeit handelt, kann dabei von der Unsichtbarkeit unserer persönlichen Identität in einem digitalen Image gesprochen werden - ausgehend von einer digitalen Identität. Weiterhin wäre damit die Unentdeckbarkeit von Attributen oder Charakteristiken gemeint, die nicht miteinander in Verbindung gebracht werden und nicht zu einer identifizierbaren Identität einer Person zusammengesetzt werden können. Abhängig vom Beobachter und seinen Einschränkungen, können partielle Identitäten im Digitalen unsichtbar sein. Der externe Zugriff auf und Zuordnung von Attributen und Charakteristiken muss dafür reguliert werden, sodass diese partielle Identität im Digitalen nicht ausreichend auf die reale Person rückschließen kann.

5. Warum fragen wir nach digitaler Unsichtbarkeit?

Aber warum möchte man überhaupt digital unsichtbar werden? Wieso gibt es den Wunsch nach einer digitalen Unsichtbarkeit? Und wer ist der Beobachtende und der Beobachtete?

In dieser Arbeit wurden an einigen Stellen schon kurz die Situationen als auch mögliche Motivationen zur digitalen Unsichtbarkeit aufgegriffen. Dieses Kapitel dient jedoch der genaueren Untersuchung von Rahmenbedingungen, die zur Frage nach einer digitalen Unsichtbarkeit beitragen. Einige von diesen Gründen, haben meist die Sorge vor dem Verlust der digitalen Selbstbestimmung gemeinsam (Branther & Steele, 2021).

5.1 Die Beständigkeit der digitalen Erinnerung und das Vergessen im Digitalen

Es gibt einige Fälle, in denen Menschen durch digitale Erinnerungen negative Erfahrungen machen mussten. Seien es beispielsweise Äußerung in Chats zu Beschwerden in ihrem Job, welche an den Chef offenbart wurden, alte Kommentare oder Tweets, mit der sich die Person nicht mehr identifiziert kann, aber derzeitige Beziehungen beeinflussen, oder noch Bilder von „mug shots“ von Verhaftungen existieren obwohl die Anklage fallen gelassen wurde oder die Vorstrafen verjährt sind. Es werden aber auch analoge Aufzeichnungen und Erinnerungen digitalisiert und verbreitet, mit denen man Jahre später nicht mehr in Verbindung gebracht werden möchte. Digitale Sammlungen und die Anwendungen dafür fördern das Teilen von Inhalten, was aber auch zu Eingriffen in die Privatheit anderer und einem Ungleichgewicht in der Informationsmacht führen kann (Mayer-Schönberger, 2018).

Das digitale Vergessen sollte jedoch nicht nur aus dem Aspekt der Privatheit betrachtet werden und dem Anliegen, dass andere die Vergangenheit eines Menschen vergessen. Professor Mayer-Schöneberger kommt zum Fazit, dass es auch problematisch sein könnte, wenn man selbst seine Vergangenheit jederzeit abrufen kann. Aus diesem Grund ist es nicht verwunderlich, dass Kunden und Bürger, immer mehr zu digitalen Tools greifen, ob Suchmaschinen oder Social Media, welche auf die Vergänglichkeit oder das Vergessen von Informationen ausgerichtet sind (Mayer-Schönberger, 2018).

Für Mayer-Schöneberger ist Vergessen ein natürlicher Vorgang im Gehirn, der keiner bewussten Anstrengung erfordert. Unser Gehirn entfernt automatisch Erinnerungen, die es für nicht mehr relevant hält. Anders als ein Archiv ist unser Kopf ein lebendiges Gedächtnis. Beim Erinnern schaffen und verändern wir Erinnerungen, da das menschliche Gedächtnis plastisch ist. So vergessen wir nicht nur bestimmte Erinnerungen, wir schreiben sie auch um [1].

Das Vergessen dient vor allem dazu, sich auf die Gegenwart und Zukunft zu fokussieren. Die Fähigkeit wichtige von unwichtiger Information zu trennen oder die Details zu vergessen und die Essenz zu identifizieren, ist für das Zurechtfinden in der Welt und dem Verstehen der Realität von Bedeutung (Mayer-Schönberger, 2018).

Immer mehr Menschen haben das Gefühl in einem Glashaus präsentiert zu werden, wobei mehr Informationen für ein weit größeres Publikum leicht zugänglich sind. Diese Situation wirft hinsichtlich der sinnvollen Unterscheidung zwischen wichtigen und unwichtigen Informationen Fragen auf. Insbesondere werden Fragen zu Nutzung und Bedeutung von

1: “*Forgetting is built deep into our brains. It comes naturally, and does not require conscious effort. Our brain routinely rids itself of memory that it deems no longer relevant. […] Our mind is not an archive; it is quite literally living memory. As we remember, we do not retrieve memory, we recreate and thus rewrite it. Every act of remembering is thus also an act of creation; human memory is malleable. Thus, we not only forget certain memories, we also rewrite them*” (Mayer-Schönberger, 2018, S.119).

Verbergen und Vergessen von gespeichertem Material aufgeworfen (Abbt, 2018).

Es kann von einer Entstehung eines telematischen Gedächtnis gesprochen werden: Das Aufnehmen von Informationen und das spätere Erinnern an diese in Zeiten von digitalen Medien mit immensen Potential der Datenerfassung, Datenspeicherung und Datenverkettung ist kaum mehr von Interesse (Abbt, 2018 ; Esposito, 2002). In Anbetracht dessen fasziniert also die Fähigkeit des Vergessens. Aber die Entscheidung, welche Inhalte ausgewertet und welche ignoriert werden können, setzt eine Fähigkeit voraus, über die Technologien basierend auf künstlicher Intelligenz nur bedingt verfügen (Abbt, 2018).

Zusammenfassend lässt sich hier ein Wunsch nach dem Vergessen öffentlich zugänglicher Informationen feststellen, die das digitale Image beeinflussen. All die öffentlich zugänglichen Informationen und Daten können gesammelt und dem digitalen Image zugeordnet werden, ohne Rücksichtnahme ob diese Information noch aktuell, relevant oder dem impliziten „Me“ entspricht. Gleichzeitig kommt auch die Frage der Übernahme der Verantwortung für die öffentlich zugänglichen Informationen auf, und wie, im Falle von entschiedener Irrelevanz, für das Vergessen werden gesorgt wird. Spätestens im Falle des eigenen Todes ist es von großer Bedeutung diese Verantwortung für Daten und digitale Informationen, die beispielsweise vergessen werden sollen, bestimmt zu haben [1] .

Vergessen kann auch nicht mit absoluter Löschung gleichgesetzt werden. Das Vergessen umfasst immer Teile des Wissens oder des Bewusstseins. Man muss wissen, dass Wissen verloren gegangen ist, um überhaupt vom Vergessen sprechen zu können (Abbt, 2018). In diesem Fall kann man von einem unsichtbar „werden“ sprechen.

5.2 Gefahren der digitalen Sichtbarkeit

In manchen Fällen geht eine Gefahr für Menschen aus, wenn sie sich digital sichtbar zeigen. Im Beispiel einer Überwachung durch repressive Regime, ist es für Bürger von großer Bedeutung anonym zu bleiben und digitale Spuren z.B ihrer freien Meinungsäußerung oder illegalen Aktionen unsichtbar zu machen. Der Beobachtungsraum ist dabei auch über verschiedene Institutionen und Lebensbereiche größer, da das Regime auch Einfluss auf Unternehmen und andere öffentliche Institutionen nehmen könnte. Da die Folgen der Sichtbarkeit im schlimmsten Fall eine Frage von Leben oder Tod bedeutet, ist die Motivation digital unsichtbar zu sein besonders hoch (Castiglione et al, 2011). Hier sind die Menschen bereit, ihre digitale Spur maximal zu minimieren, um einen hohen Grad an Unbeobachtbarkeit durch das bewusste Unterlassen von Aktionen im digitalen Raum zu erreichen (z.B durch weniger verfolgbare Zahlungen mit Bargeld und Kommunikationseinschränkungen). Wenn man von einer Überwachung oder sogar aktiven Verfolgung spricht, ist es in diesem Fall auch wichtig Spuren in der analogen Welt, welche durch Technologien digitalisiert werden können, zu minimieren (z.B durch Verschleierung vor Face Recognition) (Frey, 2023).

Für Aktionen, die über den digitalen Raum ausgeführt werden, muss für die Unbeobachtbarkeit gesorgt werden. Ein Grad der Anonymität der Personen wird durch Verschleierung der verkettbaren Atrribute erreicht, die zu einer Identifizierung der Person nötig sind. Hier werden beispielsweise Tools, wie der Tor-Browser zum Verschleiern der IP-Adresse, zum Zugang zum Internet auf Einweg-Endgeräten außerhalb des eigenen Netzwerks (am besten weit außerhalb dem derzeitigen Ort des längeren Aufenthalts) genutzt (Viangalli, 2022; Mitnick, o. J.). Um die Unentdeckbarkeit der digitalen

1: Internetnutzer hinterlassen beim Ableben große Mengen an Online-Daten, die häufig als digitale Hinterlassenschaften bezeichnet werden. In einigen Ländern lässt sich mithilfe eines digitalen Nachlasses, die Verantwortung über Accounts, Software und für den ehemaligen Nutzer zugänglich gemachte Daten festlegen und wie mit diesen weiter umgegangen werden soll (Öhman & Watson, 2019).

Spur zu erhöhen, müssten Vorkehrungen zur Verschlüsselung der Informationen zur Aktion als auch ein geeigneter Dummy-Traffic eingesetzt werden, welcher die Spur verwässert (Pfitzmann et. al, 2010). Auch sollten nach der Aktion hinterlassene Daten zur Durchführung restlos gelöscht werden, sodass weder deren Existenz als auch der Löschvorgang entdeckbar sind (Castiglione et al, 2011).

In solch einem Beobachtungsverhältnis ist die digitale Unsichtbarkeit zwar von sehr großem Interesse. Jedoch bringt das Streben nach der größtmöglichen digitalen Unsichtbarkeit auch zu ersichtlich großen Einschränkungen in den Möglichkeiten der Lebensgestaltung bei.

5.3 People Farming und der Handel mit Daten

In einem weiteren Beobachtungsverhältnis der Überwachung, handelt es sich um das Individuum und ökonomische Akteure. In dem heutigen sozio-technischem System wird dieses Verhältnis als „Surveillance Capitalism“ bezeichnet (Balkan, 2017). Der durch die Wirtschaftsprofessorin Shoshana Zuboff geprägte Begriff, beschreibt dabei eine Form des Kapitalismus, der auf der umfassenden Überwachung des Verhaltens eines Nutzers im digitalen Raum basiert. Unternehmen, vor allem Internetplattformen und Technologiefirmen, sammeln dabei eine große Menge an persönlichen Daten über den Nutzer, welche zur Analyse von Verhaltensmustern herangezogen werden. Das Ziel ist es, durch die Monetarisierung dieser Nutzerdaten, Gewinne durch personalisierte Werbung zu erzielen. „Surveillance Capitalism“ hat große Auswirkungen auf die Privatsphäre des Nutzers und fordert demokratische Normen heraus. Zudem wirft es ethische Fragen hinsichtlich des Umgangs mit persönlichen Informationen auf (Zuboff, 2015).

Der Designer und Aktivist Aral Balkan geht dabei in seinem Blogbeitrag weiter und trifft die Aussage, dass wir die Kontrolle über unsere Daten nicht verloren haben, sondern diese geklaut wurde. Er bezeichnet die großen Internetfirmen wie Google und Facebook als „people farmer“ und Datenhändler, da die Nutzer wie Viehe ihren Systemen herangezüchtet werden und einen fast endlosen Ertrag an Rohstoffen für Informationen bringen. Je mehr sie uns mit ihren Inhalten füttern, desto mehr können ihre Algorithmen uns ausbeuten. Das ist die Art des Geschäfts welches die Firmen gewählt haben: der Zugang zu Internetinhalten, im Tausch für persönliche Daten. Aber kostenlos ist da nichts. Für ihn stellt sich gar nicht mehr die Frage, ob man mit diesen Firmen an einer Zukunft des Internets zusammenarbeiten sollte. Um eine Brücke in die Zukunft des Internet nach unseren Bedürfnissen nach Selbstsouveränität und gesunder Gemeinschaft zu bauen, müssen sich die Leute für die Regulierung dieser Firmen einsetzen, die nichts mit diesen Unternehmen zu tun haben und zu tun haben wollen (Balkan, 2017).

Anhänger dieser Ansicht werden wohlmöglich, wo es nur geht, die Nutzung der Dienste von diesen Firmen einschränken bis fast gänzlich einstellen. Um trotzdem weiterhin auch digital sichtbar für diese Forderung nach Regulierung von Google und Co. zu sein, sozusagen auf Stufe 2 und 3 der digitalen Sichtbarkeit zu agieren, werden alternative Möglichkeiten und Ansätze zu Internetnutzung gefördert und verwendet. Man könnte in Bezug auf das „people farming“ von einer Art Protest, einer Auflehnung gegen die vorherrschende Machtungleichheit im Panoptikon zwischen Ausbeuter und Ausgebeuteten, sprechen [1] .Die Ermöglichung der digitalen Unsichtbarkeit in diesem Falle könnte als Teil dieser Auflehnung verwendet werden. Diese jedoch nicht in ihrem absoluten Verständnis, sondern relativ zu den Internetgiganten, gegen die sich aufgelehnt wird.

1: *„Focault hatte beschrieben, die Macht liege nun bei denen, die Schweigen und beobachten, nicht bei denen, die sprechen und über sich Auskunft geben. Über sich selbst Auskunft zu geben, ist aber eine der Praktiken, die inzwischen unvermeidlich geworden sind“* (Nassehi, 2019, S.314)

Grundsätzlich geht es aber nicht um das Erreichen einer digitalen Unsichtbarkeit, sondern um den Wunsch nach Selbstbestimmung im Netz der Zukunft.

5.4 Überschrittene Privatsphären und gebrochenes Vertrauen

Anknüpfend an das Thema des Surveillance Capitalism, wird auch die Frage nach der Privatsphäre, bzw. dem Umgang mit dem für den Nutzer sensiblen und privaten Daten laut. Wie schon in vorherigen Abschnitten dieser Arbeit festgestellt, ist die Klassifizierung von privaten Informationen und das ziehen von Privatsphären für jeden Menschen individuell. Jedoch kann sich die Erörterung der dahinter liegenden Gründe für die Frage, wieso und inwiefern Menschen digital unsichtbar werden wollen, herangezogen werden.

Der Begriff Privatsphäre kann als grundlegendes Menschenrecht, das Recht auf das "in Ruhe gelassen zu werden", betrachtet werden. Es kann auch als eine grundlegende Notwendigkeit gemäß Maslows Bedürfnishierarchie betrachtet werden, um einen privaten Raum zu schaffen, der vor anderen geschützt ist [1] .

Es gibt verschiedene Definitionen von auf Recht basierter Privatsphäre, die sich auf Einschränkungen stützt und die private Sphäre als Freiheit „von etwas“ betrachten. Privatsphäre kann auch als Affirmation für die volle Verwirklichung des liberal-autonomen Selbst konzipiert werden (Waldman, 2018). Für viele bedeutet Privatsphäre damit auch Wahlfreiheit, Autonomie und individuelle Freiheit[2]. Sie umfasst das Recht des Individuums zu bestimmen, was es verborgen halten wird und was, wie, wann und wem es persönliche Informationen preisgeben wird (Seigneur & Jensen, 2004).

Wenn jedoch Nutzer ihre Daten mit Unternehmen teilen, verlieren sie oft ihre Besitzrechte an diesen Daten und haben keinen Einfluss auf deren Verarbeitung. Man werde gezwungen, den Schutz des dort entstandenen privaten Raumes einer anderen Partei anzuvertrauen, in diesem Fall dem Unternehmen (Müller, 2018). Der Rechtsprofessor Ari Waldman stellt fest, dass die Rechtsauffassungen von Privatsphäre oft übersehen, dass Datenschutznormen durch das Teilen von Informationen ausgelöst werden (2018). Das Offenlegen und Teilen ist im Wesentlichen ein soziales Verhalten, indem wir die Kontrolle über unsere Informationen gegen das Vertrauen in mächtige soziale Normen oder soziale Grundregeln eintauschen. Diese bestimmen dann unsere Erwartungen, was mit den geteilten Informationen nach dem Teilen passieren soll [3] .

Die Privatsphäre im Kontext von Vertrauen betrachtet Informationen aus einer sozialen Perspektive und erkennt an, dass es darum geht, den Informationsfluss zu regulieren, anstatt andere auszuschließen. Ein wichtiger Aspekt ist der soziale Kontext der Privatsphäre, die nicht als Rückzug oder Begrenzung unserer Verbindung zu anderen betrachtet werden sollte. Stattdessen geht es um die sozialen Beziehungen, die das Teilen und Offenbaren von Informationen bestimmen; sowohl zwischen Individuen sowie zwischen Nutzern und Plattformen, die ihre Informationen sammeln, analysieren und manipulieren (Waldman, 2018).

Wir teilen unsere Informationen in der Erwartung, dass sie für den spezifischen Zweck verwendet werden, für den wir sie mitgeteilt haben. Vertrauen ist dabei eine soziales Gut zwischen zwei oder mehreren Parteien, das sich auf die Erwartung bezieht, dass sich die anderen anhand der akzeptierten Normen verhalten werden. Sie mildert die Verletzlichkeit und das Machtungleichgewicht, das mit der Offenbarung einhergeht. Werden Informationen in einem

1: Dies entspricht der zweiten Stufe der maslowschen Bedürfnispyramide – dem Sichertsbedürfnis. In bestimmten Fällen, wie Datenskandalen von Cambridge Analytica, wird deutlich, wie wertvoll unsere Informationen sind. Dies kann ein Gefühl der Unsicherheit und Freiheitsberaubung auslösen, wo wir uns plötzlich nirgends mehr sicher, ungestört oder unbeobachtet fühlen. Solange Unsicherheit besteht, sind wir kritisch und zurückhaltend gegenüber Datensammlern (Ehrmann, 2022).

2: Diese Bedürfnisse sind der fünften Stufe der Bedürfnispyramide zuzuweisen (Ehrmann, 2022).

3: *“They are, however, incomplete. They miss the fact that information privacy norms are triggered by disclosure. And disclosure is an essentially social behavior: once we share, we trade control of our information for reliance on powerful social norms, or background social rules that feed. into our expectations of what should happen with our personal data*” (Waldman, 2018, S.6)

vertrauenswürdigen Kontext geteilt, so wird das Vertrauen zerstört, wenn die Datenerfassung und -nutzung über das angemessene Maß hinausgeht oder Datenpannen entstehen (Waldman, 2018). Und sobald das Vertrauen gebrochen wurde, ist es schwer zum ursprünglichen Punkt des Vertrauens zurückzukehren. Die Konsequenz ist, dass das Vertrauen entzogen wird (Frei & Morriss, 2021).

Ein Vertrauensbruch aufgrund von beispielsweise Datenschutzverletzungen von Unternehmen oder Privatpersonen könnte dazu führen, dass Nutzer ihre Privatsphäre vor diesen schützen wollen, möglicherweise sogar digital unsichtbar für sie werden möchten. Dies beeinträchtigt jedoch auch das Aufrechterhalten der sozialen Norm des Vertrauens in der Gesellschaft, die das Teilen und soziale Interaktion ermöglicht [1] . Egal, ob man private Informationen aus der Perspektive der privaten Grenzen oder des Vertrauens betrachtet, das Bedürfnis nach Schutz und vor allem nach Autonomie, selbst zu bestimmen, was geteilt wird und wie damit umgegangen wird, steht an erster Stelle. Das Bedürfnis nach Autonomie und Kontrolle darüber, was mit Daten geschieht, muss anerkannt und gefördert werden, um selbstbestimmt darüber zu entscheiden, welche Informationen man digital sichtbar macht oder welcher Teil von einem digital unsichtbar bleibt.

1: *"Disclosure and privacy govern our relationships with others (persons as well as technology platforms); as such, they are social phenomena. Trust is the link between them. And strong trust norms are what allow sharing and social interaction to occur "* (Waldman, 2018, S.6)

6. Wie können wir digital unsichtbar werden?

In Folge der Erkenntnisse der letzten Kapitel wird erkennbar, dass wenn man von unserer digitalen Unsichtbarkeit spricht, zwei Auslegungen herangezogen werden könnten: die absolute digitale Unsichtbarkeit als auch die relative digitale Unsichtbarkeit. Beide Auslegungen werden in Bezug auf die Möglichkeiten, mit welchen sie erreicht werden können, diskutiert. Zudem wird die dahinterliegende Erkenntnis über das Bedürfnis, selbstbestimmt im Digitalen zu handeln, diskutiert.

6.1 Absolute digitale Unsichtbarkeit

Hierbei handelt es sich um den Ansatz, das ohne die Existenz von Daten oder einer digitalen Spur, das Digitale unsichtbar bleibt. Die Umsetzung dieses Ziels erfordert nicht nur die restlose Löschung von bestehenden digitalen Spuren, sondern auch eine umfassende Vermeidung neuer Datenentstehung, also der absoluten Datenminimierung. Zum Teil kann beispielsweise die Löschung von Online-Accounts bei Unternehmen und deren Verkettungen bei Suchmaschinen beantragt werden, wobei rechtliche Bestimmungen wie die DSGVO herangezogen werden können. Des Weiteren muss sichergegangen werden, dass alle Backups der Daten aus seiner digitalen Spur vernichtet werden, welches sich schwierig gestalten könnte. Die Vernichtung von Daten in öffentlichen Institutionen kann sich auch als besonders schwer bis fast unmöglich herausstellen.

Der Ansatz der absoluten Unsichtbarkeit basiert auf dem Prinzip des Risiko Null, bei dem das Ziel darin besteht, jegliche Möglichkeit der Beobachtung zu eliminieren.

Da gesellschaftliche Praktiken digitale Spuren hinterlassen können, sobald es maschinenlesbare Eigenschaften in dieser Spur gibt, muss jegliche Praktik im digitalen Raum als auch teils im analogen Raum eingestellt werden. Die Frage ist hierbei, inwieweit man sich vom sozialen Leben isolieren müsste.

Was sich feststellen lässt ist, dass das Streben nach absoluter digitaler Unsichtbarkeit mit erheblichen Einschränkungen der individuellen Lebensgestaltung einher geht. Diese Einschränkungen könnten für die meisten Menschen nicht im Verhältnis zu den potenziellen Vorteilen stehen, insbesondere wenn sie nicht dazu gezwungen sind, digital unsichtbar zu werden.

Es stellt sich sogar die grundsätzliche Frage, ob absolute digitale Unsichtbarkeit überhaupt realisierbar ist, also eine Unbeobachtbarkeit vom Grad 0. Dies stellt eine der Limitationen der Arbeit dar, zu welcher auch die ethischen und gesellschaftlichen Implikationen einer digitalen Unsichtbarkeit zählen. Wenn sich jedoch die System in denen wir leben, stetig digitalisieren und immer mehr soziale Praktiken Daten erzeugen, stellt sich eine mögliche Fragestellung, ob man für das Erreichen einer absoluten digitalen Unsichtbarkeit sogar aufhören müsste zu interagieren.

6.2 Relative digitale Unsichtbarkeit

Dieser Ansatz ist sowohl abhängig vom Beobachtungsverhältnis als auch vom persönlichen Bezug zu digitalen partiellen Identitäten, die ein Mensch annehmen kann. Im vorherigen Kapitel wurden mögliche Beobachtungsverhältnisse zwischen Individuen, Individuum und öffentlicher Gesellschaft, Individuum und

Internetunternehmen und Datenbrokern als auch zwischen Individuum und Regierung thematisiert sowie deren Gründe, in diesen digital unsichtbar zu werden, erörtert. Zusätzlich ließ sich feststellen, dass die Repräsentation einer Person durch Attribute und Charakteristiken in Rollen und Kontexten mehrere Identitäten, sozusagen partielle Identitäten, annehmen kann. Eine solche digitale partielle Identität und ihre Handlungen, mit denen sie in Verbindung gebracht wird, erzeugen ein Image, welches an die digitale Welt vermittelt wird. Eine digitale Teilidentität, die eine Person aber nicht vollständig identifiziert, kann ein unterschiedliches Maß an Anonymität ermöglichen.

Um digitale Identitäten voneinander getrennt zu halten, ist es wichtig übereinstimmende Attribute zu vermeiden, um einer Identifizierung mit der realen Person zu entgehen. Im Beobachtungsverhältnis zwischen Individuen oder zwischen Individuum und öffentlichem Raum können dafür beispielsweise Pseudonyme eingesetzt werden. Dabei sind Pseudonyme allgemein nicht nur als falsche Namen zu betrachten, sondern als eine Art öffentlicher Schlüssel, mit dem sie adressiert werden können. Die Anonymität der realen Person ist höher, je weniger personenbezogene Informationen zu Pseudonymen zugeordnet werden können, je weniger kontextübergreifend Pseudonyme eingesetzt werden oder desto häufiger Pseudonyme unabhängig voneinander für neue Aktionen gewählt werden (Pfitzman et. al, 2010). Es kann zwar ein öffentlich zugängliches Image aus Spuren dieser digitalen Identität entstehen, lässt sich aber abhängig von der erzeugten Anonymität der Person von Dritten in der Öffentlichkeit nicht auf sie zurückverfolgen. Trotz einer Entdeckbarkeit einer digitalen Spur, versteckt sich die Person sozusagen hinter einem Identifikator, der wenig mit der realen Person zu tun haben sollte. Wenn die Person nun ihre Aktionen über das Pseudonym minimiert und alle vorher gelegten Spuren löschen lässt, kann auch die Zusammensetzung der zugänglichen Informationen zu einem Image beeinflusst werden. Damit würde die Unentdeckbarkeit gefördert werden. Es kann dabei dann von einer Annäherung zur relativen Unsichtbarkeit einer Person im öffentlich zugänglichen digitalen Raum die Rede sein.

Wichtig ist dabei, dass keine öffentlich zugängliche Verkettung zu personenbezogenen Daten oder zwischen anderen digitalen Identitäten, welche mit personenbezogenen Daten verknüpft sind, hergestellt werden kann. Im Falle der Offenbarung von übergreifend verkettbaren Attributen wie beispielsweise eine mehrfach genutzte E-Mail oder eine personenbeziehbare IP-Adresse einer digitalen Identität, ist dabei ein Risiko der Enttarnung und dabei Sichtbarmachung entstanden.

Im Falle des Beobachtungsverhältnisses von Unternehmen oder auch Regierungen, welche Zugriff auf verkettbare identifizierende Attribute wie die IP-Adresse haben können, wird damit weniger die Anonymität durch das Verstecken oder Überdecken der Person, sondern das Verwässern und Verschlüsseln ihrer digitalen Spur von Interesse. Hier kann man beispielsweise beim Profiling von Unternehmen mit Dummy-Traffic in Form von Desinformation einsetzen, um im entstandenen digitalen Image in einem Nutzungsprofil von Services das Entdecken von relevanten Informationen zu erschweren. Die IP-Adresse kann auch durch das Neulegen der digitalen Spur verwässert werden, als auch die Anfragen auf Services im Internet verschlüsselt werden, wie es beispielsweise mit der Nutzung vom Tor Browser möglich ist (Mitnick, o. J.).

All das kann aber auch eher als Annäherung an eine relative digitale Unsichtbarkeit verstanden werden und das Erreichen dieser Unsichtbarkeit ist abhängig vom Wissen des Beobachters.

6.3 Selbstbestimmtes Handeln

Um die zu Beginn dieser Arbeit erwähnten Einflussphären aufzugreifen, lässt sich anhand der erwähnten Beispiele ein zunehmendes Machtungleichgewicht mit jeder Sphäre nach außen hin feststellen. Dies kann aufgrund des fallenden Einflusses auf die Sphäre zusammenhängen, welches auch die Kontrolle der Sichtbarkeit der eigenen Person, bzw. deren Unsichtbarkeit, beeinflusst. Je weiter außerhalb man sich befindet, desto schwieriger wird es seine Anonymität zu kontrollieren und desto wichtiger wird es für ein Grad an Unentdeckbarkeit der digitalen Spur zu sorgen.

Die aufgestellten Prozesse der Datenlöschung als auch die Datenumgangskontrolle (Speicherung, Verarbeitung, Weitergabe) sind für das Erreichen einer relativen digitalen Unsichtbarkeit von Bedeutung. Der Prozess, bei dem der Nutzer jedoch gerade am meisten eigenen Einfluss besitzt, ist die Datenminimierung.

Im Kontext der Beobachtungsverhältnisse, ist die Förderung der Autonomie des Nutzers von Bedeutung gewesen. Denn auch wenn man aus den Machtungleichgewichten der Beobachtungsverhältnisse schwer austreten kann, ist es wichtig im Handlungsrahmen der Einflussphären selbstbestimmt handeln zu können, um den Individualbedürfnissen nachzukommen. Dies kann dann im Kontext der digitalen Identität, als Förderung der Souveränität des Individuums verstanden werden. Für das Erreichen dieses Ziels, muss die selektive Offenlegung verschiedener Aspekte und Komponenten der eigenen Identität in verschiedenen Bereichen und Kontexten ermöglicht werden (Giannopoulou, 2023). Das Individuum muss die Kontrolle über seine persönlichen Daten bis zu einem gewissen Grad, als auch über die Darstellung seiner persönlichen Identität und digitalen Identitäten, behalten können (Wang & De Filippi, 2020). Das Individuum sollte ermächtigt werden, über die Freigabe seiner Daten und die Verknüpfung persönlicher Informationen zu entscheiden.

Dafür können Idenitity Management Systeme eingesetzt werden (Pfitzman et. al, 2010). Nach der jeweiligen Situation und dem Kontext unterstützt ein solches System den Benutzer dabei, beispielsweise eine informierte Auswahl von Pseudonymen zu treffen, die seine oder ihre Teilidentitäten repräsentieren. In diesem Fall hilft es dem Benutzer dabei, seine Teilidentitäten zu verwalten, d.h. verschiedene Pseudonyme mit zugehörigen Identitätsattributwerten je nach verschiedenen Kontexten, Rollen des Benutzers und Interaktionspartnern zu verwenden und zu aktualisieren. Solch ein System fungiert dabei als zentrale Schnittstelle für Interaktionen zwischen verschiedenen Anwendungen, wie dem Internetbrowsen, Online-Shopping oder auch administrativen Aufgaben bei staatlichen Stellen (Pfitzman et. al, 2010).

Gleichzeitig müsste auch das Vertrauen in solche Systeme als auch das Gegenüber im Beobachtungsverhältnis gestärkt werden, dass bei einer Offenbarung von Informationen anhand der festgelegten Erwartungsnorm umgegangen wird. Der alleinige „notice and choice“-Ansatz von Datensammlern ist unvollständig und befähigt den Nutzern kaum selbstbestimmte Entscheidungen zur Offenbarung von Informationen zu treffen. Es bietet auch weniger Schutz, wenn Internetunternehmen unsere Daten in unerwarteter Weise verwenden. Beispielsweise wenn künstliche Intelligenz oder komplexe Algorithmen auf Webplattformen verwendet werden, um unser Verhalten vorherzusagen und unsere Online-Erfahrungen zu beeinflussen (Waldman, 2018).

Hier muss dann mit gesetzlichen Mitteln reguliert werden und ein rechtliches Prinzip des Vertrauens erarbeitet werden, mit welchen Datensammler zu einem gewissen Grad zur

Verantwortung einer Treue dem Nutzer gegenüber gezogen werden können (Waldman, 2018). Andrerseits ist es wichtig, neben Internet-Plattformen, die unser Vertrauen missbrauchen, unsere Daten stehlen und uns für ihren eigenen Profit schädigen, vertrauenswürdige Alternativen und Angebote für Technologien zu schaffen. Diese können sich auf diese drei Vertrauensnormen beziehen: Authentizität, Logik und Empathie [1] .

Während sich diese Arbeit aus Sicht der digitalen Unsichtbarkeit vor allem auf die Instanz der Kontrolle fokussiert hat, darf die Instanz des Vertrauens nicht vernachlässigt werden. Denn das selbstbestimmte Handeln erfordert das Bewegen zwischen diesen Instanzen, um sowohl Wissen als auch Erfahrungen auf dem Weg zur digitalen Souveränität zu sammeln (Wittpahl, 2017).

6.4 Limitationen dieser Arbeit

Im Folgenden wird noch auf die Limitationen dieser Arbeit eingegangen. Die Ergründung der digitalen Unsichtbarkeit erfolgte aus primär konzeptioneller Sicht, weswegen nicht tiefer auf tatsächliche praktische Möglichkeiten eingegangen wurde. Um die Beantwortung der Forschungsfrage auszuweiten, wäre eine erweiterte Prüfung von technischen als auch rechtlichen Möglichkeiten anhand dem herausgesuchten Konzept der Unbeobachtbarkeit interessant gewesen. Zudem wäre eine weitere Ergründung von konzeptionellen Modellen, die unserer digitalen Unsichtbar gerecht werden, von Vorteil, um die Ergründung einer eindeutigeren Definition auszuführen. Hierbei wäre die Suche nach weiteren Modellen, die die digitale Unsichtbarkeit mit den Teilen einer Person (ihrer Identität, dem Image, welches sie vermittelt und ihrer Reputation) verbindet, von Vorteil. In dieser Arbeit wurde der Schluss unserer digitalen Unsichtbarkeit auf die Unverkettbarkeit ihrer persönlichen Identität zu den Eigenschaften und Handlungen, die eine Person mithilfe einer digitalen Identität im digitalen Raum zugeordnet werden können, gezogen.

Die Aufzählung weiterer Beispiele und Gründe für den Wunsch nach digitaler Unsichtbarkeit wäre interessant gewesen. Der nicht angesprochene Fall des digitalen Identitätsdiebstahls wäre eine weitere Verbildlichung wie der Zugriff von Anderen uns digital sichtbar machen kann. Hierbei wäre es interessant zu untersuchen gewesen, inwieweit man heutzutage auch schon über öffentlich zugängliche Informationen eine digitale Identität nachbilden kann und die Reputation einer lebenden Person beeinflussen kann.

Zum anderen ist die ethische Frage nach der Verantwortung für die erzeugten Daten und der Verantwortung für veröffentlichte Informationen zu kurz gekommen. Die ethischen Implikationen einer digitalen Unsichtbarkeit, speziell den Teil der Anonymität, könnten in Bezug auf das Vertrauen anderer in solch einen anonymen Akteur und die Zuschreibungsfähigkeit getätigter Aussagen oder Aktionen im digitalen Raum in einer Diskussion beleuchtet werden. Diese Diskussion ist vor allem im Kontext von Cyber-Hass von großer Bedeutung. Die Verantwortung kann aber auch aus der Sicht der erzeugten Menge an Daten betrachtet werden. Hier stellt sich die Frage wer die Verantwortung für die erzeugten Daten übernimmt und wie man den Besitzanspruch der Daten als auch Informationen auslegt. Denn Daten erfordern Speicherung und Verarbeitung, die natürliche Ressourcen verbraucht. Im Kontext vom Umweltschutz könnte man die Frage nach einer digitalen Unsichtbarkeit auch auf die Verantwortung der Umwelt gegenüber auslegen.

1: *„People tend to trust you when they think they are interacting with the real you (authenticity), when they have faith in your judgment and competence (logic), and when they believe that you care about them (empathy).“(*Frei & Morriss, 2021, S.20)

7. Fazit

Abschließend lässt sich feststellen, das die Thematik unserer digitalen Unsichtbarkeit komplex ist und viele verschiedene Aspekte einbezieht und beeinflussen kann. Auch die Definition unserer digitalen Unsichtbarkeit erfordert weiterer Forschung, um im Zeitalter der allumfassenden Digitalisierung relevant zu sein. Die Erkenntnis, dass unsere digitale Unsichtbarkeit sowohl im absoluten Sinne als auch im relativen Sinne zum speziellen Beobachter ausgelegt werden kann, hilft bei der Bestimmung des Handlungsspielraums, den eine Person zur Verfügung haben kann. Mehr geht es jedoch aber um die Förderung der Autonomie einer Person - das Ermächtigen selbständig in einem möglichen Sichtbarkeitsverhältnis zu handeln. Der Frage, wie man dieses selbstbestimmte Handeln fördert, beispielsweise mithilfe von Identitätsmanagement, kann sich in einem zukünftigen Projekt angenommen werden.

Abbildungsverzeichnis

Quellen

Abbt, C. (2018). 2 Forgetting: In a Digital Glasshouse. In F. Thouvenin, P. Hettich, H. Burkert, & U. Gasser (Hrsg.), *Remembering and Forgetting in the Digital Age* (S. 124–134). Springer International Publishing. https://doi.org/10.1007/978-3-319-90230-2_9

Aniello Castiglione, Giuseppe Cattaneo, Giancarlo De Maio, Alfredo De Santis. (2011). *Automatic, Selective and Secure Deletion of Digital Evidence*. 392–398. https://doi.org/10.1109/BWCCA.2011.64

Balkan, A. (2017, März 12). *We didn't lose control – it was stolen*. https://ar.al/notes/we-didnt-lose-control-it-was-stolen/

BfDI. (o. J.). *Datenschutzrechte der DSGVO - Das Recht auf Löschung / „Recht auf Vergessenwerden" (Art. 17 DSGVO)*. Abgerufen 26. November 2023, von https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_L%C3%B6schung_Vergessenwerden.html

Brantner, C., & Stehle, H. (2021). Visibility in the digital age: Introduction. *Studies in Communication Sciences*, *21*(1), Article 1. https://doi.org/10.24434/j.scoms.2021.01.006

Brighenti, A. (2007). Visibility: A Category for the Social Sciences. *Current Sociology*, *55*(3), 323–342. https://doi.org/10.1177/0011392107076079

Ehrmann, T. (2022, November 22). *Was der Schutz der Privatsphäre mit der Maslowschen Bedürfnispyramide zu tun hat*. HWZ Digital - Institute for Digital Business. https://hwzdigital.ch/was-der-schutz-der-privatsphaere-mit-der-maslowschen-bedurfnispyramide-zu-tun-hat/

Esposito, E. (2002). *Soziales Vergessen: Formen und Medien des Gedächtnisses der Gesellschaft* (1. Aufl). Suhrkamp.

Foucault, M. (1977). *Überwachen und Strafen: Die Geburt des Gefängnisses* (W. Seitter, Übers.). Suhrkamp.

Frei, F., & Morriss, A. (2021). Trust: The Foundation of Leadership. *Leader to Leader*, *2021*(99), 20–25. https://doi.org/10.1002/ltl.20544

Frey, B. S. (2023). Camouflage: A dominant reaction to worsening conditions. *Rationality and Society*, *35*(3), 366–384. https://doi.org/10.1177/10434631231157588

Giannopoulou, A. (2023). Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity. *Digital Society*, *2*(2), 18. https://doi.org/10.1007/s44206-023-00049-z

Hui, Y. (2013). *Deduktion, Induktion und Tranduktion. Über Medienästhetik und digitale Objekte*. https://doi.org/10.25969/MEDIAREP/736

Kvakic, M., & Wærdahl, R. (2022). Trust and Power in the Space Between Visibility and Invisibility. Exploring Digital and Social Media Practices in Norwegian Child Welfare Services. *European Journal of Social Work*, *0*(0), 1–12. https://doi.org/10.1080/13691457.2022.2099350

Latour, B. (2013). Achtung: Ihre Phantasie hinterlässt digitale Spuren! In H. Geiselberger & T. Moorstedt (Hrsg.), *Big Data: Das neue Versprechen der Allwissenheit* (S. 119–123). Suhrkamp Verlag.

Mayer-Schönberger, V. (2018). 1 Remembering (to) Delete: Forgetting Beyond Informational Privacy. In F. Thouvenin, P. Hettich, H. Burkert, & U. Gasser (Hrsg.), *Remembering and Forgetting in the Digital Age* (S. 118–123). Springer International Publishing. https://doi.org/10.1007/978-3-319-90230-2_8

Mead, G. H. (1934). *Mind, self, and society*. University of Chicago Press.

Mitnick, K. (o. J.). Famed Hacker Kevin Mitnick Shows You How to Go Invisible Online. *Wired*. Abgerufen 1. Dezember 2023, von https://www.wired.com/2017/02/famed-hacker-kevin-mitnick-shows-go-invisible-online/

Müller, B. (2018). *Was ist Privatsphäre?* [PDF]. https://doi.org/10.2313/NET-2018-11-1_09

Nabeth, T. (2009). Identity of Identity. In K. Rannenberg, D. Royer, & A. Deuker (Hrsg.), *The Future of Identity in the Information Society* (S. 19–69). Springer. https://doi.org/10.1007/978-3-642-01820-6_2

Nassehi, A. (2019). *Muster: Theorie der digitalen Gesellschaft*. C.H. Beck.

Neumayer, C., Rossi, L., & Struthers, D. M. (2021). Invisible Data: A Framework for Understanding Visibility Processes in Social Media Data. *Social Media + Society*, *7*(1), 2056305120984472. https://doi.org/10.1177/2056305120984472

Nyst, C., Makin, P., Pannifer, S., & Whitley, E. (2016, Juni 21). *Digital identity: Issue analysis: executive summary*. https://www.semanticscholar.org/paper/Digital-identity%3A-issue-analysis%3A-executive-summary-Nyst-Makin/4dbafd1debd15ce2a933e8573913298f70d958e7

Öhman, C. J., & Watson, D. (2019). Are the dead taking over Facebook? A Big Data approach to the future of death online. *Big Data & Society*, *6*(1), 2053951719842540. https://doi.org/10.1177/2053951719842540

Pfitzmann, A., Dresden, T., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*.

Ricoeur, P. (1992). *Oneself as another*. University of Chicago Press.

Seigneur, J.-M., & Jensen, C. D. (2004). Trading Privacy for Trust. In C. Jensen, S. Poslad, & T. Dimitrakos (Hrsg.), *Trust Management* (S. 93–107). Springer. https://doi.org/10.1007/978-3-540-24747-0_8

Stasch, D. (o.J.). Einflusssphären. *Bezogen aus einer Unterrichtseinheit*

Stohl, C., Stohl, M., & Leonardi, P. M. (2016). Digital Age | Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age. *International Journal of Communication*, *10*(0), Article 0.

Thompson, J. B. (2005). The New Visibility. *Theory, Culture & Society*, *22*(6), 31–51. https://doi.org/10.1177/0263276405059413

Viangalli, F. (2022). *The Invisible Man in the Digital Age: From Myth to Reality* (SSRN Scholarly Paper 4166807). https://doi.org/10.2139/ssrn.4166807

Waldman, A. E. (2018). *Privacy as Trust: Information Privacy for an Information Age* (1. Aufl.). Cambridge University Press. https://doi.org/10.1017/9781316888667

Wang, F., & De Filippi, P. (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*. https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028

Westin, A. F. (1967). *Privacy and freedom*. New York, Atheneum. http://archive.org/details/privacyfreedom00west

Wilms, R. A. (2023, Juli 25). *Datenlöschung: Informationen zur Datenvernichtung*. Herfurtner Rechtsanwälte. https://kanzlei-herfurtner.de/datenloeschung/

Wittpahl, V. (Hrsg.). (2017). *Digitale Souveränität*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-55796-9

Zuboff, S. (2015). *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization* (SSRN Scholarly Paper 2594754). https://papers.ssrn.com/abstract=2594754

Eidesstattliche Erklärung

Ich versichere, dass die vorliegende Arbeit selbstständig verfasst und keine anderen als die im Quellenverzeichnis angegebenen Quellen verwendet wurden. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichen Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit ist in gleicher oder ähnlichen Form noch bei keiner anderen Prüfungsbehörde eingereicht worden. Mir ist bekannt, dass ein Täuschungsversuch, der zur Exmatrikulation führen kann, vorliegt, wenn sich die vorstehende Erklärung als unrichtig erweist.

Darmstadt, den 01.12.2023

J.Podlipensky

Julia Podlipensky