

6 Privatsphäre

Die Verletzung der Privatsphäre ist ein Risiko, welchem die Datenquellen in einem Datenökosystem ausgesetzt werden. In diesem Kapitel wird erarbeitet, wieso die Verletzung der Privatsphäre überhaupt ein unerwünschtes Ereignis wäre, warum eine solche Verletzung eine verbotene Handlungsfolge wäre und wie man die Privatsphäre schützen bzw. fördern kann. Dafür ist es zuerst einmal notwendig zu definieren, was genau mit Privatsphäre gemeint ist – insbesondere wann Privatsphäre intakt ist und wann sie verletzt ist. Nur so können Bedingungen abgeleitet werden, unter denen es möglich ist, vor der Verletzung zu schützen und die intakte Privatsphäre zu fördern bei der Gestaltung eines Datenökosystems. Deshalb soll das Phänomen der Privatsphäre zunächst deskriptiv erfasst werden. Erst wenn klar definiert ist, unter welchen Umständen Privatsphäre intakt oder verletzt ist, soll ein normativer Maßstab angelegt werden und auch gefragt werden, ob es eine moralische Pflicht zum Schutz der Privatsphäre gibt. Wenn bei der rein deskriptiven Definition des Begriffes der Privatsphäre schon von einem Recht auf Privatsphäre die Rede ist, wird dieses Recht vorläufig als Anspruch verstanden, der sich aus einer moralischen Pflicht ableitet.

Der Politik- und Geschichtsphilosoph Raymond Geuss meint, öffentlich und privat lassen sich nicht klar voneinander unterscheiden, da sich diese beiden Sphären überschneiden. Seiner Meinung nach wird der Unterscheidung zwischen öffentlich und privat eine zu große Bedeutung zugeschrieben.⁵²⁶ Es reiche nicht, auf die Frage, warum wir uns nicht einmischen sollten, „weil es privat ist“ zu antworten. Denn daraufhin müsste die Frage beantwortet werden, warum wir denken, dass wir uns in private Vorgänge nicht einmischen sollten. Geuss nimmt an, dass die Gründe sehr unterschiedlich wären und hier keine einheitliche Erklärung gefunden werden kann.⁵²⁷

526 Geuss 2001:5

527 Ebd.:107

Im Folgenden möchte ich zeigen, dass es doch eine einheitliche Erklärung gibt, und dass es bei dem Konzept der Privatsphäre weniger um die Ablehnung von Einmischung geht, sondern mehr um die Ablehnung von Kontrollverlust.

Laut Duden kommt das Wort „privat“ vom lateinischen „privatus“ und bedeutet „(der Herrschaft) beraubt; gesondert, für sich stehend; nicht öffentlich“.⁵²⁸ Der Jurist Thomas McIntyre Cooley orientiert sich bei seiner Definition von Privatsphäre sehr nah an dieser ursprünglichen Begriffsbedeutung: „The right to one's person may be said to be a right of complete immunity: to be let alone.“⁵²⁹ Ursprünglich wurde unter Privatsphäre also die Abgeschiedenheit von der Gesellschaft, das In-Ruhe-gelassen-werden verstanden.

Der Rechtsphilosoph und Ethiker William Parent ist der Meinung, dass die Definition von Privatsphäre als reine Abgeschiedenheit zu weit gefasst ist und dass sie den begrifflichen Kern der Privatsphäre völlig verkennt. Angenommen, eine Person A wird von B angegriffen. B hat A nicht in Ruhe gelassen, aber das bedeutet nicht, dass B in die Privatsphäre von A eingedrungen ist. Vielmehr sind zuerst einmal Begriffe wie Übergriff, Angriff und Gewalt hilfreich zum Beschreiben des Vorfalls. Das Konzept der Privatsphäre würde erst dann benötigt, wenn zum Beispiel B das Portemonnaie von A stiehlt und beim Ausräumen etwas Persönliches über A erfährt. Die Definition der Privatsphäre als Rückzug der Person von der Gesellschaft suggeriert fälschlicherweise, dass jedes Mal, wenn eine Person mit der Gesellschaft in Kontakt kommt, ihre Privatsphäre beeinträchtigt wird.⁵³⁰ Hier wird deutlich, dass ein angemessenes Konzept der Privatsphäre nicht zulassen darf, dass die Privatsphäre einer Person bereits dadurch verletzt werden kann, indem sie in der Öffentlichkeit wahrgenommen wird.⁵³¹

Es gibt verschiedene Dimensionen des Privaten: Rössler unterscheidet zwischen lokaler, dezisionaler und informationeller Privatheit.⁵³² Auch der Datenethiker und Technologiephilosoph Adam D.

528 Duden 2023

529 Cooley 1879:29; Oft werden als Autoren dieser Definition fälschlicherweise die Juristen Samuel D. Warren und Louis D. Brandeis genannt, welche sich jedoch auf Cooley beziehen (Warren, Brandeis 1890:195).

530 Parent 1983b:342

531 Ebd.:344

532 Rössler 2003:31

Moore macht einen Unterschied zwischen privaten Orten und Informationen – anstatt auf private Entscheidungen legt er aber den Fokus auf die Privatheit von Körpern.⁵³³ Ich denke, die Privatheit von Körpern ist nicht zu vernachlässigen, da sie vor ungewollten Übergriffen schützen kann. Private Entscheidungen beziehen sich auf Entscheidungen, die über den eigenen Körper und private Orte hinaus gehen: „(...) mit wem will ich zusammenleben; welchen Beruf will ich ergreifen; aber auch: welche Kleidung trage ich (...)“.⁵³⁴ Auch hier ermöglicht die Privatsphäre einen Rückzug und dadurch eine Entscheidung ohne Beeinträchtigung. Die Dimensionen der Privatheit sind also Informationen, Orte, Körper und Entscheidungen.

Vor der Digitalisierung war die Zugangskontrolle zu Orten und Körpern das vorrangige Ziel der Privatsphäre, da alle persönlichen Informationen dort zu finden waren. Im Kontext der Digitalisierung sind persönliche Informationen allerdings von überall her zugänglich. Nun muss sich der Datenschutz an die technologischen Entwicklungen anpassen, indem er seinen Schwerpunkt auf den Schutz personenbezogener Daten verlagert. Die Wirtschaftswissenschaftler:innen Alessandro Acquisti, Laura Brandimarte und Jeff Hancock stimmen zu: „(...) the very boundaries of privacy have evolved with the digital transition—from predominantly physical to predominantly informational.“⁵³⁵ Da in dieser Arbeit der Umgang mit personenbezogenen Daten ethisch betrachtet wird, ist die Dimension der informationellen Privatheit besonders interessant. Im Folgenden ist deshalb mit Privatsphäre immer informationelle Privatsphäre gemeint.

Persönliche Informationen

Es fragt sich nun, was genau unter „persönliche Informationen“ oder aber „personenbezogene Daten“ fällt. Von dieser Definition ist abhängig, über welchen Gegenstand private Individuen die Kontrolle haben sollten. Die DSGVO bezeichnet als „(...) „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder

533 Moore 2010:27

534 Rössler 2003:31

535 Acquisti et al. 2022:271

identifizierbare natürliche Person (...) beziehen (...).“⁵³⁶ In gleicher Weise sind mit „persönlichen Informationen“ laut O’Neill solche Informationen gemeint, welche ein Individuum identifizierbar machen: „The standard approach is to deem information ‘personal’ if it enables the identification of individuals.“⁵³⁷ Eine solche Definition wäre allerdings zu weit gefasst, da viele Informationen, die ein Individuum identifizierbar machen, öffentlich verfügbar sind, dadurch dass sich das Individuum zum Beispiel an öffentlichen Orten aufhält. So schreiben der Religionsphilosoph Neil Manson und die bereits erwähnte Ethikerin und politische Philosophin Onora O’Neill: „Personal information, in the sense that may be relevant to an account of informational privacy, cannot include publicly available knowledge about individuals.“⁵³⁸ Wenn es um frei verfügbare Informationen geht, von denen Außenstehende unweigerlich Kenntnis erlangen, kann sich das Individuum nicht auf die Privatsphäre berufen, um den Außenstehenden zu verbieten, von diesen Informationen Kenntnis zu erlangen.

Eine andere Möglichkeit wäre, nur die als persönliche Informationen zu definieren, die genau eine Person identifizierbar machen. Aber diese Definition ist wiederum zu eng, denn auch wenn die Information „Jemand hat Krebs“ auf viele Individuen zutrifft, könnte jedes dieser Individuen ein Interesse daran haben, diese Tatsache über seine Gesundheit privat zu halten. Manson und O’Neill schlussfolgern: „So private information is at most a subset of the information that is true of a person and not already public knowledge.“⁵³⁹ Persönliche Informationen müssen also auf eine Person zutreffen und dürfen nicht bereits öffentlich bekannt sein. Um genauer zu definieren, was in diese Kategorie fällt, könnte man sich auf das Interesse an Privatsphäre fokussieren. Dadurch würde allerdings das Problem nur verlagert, da man spezifizieren müsste, was vernünftigerweise als intim oder sensibel anzusehen ist.⁵⁴⁰

Der Medizinethiker Andrea Martani und der Technologieethiker Patrik Hummel sind der Meinung, dass nicht nur personenbezoge-

536 Art. 4, Abs. 1, Satz 1 DSGVO

537 O’Neill 2021:81

538 Manson, O’Neill 2007:103

539 Ebd.

540 Ebd.:103f.

ne Daten ein Schutzgegenstand des Datenschutzes sein sollten, da Daten nicht personenbezogen sein müssen, um durch ihre Verarbeitung eine Gefahr für ein Individuum darzustellen.⁵⁴¹ Denn es ist möglich, dass aus nicht-persönlichen Informationen, persönliche Informationen über geschützte Merkmale abgeleitet werden.⁵⁴² Das geschieht durch sogenannte Inferenzen. Der Datenethiker Jakob Mainz erklärt ihre Funktionsweise mit Bezug auf Barocas und Nissenbaum folgendermaßen: „(...) pieces of information that are clearly personal can often be inferred from pieces of information that are clearly non-personal (...)“⁵⁴³ Inferenzen sind Informationen, die durch Schlussfolgerungen oder Überlegungen und nicht durch direkte Beobachtung oder Erhebung bei der betroffenen Person gewonnen werden.⁵⁴⁴ Durch solche indirekten Mittel ist es möglich, Rückschlüsse auf genau die Eigenschaften zu ziehen, die ohne identifizierende Informationen lange Zeit nicht bekannt zu sein schienen.⁵⁴⁵

Auf Grund eines Artikels von dem Journalisten Charles Duhigg im New York Times Magazine kursiert eine Anekdote, die ein gutes Beispiel liefert für solche möglichen Inferenzen: Eine junge Frau soll auf Grund ihres Kaufverhaltens bei Target (einer der größten Einzelhändler der USA) Gutscheine für Babykleidung und Kinderbetten zugeschiedt bekommen haben. Sie soll wirklich schwanger gewesen sein, aber ihr Vater, bei dem sie wohnte, soll nichts davon gewusst haben und erst durch die zugesandten Gutscheine davon erfahren haben. Eine solche Schlussfolgerung über die Schwangerschaft einer Konsumentin lässt sich deshalb ziehen, weil andere Konsumentinnen preisgeben, dass sie schwanger sind. Diese schwangeren Frauen weisen ein bestimmtes Konsumverhalten auf und kauften zum Beispiel größere Mengen an unparfümierter Lotion sowie Nahrungsergänzungsmittel wie Kalzium, Magnesium und Zink. Wenn eine andere Frau das gleiche Konsumverhalten zeigt, wird daraus geschlossen, dass sie auch schwanger ist.⁵⁴⁶ Die Anekdote beweist nicht ein-

541 Martani, Hummel 2022:37

542 Manson, O'Neill 2007:104; Wachter, Mittelstadt 2019:564; Martani, Hummel 2022:34

543 Mainz 2022:565, Fußnote 14; Vgl. Barocas, Nissenbaum 2014:55

544 Wachter und Mittelstadt 2019:515; Martani, Hummel 2022:33

545 Barocas, Nissenbaum 2014:55

546 Duhigg 2012; Hill 2012; Barocas, Nissenbaum 2014:62

deutig, dass Target die Schwangerschaft der jungen Frau aus ihrem Konsumverhalten abgeleitet hat⁵⁴⁷, zeigt aber beispielhaft, welches Potenzial datenbasierte Inferenzen haben können.

Dieses Handeln auf Grundlage der Inferenzen hat dann aber nicht mehr notwendigerweise einen Bezug zur Privatsphäre des Einzelnen. Es wird zwar nach kleinen, aussagekräftigen Verbindungen zwischen Einzelpersonen gesucht, aber daraus werden Gruppenprofile erstellt, um noch mehr Informationen über Dritte herausfinden zu können.⁵⁴⁸ Autoren wie der Technologiephilosoph und Digitalethiker Luciano Floridi behaupten, es handle sich hier um eine Gruppenprivatsphäre, die verletzt würde.⁵⁴⁹ Er erklärt diese mit folgender Analogie: „The individual sardine may believe that the encircling net is trying to catch it. It is not. It is trying to catch the whole shoal. It is therefore the shoal that needs to be protected, if the sardine is to be saved.“⁵⁵⁰ Floridi argumentiert, dass bei der Datenverarbeitung eher Typen bzw. Gruppen behandelt werden als Einzelpersonen.⁵⁵¹ Denn Einzelpersonen werden in Gruppen eingeteilt von zum Beispiel schwangeren Frauen: „(...) most people are not targeted (...) as individuals but as members of specific groups (...)“⁵⁵² Laut Floridi können Einzelpersonen manchmal nur dadurch geschützt werden, dass die Gruppe geschützt wird, welcher die Einzelpersonen angehören.⁵⁵³

Die Gruppenprivatsphäre ist in solchen Kontexten relevant, in denen Inferenzen genutzt werden, um Nutzerpräferenzen, sensible Attribute und Meinungen abzuleiten oder Verhaltensweisen vorherzusagen.⁵⁵⁴ So kann zum Beispiel von dem Online-Verhalten der Facebook Nutzenden politische Meinungen und der Gemütszustand abgeleitet werden und dann genutzt werden, um gezielt Werbung zu machen.⁵⁵⁵ Auch im Kontext von Versicherungen oder Bepreisung von Produkten sollte die Gruppenprivatsphäre Beachtung finden, da

547 Fraser 2020

548 Wachter, Mittelstadt 2019:506

549 Floridi 2017

550 Floridi 2014:3

551 Ebd.:1f.

552 Ebd.:1

553 Ebd.:3

554 Wachter, Mittelstadt 2019:497

555 Merrill 2016; Reilly 2017; Wachter, Mittelstadt 2019:506f.

es hier möglich ist, dass die Menschen auf Grund der Zugehörigkeit zu einer Gruppe schlechter gestellt werden. In dieser Arbeit soll jedoch ausschließlich die individuelle Privatsphäre betrachtet werden, da es im Verwaltungskontext meist eine Person ist, die eine Verwaltungsleistung in Anspruch nimmt und dann individuelle Ergebnisse zur Verfügung gestellt bekommt. Selbst wenn eine Gruppe von Personen, wie zum Beispiel Eltern, gemeinsam eine Verwaltungsleistung in Anspruch nehmen, werden zur Bearbeitung des Antrags keine Gruppenprofile erstellt, sodass die Gruppenprivatsphäre keine Rolle spielt.

Trotzdem gibt die Möglichkeit der Inferenzen wichtige Hinweise für die Bestimmung von persönlichen Informationen, da hier potenzielle Schäden nicht dadurch entstehen, dass die verarbeiteten Daten personenbezogen waren, sondern dass sie verwendet wurden um Personen zu beeinflussen oder um Entscheidungen über sie zu fällen.⁵⁵⁶ Die Rechtswissenschaftlerin Sandra Wachter und der bereits erwähnte Datenethiker Brent Mittelstadt fügen hinzu: „The belief that certain categories of data are fundamentally less harmful or risky than others is undermined by Big Data analytics.“⁵⁵⁷ Auf Grund der Möglichkeit, Inferenzen zu bilden, sei es schwierig, wirklich neutrale Informationen zu finden, die nicht in personenbezogene Daten umgewandelt werden können.⁵⁵⁸ Dies zeigt auf, dass die Unterscheidung von persönlichen und nicht-persönlichen Informationen wenig hilfreich ist, da jegliche Information in Kombination mit anderen Informationen persönlich werden kann.

Auch Manson und O'Neill sind der Meinung, dass es nicht darum geht, welche Informationen persönlich sind und dementsprechend in den Bereich der Privatsphäre fallen. Denn Informationen an sich hätten keine ethische Bedeutung und seien nicht als solche schutzbedürftig: „What is informative and significant for one person is often meaningless or irrelevant to another.“⁵⁵⁹ Außerdem kann niemand den Anspruch erheben, dass Außenstehende bestimmte Informationen nicht über ihn/sie wissen dürfen.⁵⁶⁰ Denn kein Individuum

556 Wachter, Mittelstadt 2019:616

557 Ebd.:616

558 Ebd.:518

559 Manson, O'Neill 2007:108

560 Thomson 1975:307

kann kontrollieren, was Außenstehende über es denken oder welche Schlüsse Außenstehende aus öffentlich verfügbaren Informationen über das Individuum ziehen.⁵⁶¹

Manson und O'Neill machen stattdessen auf die Art der Beschaffung der Daten aufmerksam: „The acquisition of ‘personal’ information is often an unavoidable or highly likely consequence of morally permissible action. However, in some cases the routes or means by which such knowledge is acquired may be intrusive and impermissible.”⁵⁶² Deshalb geht es bei der Privatsphäre nicht um den Inhalt der Informationen, sondern um Handlungen und Kommunikation, die zur Beschaffung von „persönlichen“ Informationen führen können, sowie um die Verwendungen solcher Informationen. Mainz zufolge sind Inferenzen zulässig, solange das Erwerben der Daten zulässig war. Eine Inferenz verletzt jedoch die Privatsphäre der Betroffenen, wenn die für die Inferenz notwendigen Informationen nicht rechtmäßig erlangt wurden.⁵⁶³

Auch laut Manson und O'Neill muss unterschieden werden zwischen moralisch zulässigen und moralisch unzulässigen Handlungen, welche zur Beschaffung und Verarbeitung von Informationen über andere führen.⁵⁶⁴ Solche Handlungen können moralisch unzulässig sein, wenn sie zum Beispiel unverständlich, irrelevant, zwanghaft, schädlich, belastend, irreführend oder unehrlich sind, und damit gegen ethische und epistemische Normen verstoßen.⁵⁶⁵ Deshalb sollte es für diejenigen, die Informationen über andere beschaffen und verarbeiten, bestimmte Pflichten geben.⁵⁶⁶ In dieser Arbeit wurde Kants dritte Formel des Kategorischen Imperativs als eine solche Pflicht für das Sammeln und Verarbeitung von Daten eingeführt – das heißt, niemand darf dabei als bloßes Mittel gebraucht werden. Bei der informationellen Privatsphäre geht es also weniger darum, welche Informationen privat sind, sondern mehr darum, wie die

561 Manson, O'Neill 2007:106

562 Ebd.

563 Mainz 2022:569

564 Ebd.:110

565 Ebd.:121

566 Ebd.:111

Informationen erlangt werden und zu welchem Zweck sie verarbeitet werden.⁵⁶⁷

6.1 Kriterien für eine Definition

Es stellt sich weiterhin die Frage, wann Privatsphäre intakt und wann sie verletzt ist. Hierzu gibt es verschiedene Auffassungen in der Literatur, wie zum Beispiel das Verständnis von Privatsphäre als das Recht in Ruhe gelassen zu werden⁵⁶⁸ – auch der Zugangs-Ansatz und der Kontroll-Ansatz werden im Folgenden eine Rolle spielen. Aber zuerst muss geklärt werden, wie festgestellt werden kann, ob sich ein Ansatz als Definition von Privatsphäre eignet.

Der Ethiker, Sozial- und politische Philosoph Leonhard Menges identifiziert in der Literatur ein Standardverfahren zur Prüfung der Angemessenheit von Definitionen der Privatsphäre. Dafür wird eine beispielhafte Situation entwickelt, in der es intuitiv plausibel ist, dass ein Akteur in Bezug auf eine bestimmte Information Privatsphäre hat. Auch die zu prüfende Definition von Privatsphäre sollte in dieser Situation zu dem Schluss kommen, dass die Privatsphäre des betroffenen Akteurs gegeben ist. Als nächstes stellt man sich ein Ereignis vor, das die Situation in einer Weise verändert, die entweder (a) intuitiv die Privatsphäre der Person nicht beeinträchtigt oder (b) intuitiv die Privatsphäre der Person beeinträchtigt. Die Definition von Privatsphäre wird dann geprüft, indem sie auf die durch das Ereignis veränderte Situation angewendet wird. Wenn das Ereignis (a) intuitiv die Privatsphäre der Person nicht beeinträchtigt, die Definition aber impliziert, dass dies der Fall ist, dann ist die Definition zu weit gefasst und impliziert falsch-positive Ergebnisse. Wenn das Ereignis (b) intuitiv die Privatsphäre der Person beeinträchtigt, die

567 Im Folgenden wird angenommen, dass die Daten im Verwaltungskontext immer Individuen betreffen und es deshalb relevant ist, wie die Informationen erlangt werden und zu welchem Zweck sie verarbeitet werden. Die Begriffe ‚persönlich‘ und ‚personenbezogen‘ werden im Folgenden in Bezug auf Informationen und Daten verwendet, um zu kennzeichnen, dass Individuen betroffen sind.

568 Cooley 1879:29; Warren, Brandeis 1890:195

Definition aber impliziert, dass dies nicht der Fall ist, dann ist die Definition zu eng und impliziert falsch-negative Ergebnisse.⁵⁶⁹

Beispiele für Ereignisse vom Typ (a), durch welche die Privatsphäre intuitiv nicht beeinträchtigt wird, sind sogenannte *Threatened Loss Cases*. Ein Beispiel dieser Art von der Moralphilosophin und Metaphysikerin Judith Jarvis Thomson, weiterentwickelt von Parent und Menges, ist ein Streit zwischen zwei Partner:innen in ihrem eigenen Haus – es sei intuitiv plausibel, dass die streitenden Personen in Bezug auf die Information, dass sie streiten und worüber sie streiten, Privatsphäre haben. Das Ereignis, durch welches die Lage der Privatsphäre neu bewertet werden muss, ist die Erfindung eines Röntgengeräts, das durch Wände schauen kann und auf das Haus der Streitenden gerichtet ist, aber nicht benutzt wird – intuitiv wird dadurch laut Thomson die Privatsphäre der Personen nicht beeinträchtigt⁵⁷⁰: „(...) my right to privacy is not violated until my neighbor actually does train the device on the wall of my house. It is the actual looking that violates it, not the acquisition of power to look.“⁵⁷¹ Ein weiteres Beispiel dieser Art von dem Technologieethiker Kevin Macnish ist eine Situation, in der eine Person im Café persönliche Gefühle und Gedanken in ihr Tagebuch schreibt – es sei intuitiv plausibel, dass die Person in Bezug auf diese Gefühle und Gedanken Privatsphäre hat. Dann verlässt aber die Person das Café und vergisst ihr Tagebuch auf dem Tisch. Eine andere Cafébesucherin legt das Tagebuch auf ihren Tisch, ohne es zu lesen und wartet auf die Rückkehr der Person – intuitiv werde dadurch die Privatsphäre der Person nicht beeinträchtigt.⁵⁷²

Beispiele für Ereignisse vom Typ (b), durch welche die Privatsphäre intuitiv beeinträchtigt wird, sind *Voluntary Divulgence Cases*. Ein Beispiel dieser Art ist eine Situation, in der jemand wegen Selbstzweifeln eine Flasche Schnaps am Tag trinkt, aber niemand davon weiß – es sei intuitiv plausibel, dass die Person in Bezug auf diese Information Privatsphäre hat. Das Ereignis, durch welches die Lage der Privatsphäre neu bewertet werden muss, ist, dass die Person freiwillig und nüchtern fremden Menschen von ihren persönli-

569 Menges 2022:697

570 Parent 1983b:344; Menges 2022:697

571 Thomson 1975:305, Fußnote 1

572 Macnish 2018:420

chen Problemen und dem regelmäßigen Alkoholkonsum erzählt – intuitiv werde dadurch die Privatsphäre der Person beeinträchtigt.⁵⁷³

Das Problem an diesem Standardverfahren zur Prüfung der Angemessenheit von Definitionen der Privatsphäre ist, dass womöglich nicht alle Menschen die gleiche Intuition haben bezüglich dieser Beispiele.⁵⁷⁴ Wenn wir aber die Definition von Privatsphäre in verschiedenen Beispielszenarien ausschließlich an Intuitionen messen, dann müssten alle die gleiche Intuition haben, damit diese Messungen allgemeingültig sind. Zu folgendem Beispiel gibt es sogar in der Literatur unterschiedliche Intuitionen: Der Wind weht das Tagebuch aus dem offenen Rucksack einer Person, und es landet mit den Seiten nach oben auf dem Bürgersteig. Eine andere Fußgängerin ist so freundlich, das Tagebuch aufzuheben, doch dabei kann sie nicht umhin, einen Teil des Inhalts zu lesen. Die Datenethikerin Haleh Asgarinia vertritt die Intuition, dass in diesem Beispiel die Privatsphäre der Tagebuchbesitzerin verletzt wird, da die Fußgängerin einen Teil des Tagebuchinhalts liest, obwohl die Tagebuchbesitzerin sich nicht wünscht, dass die Fußgängerin das Tagebuch liest.⁵⁷⁵ Den Datenethikern Jakob Thrane Mainz und Rasmus Uhrenfeldt zufolge wird dadurch jedoch intuitiv die Privatsphäre der Person nicht beeinträchtigt, weil der Kontrollverlust über das Tagebuch nicht auf die Handlung eines anderen Akteurs zurückzuführen ist.⁵⁷⁶ Hier zeigt sich, dass sich die Debatte zum Teil darum dreht, welche Intuitionen richtig sind.⁵⁷⁷ Insbesondere, wenn es gegensätzliche Intuitionen in Bezug auf eine Situation gibt, wird deutlich, dass es problematisch ist, eine Intuition als Kriterium für die Definition eines Begriffes zu betrachten.

Deshalb wird in dieser Arbeit die Angemessenheit von Definitionen der Privatsphäre nicht anhand von Gegenbeispielen geprüft. Stattdessen lässt sich allein auf Grund der Fragestellung in diesem Kapitel ein Kriterium für eine Definition von Privatsphäre aufstellen: Eine Definition der Privatsphäre sollte die Möglichkeit bieten, nicht nur zu bestimmen, wann die Privatsphäre durch Außenstehende verletzt wird, sondern auch wann sie intakt ist.

573 Parent 1983a:273; Menges 2022:698

574 Menges 2020c:394; Lundgren 2021a:672

575 Asgarinia 2023:335

576 Mainz, Uhrenfeldt 2021:298

577 Lundgren 2021a:672

6.1.1 Individuelle Intuitionen

Die unterschiedlichen Intuitionen bezüglich der Bedeutung von Privatsphäre lassen sich unter anderem auf unterschiedliche kulturelle Prägungen zurückführen. Denn es lässt sich beobachten, dass Privatsphäre in verschiedenen Kulturen unterschiedlich gelebt wird. Der Jurist Charles Fried stimmt zu: „(...) the concrete expressions of privacy in particular societies and cultures differ enormously.“⁵⁷⁸ So hängt es zum Beispiel von der Kultur ab, ob eine Berührung eine Verletzung der Privatsphäre darstellt. Auch laut Moore gibt es je nach Kultur unterschiedliche normative Ansprüche in Bezug auf die Privatsphäre.⁵⁷⁹ Man könnte auch vermuten, dass verschiedene Generationen der gleichen Kultur ihre Privatsphäre unterschiedlich ausleben. Insbesondere durch die Entstehung von Sozialen Medien ist es seit ca. 30 Jahren möglich, Informationen über sich mit vielen fremden Menschen zu teilen. Es sind vor allem jüngere Menschen – die Generationen, die mit Sozialen Medien aufgewachsen sind –, welche diese Möglichkeit nutzen und persönliche Informationen online teilen. Solche Informationen, zum Beispiel über ihre sexuelle Orientierung oder ihre politische Einstellung, teilen manche Menschen aus älteren Generationen der gleichen Kultur nicht einmal mit ihrem engsten Umfeld.

Ich argumentiere jedoch, dass das Ausleben der Privatsphäre sogar noch individueller ist. Denn jede Person kann individuell entscheiden, ob sie Informationen teilt, welche und mit wem. Deshalb gibt es in jeder Kultur und in jeder Generation Menschen, die sich aktiv dafür entscheiden, persönliche Informationen in Sozialen Medien zu teilen. Der Zweck kann Selbstdarstellung sein, das Finden einer Gruppe von Gleichgesinnten oder auch das Verdienen seines Lebensunterhalts. Die Gruppe von Nutzenden, die Zugriff auf die Informationen bekommen, kann beschränkt werden oder bewusst nicht eingeschränkt werden. Außerdem werden ganz bestimmte Informationen geteilt, viele andere persönliche Informationen behalten die auf Sozialen Medien Aktiven aber für sich. Gleichzeitig gibt es in jeder Kultur und in jeder Generation Menschen, die ihre per-

578 Fried 1968:213

579 Moore 2010:26

sönlichen Informationen nicht online teilen – das Gleiche gilt im analogen Austausch mit Mitmenschen.

Fried zufolge kann in konkreten Situationen und Gesellschaften die Möglichkeit, frei zu entscheiden, ob man Informationen über die eigene Person teilt, relativ und eingeschränkt sein.⁵⁸⁰ Denn wenn in einer Gesellschaft der Zugang zu Sozialen Medien beschränkt ist oder das Veröffentlichen von Informationen über zum Beispiel die sexuelle Orientierung oder die politische Einstellung negative Konsequenzen nach sich ziehen könnte, dann ist es nicht möglich bzw. nicht ratsam bestimmte Informationen auf diesem Weg zu teilen. Das heißt, die Möglichkeit, die eigene Privatsphäre individuell zu gestalten, kann von außen beschränkt sein. Trotzdem können wir hierdurch etwas über die Privatsphäre lernen. So schreibt Moore: „The forms of privacy may be culturally relative, but the need for privacy is not.”⁵⁸¹ Unabhängig davon, wie eine Person ihre Privatsphäre versteht und auslebt, braucht sie Privatsphäre.⁵⁸²

Dadurch wird klar, dass die Definition von Privatsphäre individuellen Intuitionen gerecht werden muss. Insbesondere weil das individuelle Empfinden darüber, welche Informationen persönlich sind, variieren kann, sollte die individuelle Entscheidung darüber, welche Informationen geteilt werden, respektiert werden. Deshalb ist ein weiteres Kriterium für eine Definition von Privatsphäre, neben der Bestimmung von intakter und verletzter Privatsphäre, dass Individuen ihre Privatsphäre unterschiedlich empfinden und ausleben können müssen.

6.2 Ansätze zur Definition von Privatsphäre

Um einer Definition von Privatsphäre näher zu kommen, welche Raum lässt für individuelle Intuitionen und es ermöglicht zu bestimmen, wann Privatsphäre intakt und wann verletzt ist, werden im Folgenden zwei in der Literatur prominente Ansätze vorgestellt und

580 Fried 1968:213

581 Moore 2010:56

582 Warum wird erklärt in Kapitel 6.3

anhand dieser Kriterien bewertet: der Zugangs-Ansatz und der Kontroll-Ansatz.⁵⁸³

6.2.1 Zugangs-Ansatz

Der bereits erwähnte Technologieethiker Kevin Macnish argumentiert, dass ein Verlust der Privatsphäre nur dann eintritt, wenn auf die eigenen Daten tatsächlich zugegriffen wird. Aus Sicht des Zugangs-Ansatzes stellt das Sammeln der Informationen allein keinen Eingriff in die Privatsphäre dar – erst wenn tatsächlich auf die Informationen zugegriffen wird, wird die Privatsphäre verletzt.⁵⁸⁴ Zur Illustration schlägt Macnish das unter 6.1 erwähnte Tagebuchbeispiel vor: Eine Person vergisst ihr Tagebuch auf dem Tisch im Café, und als sie nach 30 Minuten zurückkommt, liegt das Tagebuch auf dem Tisch einer Fremden. Laut Macnish gehen starke Gefühle mit einem solchen Kontrollverlust einher, aber seiner Meinung nach ist es ein Fehler, diese Gefühle mit einer Verletzung der Privatsphäre in Verbindung zu bringen. Wenn die Person ihr Tagebuch auf dem Tisch einer Fremden sieht, befürchtet sie, dass ihre Privatsphäre verletzt wurde, und das ist möglich. Allerdings wurde laut Macnish nur dann die Privatsphäre verletzt, wenn das Tagebuch tatsächlich geöffnet und gelesen wurde. In diesem Beispiel hat die fremde Café-Besucherin das Tagebuch auf ihren Tisch gelegt, ohne es zu lesen und hat aufgepasst, dass auch niemand anderes im Tagebuch liest. Das bedeutet aus der Sicht von Macnish, dass die Privatsphäre der Besitzerin des Tagebuchs nicht verletzt wurde.

583 Es gibt auch andere, viel beachtete Ansätze zur Definition von Privatsphäre, die hier nicht diskutiert werden, wie zum Beispiel den Ansatz der „contextual integrity“ von Nissenbaum. Ihrer Meinung nach ist die Privatsphäre intakt, solange der Informationsfluss mit den kontextspezifischen Informationsnormen übereinstimmt (Nissenbaum 2010:188; Barocas, Nissenbaum 2014:47). Allerdings erlauben die für alle gleichermaßen geltenden Informationsnormen keinen Raum für individuelle Intuitionen. So wird Nissenbaums Ansatz nicht den Tatsachen gerecht, dass es viele verschiedene Interpretationen dessen gibt, wann Informationen mit dem Kontext konsistent verwendet werden, und dass unterschiedliche Individuen unterschiedliche Verwendungen ihrer Daten bevorzugen (Rule 2019:274).

584 Macnish 2018:417f.

Macnish trennt Verletzung der Privatsphäre von anderen Schäden wie zum Beispiel der Verringerung der Sicherheit: „(...) there are other harms associated with privacy violations besides the loss of privacy.“⁵⁸⁵ In einer anderen Version des Tagebuchbeispiels hat die Fremde im Café das Tagebuch gelesen und erpresst die Person, der das Tagebuch gehört, indem sie mit einer Veröffentlichung der Inhalte droht. In diesem Fall wurde, auch nach Macnish's Verständnis, die Privatsphäre der Person verletzt, aber es gibt einen weiteren Schaden: Die Verringerung der Sicherheit der Person auf Grund ihrer Erpressung. In einer weiteren Version des Tagebuchbeispiels gibt die Fremde im Café nur vor, das Tagebuch gelesen zu haben, und versucht die Person zu erpressen, indem sie mit Veröffentlichung der Informationen droht. Hier würde Macnish behaupten, dass die Privatsphäre der Person unverletzt bleibt, aber der weitere Schaden an der Sicherheit der Person bleibt bestehen: „(...) it is the reduction in security that is the greater harm.“⁵⁸⁶ Er hält die Verletzung der Sicherheit sogar für größer als die (potenzielle) Verletzung der Privatsphäre.

Der Technologieethiker Björn Lundgren ist wie Macnish ein Vertreter des Zugangs-Ansatzes⁵⁸⁷ und meint, dass der Anspruch auf Privatsphäre auch einen Schutz vor bestimmten Risiken für die Privatsphäre umfasst: „(...) the right to privacy includes a right not to have others put one's privacy at substantial risk.“⁵⁸⁸ Da wir Menschen uns in einer Gesellschaft aber täglich gegenseitig Risiken aussetzen, kann nicht jedes Risiko für die Privatsphäre verboten sein. Deshalb kann dieser Anspruch auf Privatsphäre und Nicht-Risikoexposition auch außer Kraft gesetzt werden, wenn es zum Beispiel unvermeidbar oder notwendig ist, persönliche Informationen von anderen einzuholen.⁵⁸⁹ Verletzt wird die Privatsphäre von Individuen dann, wenn durch Außenstehende ihre Überzeugungen oder ihr Wissen über den Zugang zu ihren privaten Angelegenheiten erheblich beeinträchtigt werden.⁵⁹⁰

585 Macnish 2018:425

586 Ebd.:425

587 Lundgren 2020:172f.

588 Lundgren 2021b:385f.

589 Ebd.:384–387

590 Ebd.:390

Das heißt, laut Lundgren verletzen Außenstehende die Privatsphäre eines Individuums dann,

- wenn sie tatsächlich auf persönliche Informationen des Individuums zugreifen⁵⁹¹,
- wenn sie das Individuum einem substanziell größeren Risiko aussetzen, dass eine andere außenstehende Person auf seine persönlichen Informationen zugreift⁵⁹²,
- wenn sie dafür sorgen, dass das Individuum glaubt, dass seine privaten Angelegenheiten dem Risiko des Zugriffs durch eine andere außenstehende Person ausgesetzt sind⁵⁹³ oder
- wenn sie dafür sorgen, dass das Individuum unsicher ist, ob seine privaten Angelegenheiten dem Risiko des Zugriffs durch eine andere außenstehende Person ausgesetzt sind.⁵⁹⁴

An dieser Stelle stellt sich die Frage, wann genau es zu einem tatsächlichen Zugang zu persönlichen Daten kommt. Mainz und Uhrenfeldt sind der Meinung, dass ein tatsächlicher Zugang dann möglich ist, wenn eine außenstehende Person eine epistemische Beziehung zu der betreffenden Information aufgebaut hat.⁵⁹⁵ Macnish postuliert, dass die Privatsphäre nur dann beeinträchtigt ist, wenn diejenigen, die auf persönliche Informationen zugreifen, die Informationen verstehen können.⁵⁹⁶ Das heißt, wenn die Informationen im Tagebuch für die Fremde im Café gar nicht verständlich sind, weil sie zum Beispiel die Sprache nicht spricht, in welcher das Tagebuch verfasst ist, dann wird keine epistemische Beziehung zu der betreffenden Information aufgebaut und die Privatsphäre des Tagebuchbesitzers bleibt intakt.⁵⁹⁷ Die Datenethiker Lauritz Munch und Jakob Mainz sind aber der Meinung, dass für eine Verletzung der Privatsphäre neben der epistemisch begründeten Überzeugung in Bezug auf die persönlichen Informationen explizit auch eine Wahrnehmung der Information erfolgen muss⁵⁹⁸: „If no one forms

591 Macnish 2018:417f.; Lundgren 2021b:387

592 Lundgren 2021b:387

593 Ebd.:389

594 Ebd.

595 Mainz, Uhrenfeldt 2021:291f.

596 Macnish 2020; Asgarinia 2023:338

597 Munch, Mainz 2023:252f.

598 Ebd.:247f.

a warranted belief about A's personal matters, and no one perceives them, then A has full privacy."⁵⁹⁹ Die Autoren entwickeln folgendes Beispiel, um die Relevanz der Wahrnehmung einer Information zu unterstreichen: B benutzt ein Röntgengerät, um sich den Inhalt des Safes von A anzuschauen. Dadurch sieht B ein Nacktfoto von A, das in dem Safe aufbewahrt wird. B glaubt jedoch, dass er halluziniert und meint fälschlicherweise, dass er das Foto nicht richtig wahrnimmt.⁶⁰⁰ Laut Munch und Mainz wird hier die Privatsphäre verletzt, weil B den Inhalt von A's Safe wahrnimmt – unabhängig davon, dass B als Reaktion auf diese Wahrnehmungserfahrung weder eine Überzeugung bildet noch eine Rechtfertigung aus ihr gewinnt.⁶⁰¹

6.2.1.1 Argumente gegen den Zugangs-Ansatz

Munch und Mainz erklären, dass sie sich neben der Bildung begründeter Überzeugungen und der tatsächlichen Wahrnehmung keine weiteren Prozesse vorstellen können, welche die Privatsphäre auf plausible Weise beeinträchtigen.⁶⁰² Ich denke jedoch, ihr eigenes Beispiel zeigt eindrücklich, dass allein der Versuch, eine epistemische Beziehung zu der betreffenden Information aufzubauen, zu der einem nicht aktiv Zugang gewährt wurde, eine Verletzung der Privatsphäre darstellt. Denn ich denke, das Problem ist, dass B in den Safe von A schaut. Es geht nicht darum, was B wahrnimmt und woran er sich erinnert, sondern dass B überhaupt in den Safe von A schaut. Das Verhalten von B, sich Zugang zu verschaffen zu Informationen, die A offensichtlich nicht mit ihm teilen möchte, ist das Problem – das Umgehen von As Kontrolle über diese Informationen ist das, was ihre Privatsphäre verletzt. Ob B den Inhalt vom Safe wahrnimmt und sich auch darüber bewusst ist, dass er ihn wahrnimmt, ist unwichtig – selbst wenn der Safe leer wäre, hätte B durch diesen unerwünschten Zugriff As Privatsphäre verletzt.

Einerseits werden also durch den Zugangs-Ansatz *unerwünschte* Zugriffe nicht früh genug als Verletzung der Privatsphäre eingestuft

599 Munch, Mainz 2023:255

600 Ebd.:249

601 Ebd.:253

602 Ebd.:256

– es muss erst eine Wahrnehmungserfahrung geben⁶⁰³, eine epistemische Beziehung zur Information aufgebaut sein⁶⁰⁴, oder die Information verstanden werden⁶⁰⁵. Andererseits werden durch den Zugangs-Ansatz *erwünschte* Zugriffe zu früh als Verletzung der Privatsphäre eingestuft. So schreibt Asgarinia: „(...) this view implies that we lose our privacy when we freely and knowingly tell our friends about our problems and secrets.“⁶⁰⁶ Nach dem Zugangs-Ansatz wird unsere Privatsphäre immer dann beeinträchtigt, wenn ein anderer auf unsere persönlichen Daten zugreift, unabhängig davon, ob wir die Absicht haben, unsere persönlichen Daten mit einem anderen Akteur zu teilen. So wird es also auch als eine Verletzung der Privatsphäre eingestuft, wenn der Zugang durch das Individuum gewährt wurde. Aber laut der Philosophin Julie Inness und laut Menges können wir uns bewusst anderen Menschen mitteilen und andere in unseren Bereich der Privatsphäre einbeziehen, ohne unsere Privatsphäre zu beeinträchtigen.⁶⁰⁷

Nicht nur die Bestimmung dessen, wann die Privatsphäre verletzt ist, stößt auf Probleme. Auch die Bestimmung dessen, wann die Privatsphäre intakt ist, löst Schwierigkeiten aus. Laut Munch und Mainz ist die Privatsphäre einer Person intakt, wenn sich niemand eine begründete Meinung über ihre persönlichen Angelegenheiten bildet und niemand diese wahrnimmt.⁶⁰⁸ Das heißt, die Privatsphäre ist intakt, wenn niemand Zugang zu den Informationen des Individuums hat und dementsprechend Außenstehende nicht auf Informationen über das Individuum zugreifen. Wie in Tabelle 1 deutlich wird, erinnert diese Definition von Privatsphäre an das Recht in Ruhe gelassen zu werden aus Teilkapitel 6.1.⁶⁰⁹ Das Problem bei dieser Definition von Privatsphäre als reine Abgeschiedenheit ist, dass sie zu weit gefasst ist, denn sie suggeriert, dass jedes Mal, wenn eine Person mit der Gesellschaft in Kontakt kommt, ihre Privatsphäre beeinträchtigt wird.⁶¹⁰

603 Munch, Mainz 2023:253

604 Mainz, Uhrenfeldt 2021:291f.

605 Munch, Mainz 2023:252f.

606 Asgarinia 2023:338

607 Inness 1992:46; Menges 2022:702f.

608 Munch, Mainz 2023:255

609 Cooley 1879:29; Warren, Brandeis 1890:195

610 Parent 1983b:342

Tabelle 1 Teile der Privatsphäre nach dem Zugangsansatz⁶¹¹

Zugangs-Ansatz	Individuum	Außenstehende
Privatsphäre intakt	Niemand bildet sich eine begründete Meinung über die persönlichen Angelegenheiten des Individuums und niemand nimmt sie wahr. ^{612*}	Außenstehende haben keinen Zugang zu den Informationen des Individuums, bilden sich keine begründete Meinung über seine persönlichen Angelegenheiten und nehmen diese auch nicht wahr. ^{613*}
Privatsphäre verletzt	Jemand hat Zugang zu den Informationen des Individuums, bildet sich eine begründete Meinung über die persönlichen Angelegenheiten des Individuums und nimmt sie wahr. ^{614*}	Außenstehende greifen tatsächlich auf persönliche Informationen des Individuums zu. ⁶¹⁵ ODER Außenstehende sorgen dafür, dass das Individuum einem substanziell größeren Risiko ausgesetzt ist, dass eine andere außenstehende Person auf seine persönlichen Informationen zugreift. ⁶¹⁶ ODER Außenstehende sorgen dafür, dass das Individuum glaubt, dass ODER unsicher ist, ob seine privaten Angelegenheiten dem Risiko des Zugriffs durch eine andere außenstehende Person ausgesetzt sind. ⁶¹⁷
* Erinnert an das Recht in Ruhe gelassen zu werden. ⁶¹⁸		

Das führt zu Schwierigkeiten mit den von mir aufgestellten Kriterien für eine Definition von Privatsphäre. Denn mit Hilfe des Zugangs-Ansatzes werden *unerwünschte* Zugriffe nicht früh genug und *erwünschte* Zugriffe zu früh als Verletzung der Privatsphäre eingestuft. Auch die Bestimmung, wann die Privatsphäre intakt ist, führt den Zugangs-Ansatz zu der Annahme, dass jede Wahrnehmungserfahrung eine Gefahr darstellt – dann wäre es beim gesellschaftlichen

611 Eigene Darstellung

612 Munch, Mainz 2023:255

613 Ebd.

614 Ebd.

615 Macnish 2018:417f.; Lundgren 2021b:387

616 Lundgren 2021b:387

617 Ebd.:389

618 Cooley 1879:29; Warren, Brandeis 1890:195

Zusammenleben jedoch sehr schwer eine intakte Privatsphäre zu erhalten. Insbesondere durch die Einstufung erwünschter Zugriffe als Verletzungen der Privatsphäre bietet der Zugangs-Ansatz keinen Raum für individuelle Intuitionen und das Ausleben der Privatsphäre nach den eigenen Vorstellungen.

Um das letztere Problem zu lösen schlägt Asgarinia eine Revision des Zugangs-Ansatzes vor: „A’s privacy is lost iff: B actually accesses personal information P about A, and A intends that P remain private, or, B has reason to think that A intends to keep it private.“⁶¹⁹ Nur wenn eine Person ihre persönlichen Informationen gerne für sich behalten würde, stellt der Zugang zu diesen Informationen eine Verletzung ihrer Privatsphäre dar. Diese Intention, die Informationen für sich zu behalten, kann entweder konkret geäußert werden, oder die Außenstehenden können diese antizipieren. Bei einem Tagebuch kann man sich zum Beispiel denken, dass der gesamte Inhalt privat bleiben soll. Im Allgemeinen gibt es viele Situationen, in denen der Zugang zu Informationen ausschließlich zu einem bestimmten Zweck gewährt wird. So zum Beispiel, wenn man seine Bankdaten bei einem Online-Einkauf angibt – da sollen die Informationen nur dazu benutzt werden, um den Einkauf abzuwickeln, aber nicht für andere Zwecke. Diese Form des Zugangs-Ansatzes plädiert also für zweckgebundene Verarbeitung von persönlichen Informationen – immer mit Rücksicht auf die Intention des Individuums.

Asgarinias Revision schärft die Bestimmung dessen, wann die Privatsphäre verletzt wird – nämlich dann, wenn jemand tatsächlich Zugang zu Informationen über eine Person hat, obwohl die Person die Information geheim halten wollte. Mainz und Uhrenfeld kritisieren Asgarinias Revision, denn sie meinen die Unerwünschtheit des Zugangs könne keine notwendige Bedingung sein für die Verletzung der Privatsphäre, da es Fälle geben kann, in denen die Privatsphäre durch einen Zugang verletzt wird, der durch die verletzte Person gewollt ist.⁶²⁰ Man kann eine Privatsphärenverletzung wollen, wenn man sich zum Beispiel heimlich wünscht, dass man belauscht wird, während man eine Entschuldigung ausspricht, damit man die Ent-

619 Asgarinia 2023:340; Kursive Betonung entfernt

620 Man kann eine Privatsphärenverletzung wollen, wenn man sich zum Beispiel heimlich wünscht, dass man belauscht wird, während man eine Entschuldigung ausspricht, damit man die Entschuldigung nicht nochmal vortragen muss (Mainz, Uhrenfeldt 2021:297).

schuldigung nicht nochmal vortragen muss. Laut Mainz und Uhrenfeldt bleibt das Belauschen aber trotz Wunsch der sprechenden Person eine Verletzung der Privatsphäre. Das heißt, die Privatsphäre kann auch verletzt werden, wenn jemand tatsächlich Zugang zu Informationen über eine Person hat und die Person sich das heimlich gewünscht hat.

Asgarinas Revision gibt trotzdem einen interessanten Hinweis, da sie im Umkehrschluss klarer macht, wann die Privatsphäre intakt ist; nämlich dann, wenn niemand Zugang hat oder die Person ihre Informationen nicht geheim halten will und deshalb Zugang gewährt. Damit bietet Asgarinas Revision Raum für individuelle Intuitionen, in Form von zum Beispiel dem Bedürfnis guten Freunden Zugriff auf die eigenen Informationen zu gewähren. Diese Möglichkeit aktiv Zugang zu gewähren, erinnert an den Kontroll-Ansatz, der im Folgenden vorgestellt wird.

6.2.2 Kontroll-Ansatz

Beim Kontroll-Ansatz stellt die selektive Offenlegung den Kern der Privatsphäre dar.⁶²¹ Viele Autor:innen definieren Privatsphäre in dem Zuge als Möglichkeit zur Kontrolle.⁶²² Laut Fried ist Privatsphäre die Kontrolle über das Wissen über die eigene Person. Das heißt, eine Person, die Privatsphäre genießt, ist in der Lage, anderen den Zugang zu Wissen über sich selbst zu gewähren oder zu verweigern. Dabei gelte nicht, dass wir umso mehr Privatsphäre haben, je weniger über uns bekannt ist: „Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.”⁶²³ Hierbei gehe es nicht nur um die Kontrolle der Quantität der Informationen, sondern auch um die Qualität des Wissens: „We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details.”⁶²⁴ Auch Rössler definiert etwas als privat, wenn man selbst den Zugriff auf dieses „Etwas“ kontrollieren kann: „(...)

621 Parent 1983b:343

622 Westin 1967; Fried 1968, Rachels 1975, Inness 1992, Rössler 2004; Moore 2010

623 Fried 1970:140; Fried 1968:209

624 Fried 1968:210

the protection of privacy means protection against unwanted access by other people.“⁶²⁵ Ist die Privatsphäre einer Person geschützt, so ist die Person geschützt vor einem unerwünschten Zugriff durch andere Personen. Es handelt sich hierbei um den Schutz vor Einspruchs- oder Rückschlussmöglichkeiten anderer, wenn es um bestimmte private Entscheidungen, Handlungen, Verhaltensweisen oder Lebensweisen geht.⁶²⁶

Moore definiert das Recht auf Privatsphäre als Recht zur Kontrolle über Zugang zu und Benutzung von persönlichen Informationen.⁶²⁷ Er meint, die Privatsphäre ist dann intakt, wenn eine Person sich freiwillig von ihren Mitmenschen abgrenzt und den Zugang einschränkt. Selbst wenn der Zugang möglich ist, folgt daraus nicht zwangsläufig, dass alle nachfolgenden Verwendungen der durch diesen Zugang erlangten Informationen ebenfalls zulässig sind.⁶²⁸ Deshalb legt Moore Wert darauf, dass Privatsphäre nicht nur Kontrolle über den Zugang zu persönlichen Informationen ermöglicht, sondern auch Kontrolle über die Benutzung der zugänglich gemachten Informationen. Ein Fallbeispiel macht den Effekt der ergänzten Benutzung von Informationen deutlich: Jones hört zufällig mit, als Smith seinem Freund erzählt, dass er geschieden ist, und spricht mit anderen Freunden darüber.⁶²⁹ Jones bekommt zufällig Zugang zu der Information über die Scheidung und man kann nicht von Jones erwarten, dass er sich die Ohren zuhält, wenn er sich in der Nähe von privaten Gesprächen befindet. Aber die Verwendung der mitgehörten Information in Gesprächen mit Freunden verletzt Smith's Privatsphäre. Nur weil Jones Zugang zu den Informationen bekommen hat, bedeutet das nicht, dass er die fraglichen Informationen nutzen oder verbreiten darf.⁶³⁰

Acquisti et al. definieren informationelle Privatsphäre folgendermaßen: „(...) privacy as the selective, self-interested opening and

625 Rössler 2004:8

626 Ebd.:8f.

627 Moore bezieht sich auch auf Orte und Körper, aber diese Dimensionen sind hier nicht relevant, da es in dieser Arbeit ausschließlich um informationelle Privatsphäre geht (Moore 2010:27).

628 Moore 2010:28

629 Rachels 1975:333; Moore 2010:30

630 Moore 2010:31

closing of the self to others.“⁶³¹ Es geht ihrer Meinung nach nicht nur um den Rückzug und das Verstecken der eigenen Informationen, sondern auch um das selektive Öffnen vor anderen aus Eigeninteresse. Acquisti et al. erklären unsere Fähigkeit zu entscheiden, wann wir uns öffnen und wann verschließen, mit Hilfe eines evolutionären Ansatzes. Denn ursprünglich ging es darum, die Anwesenheit anderer Menschen wahrzunehmen und angemessen darauf zu reagieren. Diese Fähigkeit, „sensorial cues“ richtig zu interpretieren, kann Menschen vor Risiken schützen und ihnen Vorteile bringen. So kann ein Individuum seine Interessen und Präferenzen mit einem „marketer“ teilen, um passende Kaufangebote zu bekommen (Vorteil) und gleichzeitig verheimlichen, wieviel es bereit ist dafür zu zahlen, um Preisdiskriminierung zu vermeiden (Schutz vor Risiken).⁶³²

Die Privatsphäre einer Person kann laut Mainz und Uhrenfeldt nur dann verletzt werden, wenn der Verlust der Kontrolle über ihre Informationen auf die Handlung(en) eines anderen Akteurs zurückzuführen ist. Denn wenn man zum Beispiel sein Tagebuch im Café liegen lässt, wurde einem die Kontrolle über die Informationen darin nicht durch andere verwehrt, solange es nicht gelesen wird.⁶³³ Daraus ergibt sich der folgende Kontroll-Ansatz: „For any agent A to have her right to privacy violated, there is a necessary and sufficient condition that must be satisfied: Agent A has involuntarily lost Negative Control over the access to personal information P about agent A, *due to action(s) of agent B, of which B is responsible.*“⁶³⁴ Die Privatsphäre einer Person ist also nur dann verletzt, wenn sie unfreiwillig die Negative Kontrolle⁶³⁵ über den Zugang zu persönlichen Informationen über sich verloren hat, und zwar aufgrund von Handlungen eines anderen Akteurs, für die dieser Akteur auch verantwortlich ist.

Nach dem Kontroll-Ansatz ist die Privatsphäre einer Person intakt, wenn sie den Zugang zu Informationen über sich gewähren

631 Acquisti et al. 2022:270

632 Ebd.

633 Mainz, Uhrenfeldt 2021:298

634 Ebd.:298; Die Autoren formulieren auch den Zugangs-Ansatz auf die Weise um, aber werfen ihn auf Grund eines Gegenbeispiels.

635 Negative Kontrolle bezeichnet die Möglichkeit andere am Zugang zu den eigenen Informationen zu hindern (Mainz, Uhrenfeldt 2021:293). Was genau damit gemeint ist, wird im folgenden Teilkapitel unter 6.2.2.1 erklärt.

oder verweigern kann, indem sie Kontrolle über den Zugang zu und die Benutzung von den eigenen Informationen hat. Verletzt wird die Privatsphäre der Person hingegen dann, wenn sie die Kontrolle über den Zugang zu ihren Informationen aufgrund von Handlungen eines anderen Akteurs verloren hat. Somit ermöglicht es diese Definition von Privatsphäre nach dem Kontroll-Ansatz zu bestimmen, wann Privatsphäre intakt und wann verletzt ist. Außerdem lässt sich Raum für individuelle Intuitionen, weil der Zugang zu den Informationen selbstständig gewährt oder verweigert werden kann. Um genauer zu verstehen, was mit Kontrolle gemeint ist, werden im Folgenden verschiedene Definitionen von Kontrolle vorgestellt und diskutiert.

6.2.2.1 Definition von Kontrolle

Mainz und Uhrenfeldt unterscheiden zwischen Positiver, Negativer und Republikanischer Kontrolle: Positive Kontrolle über den Zugang zu relevanten Informationen hat man dann, wenn man versucht oder versuchen könnte, jemand anderem tatsächlichen Zugang zu den Informationen zu gewähren und dies gelingt. Negative Kontrolle über den Zugang zu relevanten Informationen hat man hingegen dann, wenn man in der Lage ist, jemand anderen, der versucht, sich Zugang zu verschaffen, am Zugang zu den Informationen zu hindern.⁶³⁶ Und Republikanische Kontrolle über den Zugang zu relevanten Informationen hat man dann, wenn andere gar nicht erst die Möglichkeit haben, Zugang zu persönlichen Informationen zu erhalten.⁶³⁷

Republikanische Kontrolle

Das Problem der Republikanischen Kontrolle ist ihre Strenge. Denn sie führt zu der Annahme, dass die Privatsphäre nur dann intakt ist, wenn andere gar nicht erst die Möglichkeit haben, Zugang zu persönlichen Informationen zu erhalten. Das würde allerdings bedeuten, dass die Privatsphäre auch verletzt wird, wenn man anderen Zugang zu den eigenen Informationen gewährt. Dadurch würde eine Definition der Privatsphäre als Republikanische Kontrolle über

636 Mainz, Uhrenfeldt 2021:293

637 Ebd.

Zugang zu und Benutzung von den eigenen Informationen keinen Raum lassen für individuelle Intuitionen und dementsprechend eins meiner Kriterien nicht erfüllen.

Positive Kontrolle

Laut Mainz und Uhrenfeldt hat man dann Positive Kontrolle über den Zugang zu relevanten Informationen, wenn man versucht (oder versuchen könnte), jemand anderem tatsächlichen Zugang zu den Informationen zu gewähren und dies gelingt.⁶³⁸ Sie verdeutlichen die Bedeutung der Positiven Kontrolle durch das „Too much info“ Beispiel: Smith erzählt seinem Kollegen Jones persönliche Details über sein Sexleben, aber Jones hält sich die Ohren zu und hört die Informationen nicht. Wenn man Kontrolle als Positive Kontrolle interpretiert, hat Jones das Recht von Smith auf Privatsphäre verletzt, indem er seine Ohren zuhält, da Smith dadurch die Positive Kontrolle über den Zugang zu den Informationen verliert.⁶³⁹ Deshalb verwerfen Mainz und Uhrenfeldt die Positive Kontrolle und auch ich behaupte, dass das Gelingen des Teilens von Informationen keine Bedingung für das Bestehen der Privatsphäre sein kann.

Positive Kontrolle ist trotzdem wichtig, weil man ohne das Gelingen des Teilens von Informationen zum Beispiel keinen Wohngeldantrag stellen könnte. Allerdings hat das dann nichts mehr mit der Privatsphäre der Informationen teilenden Person zu tun, sondern mit erfolgreicher Kommunikation, welche notwendig ist, um bestimmte Zwecke zu erreichen. In Bezug auf die Privatsphäre bedeutet die Möglichkeit Zugang zu gewähren, dass ich Informationen teilen darf, aber das bedeutet nicht, dass ich bestimmen kann, ob die Informationen auch bei dem vorgesehenen Empfänger ankommen.

Negative Kontrolle

Laut Mainz und Uhrenfeldt kann nur der Verlust der Negativen Kontrolle plausibel die Privatsphäre verletzen.⁶⁴⁰ Man hat Negative Kontrolle, wenn man andere am Zugang zu seinen Informationen hindern kann – wichtig ist den Autoren dabei, dass auch wirklich jemand anderes versucht sich Zugang zu den Informationen zu

638 Mainz, Uhrenfeldt 2021:293

639 Ebd.:294

640 Ebd.

verschaffen. Das gilt auch für die Verletzung der Privatsphäre: „In order for Negative Control to be lost, someone must *attempt* to get access (...).“⁶⁴¹ Menges argumentiert hingegen, dass die Fähigkeit, andere am Zugang zu hindern, durchaus verringert werden kann, ohne dass jemand überhaupt versucht, Zugang zu erhalten. Wenn man zum Beispiel betäubt ist durch K.O.-Tropfen, ist man nicht in der Lage, andere am Zugang zu hindern und einen zu berühren. Unabhängig davon, ob jemand versucht, tatsächlich Zugang zu bekommen und einen zu berühren, ist man nicht in der Lage dazu, den Zugang zu verhindern: „(...) they lack negative control over whether others touch them even if others do not attempt to touch them.“⁶⁴² In diesem Fall stimmt es also nicht, dass jemand versuchen muss, tatsächlich Zugang zu bekommen, damit die betroffene Person die negative Kontrolle verliert.

Ich denke jedoch man muss sich hier die Frage stellen, warum die betroffene Person nicht in der Lage ist, andere am Zugang zu hindern, und somit die Negative Kontrolle verloren hat: die K.O.-Tropfen sind der Grund. Deshalb behaupte ich Mainz und Uhrenfeldt würden auf Menges Einwand erwidern, dass es darauf ankommt, ob man sich selber mit K.O.-Tropfen betäubt hat oder ob sie einem von jemand anderem verabreicht wurden. Im letzteren Fall hätte die betäubte Person unfreiwillig die Negative Kontrolle über den Zugang zu den eigenen Informationen verloren, und zwar aufgrund von Handlungen einer anderen Person. Allein das Betäuben der Person könnte dann schon als versuchter Zugang gewertet werden.⁶⁴³ Denn dem negativen Kontroll-Ansatz von Mainz und Uhrenfeldt zufolge ist die Privatsphäre einer Person nur dann verletzt, wenn sie unfreiwillig die negative Kontrolle über den Zugang zu persönlichen Informationen über sich verloren hat, und zwar aufgrund von Handlungen eines anderen Akteurs, für die dieser Akteur auch verantwortlich ist.⁶⁴⁴

641 Mainz, Uhrenfeldt 2021:300

642 Menges 2022:701f.

643 Das Betäuben einer Person durch die Verabreichung von K.O.-Tropfen verletzt diese Person natürlich auch in anderer Hinsicht, zum Beispiel als Körperverletzung. Aber es ist unter anderem auch die Privatsphäre betroffen.

644 Mainz, Uhrenfeldt 2021:298

Für meine Kriterien heißt das, dass man mit einer Definition von Privatsphäre als Negative Kontrolle über Zugang zu und Benutzung von persönlichen Informationen bestimmen könnte, wann Privatsphäre intakt und wann verletzt ist. Denn die Privatsphäre einer Person ist demnach intakt, solange die Person in der Lage ist, jemand anderen, der versucht, sich Zugang zu verschaffen, am Zugang zu den Informationen zu hindern.⁶⁴⁵ Und die Privatsphäre einer Person ist verletzt, sobald die Person einen Zugangsversuch aufgrund von Handlungen anderer Akteure nicht verhindern kann.⁶⁴⁶ Diese Definition versperrt im Prinzip nicht den Raum für individuelle Intuitionen, da die Person sich Freunden mitteilen könnte – das scheint keinen Einfluss auf die Privatsphäre zu haben. Dadurch, dass die Privatsphäre als Negative Kontrolle definiert wird, ist allerdings das aktive Teilen von Informationen auch kein Teil der Privatsphäre.

6.2.2.2 Wahl-Kontrolle

Um einen Kompromiss zu finden zwischen dem positiven Gewähren von Zugang und dem negativen Verhindern von Zugang, definiere ich Kontrolle als die Möglichkeit zur Wahl: Das Individuum hat die Kontrolle darüber, mit wem es welche Informationen zu welchem Zweck teilt. Mit der Bezeichnung „Wahl-Kontrolle“ orientiere ich mich an dem Control-as-Choice view aus der Literatur, welcher laut Menges impliziert, dass Privatsphäre die Wahl ermöglicht, ob andere Zugang haben oder nicht. Die Vertreter:innen des Kontroll-Ansatzes behaupten laut Menges, dass Privatsphäre im Wesentlichen eine Wahl zwischen Optionen beinhaltet.⁶⁴⁷ Dementsprechend stützt sich die Wahl-Kontrolle aus meiner Sicht weder auf rein Positive oder Negative Kontrolle, noch auf Republikanische Kontrolle.⁶⁴⁸ Vielmehr vereint sie die Positive und Negative Kontrolle, weil Wahl-Kontrolle bedeutet, dass man in jeder Situation wählen kann, ob man Zugang gewähren oder verhindern möchte.

Ein ähnliches Verständnis von Kontrolle ist das, was Menges „leeway control“ (Spielraumkontrolle) nennt: „(...) the ability to

645 Mainz, Uhrenfeldt 2021:293

646 Ebd.:298

647 Menges 2022:693ff.

648 Mainz, Uhrenfeldt 2021:293

do otherwise (...).“⁶⁴⁹ Dem Begriff der Spielraumkontrolle zufolge beinhaltet der Schutz der Privatsphäre die Möglichkeit, selbst zu entscheiden, ob andere von bestimmten Informationen erfahren oder Zugang zu ihnen haben sollen oder nicht.⁶⁵⁰ Der Begriff der Spielraumkontrolle unterscheidet sich von dem Begriff der Wahl-Kontrolle in zwei Punkten: Erstens geht es bei der Wahl-Kontrolle nicht darum, dass man Kontrolle darüber hat, was andere erfahren – denn hier ist nicht rein Positive Kontrolle gemeint. Vielmehr geht es darum, welche Informationen man bereit ist mit wem zu teilen und zu welchem Zweck. Deshalb ist zweitens die Benutzung der Informationen aus Moores Definition von Privatsphäre wichtig für den Begriff der Wahl-Kontrolle: Nur weil man Zugang zu gewissen Informationen gewährt bekommen hat, heißt das nicht, dass man sie zu jedem Zweck benutzen kann.⁶⁵¹

Bei der Definition von Privatsphäre orientiere ich mich an dem Kontroll-Ansatz von Moore: „A right to privacy is a right to control access to, and uses of (...) personal information.“⁶⁵² Da in dieser Arbeit davon ausgegangen wird, dass ein solches moralisches Recht auf Privatsphäre nur aus einer Pflicht zum Schutz der Privatsphäre resultieren könnte⁶⁵³ und diese Pflicht erst unter 6.3 begründet wird, möchte ich den Begriff des Rechts umgehen – auch um klarer über den Begriff der Privatsphäre sprechen zu können. Nun lässt sich aber das „Recht“ nicht einfach aus der Definition von Moore rausstreichen. Aus meiner Sicht lässt sich die Formulierung aber übersetzen in: Wer Privatsphäre hat, hat Kontrolle über Zugang zu und Benutzung von persönlichen Informationen. Moore selbst scheint Kontrolle als negative Kontrolle zu interpretieren, denn seiner Meinung nach ist der Zustand der Privatsphäre gegeben, wenn eine Person sich freiwillig von ihren Mitmenschen abgrenzt und den Zugang zu ihren persönlichen Informationen einschränkt.⁶⁵⁴ Ich möchte jedoch dieses negative Verständnis von Kontrolle ersetzen durch das Verständnis von Kontrolle als Wahl darüber, mit wem man welche Informationen zu welchem Zweck teilt.

649 Menges 2020a:34

650 Ebd.:45

651 Moore 2010:28

652 Ebd.:27

653 Mohr 2010:77

654 Mainz, Uhrenfeldt 2021:294; Moore 2010:26

Intakte Privatsphäre

Nach dieser Definition ist die Privatsphäre einer Person intakt, wenn sie wählen kann, wem sie Zugang zu welchen Informationen gewährt oder verweigert, und wenn sie zudem wählen kann, zu welchem Zweck ihre Informationen benutzt werden. Bei dieser Wahl kann der Kontext des Informationsflusses eine wichtige Rolle spielen. Beispielsweise berichtet ein Individuum seiner Ärztin Details über seinen Gesundheitszustand, die es selbst mit guten Freunden nicht teilen würde. Dafür erzählt das Individuum guten Freunden von einem Streit, von dem es wiederum seine Ärztin nicht in Kenntnis setzen würde. Was die Person mit wem teilt und zu welchem Zweck ist aber nicht wie bei der Technologiephilosophin Helen Nissenbaum⁶⁵⁵ an Informationsnormen gebunden, sondern erfolgt nach individueller Intuition – im besten Fall gekoppelt mit Wissen über die Konsequenzen.

Nicht immer sind sich die betroffenen Individuen allen Konsequenzen bewusst. So kann zum Beispiel beim Gewähren des Zugangs zu Informationen die Wahl-Kontrolle vermindert sein durch zum Beispiel Drogen, psychische Probleme oder Unwissenheit. Wenn diese verminderte Kontrolle ausgeübt wird, wird dadurch auch die Privatsphäre vermindert.⁶⁵⁶ Aber bei unverminderter Kontrolle bedeutet das Preisgeben von persönlichen Informationen nicht, dass dadurch die Privatsphäre aufgegeben wurde. So schreibt Menges: „(...) we can share private information with a good friend without giving up privacy.“⁶⁵⁷ Wenn wir uns bewusst anderen Menschen mitteilen, beziehen wir die Anderen in unseren Bereich der Privatsphäre ein, ohne unsere Privatsphäre zu beeinträchtigen.⁶⁵⁸

Es gibt Kritiker, die einwenden, dass die Kontrolle allein nicht die Privatsphäre ausmacht – es müsse auch um einen Grad der Abgeschiedenheit gehen.⁶⁵⁹ Wenn eine Person, wie im *Voluntary Divulgence Case* unter 6.1, Fremden von ihren Problemen erzählt, hat sie Zugang zu ihren Informationen gewährt und man kann nicht davon sprechen, dass sie dadurch ihre Abgeschiedenheit för-

655 Nissenbaum 2010:188

656 Menges 2022:702

657 Ebd.:702f.

658 Inness 1992:46

659 Masur et al. 2018:5f.

dert. Angenommen, sie hat sich bewusst dazu entschieden, diese Informationen zu teilen, so hat sie ihre Wahl-Kontrolle über den Zugang zu diesen Informationen ausgeübt. Sie hat sich nicht für den Rückzug entschieden, sondern kontrolliert ihre Informationen geteilt. Das heißt aber nicht, dass sich die Person auch zukünftig dafür entscheiden wird, ihre Probleme mit Fremden zu teilen. Die Entscheidung, Informationen kontrolliert zu teilen, hebt nicht die Möglichkeit zum Rückzug auf. Die Person hat durch das einmalige Teilen ihrer privaten Informationen ihre Privatsphäre nicht verletzt – sie wurde nur temporär ausgeweitet. Nach der Ansicht des Psychologen Irwin Altman schwankt das gewünschte Maß an Privatsphäre je nach Situation und Interaktion, deshalb passen die Menschen ihre eigenen Grenzen immer wieder an.⁶⁶⁰

Hier kommt jedoch eine zeitliche Dimension hinzu: Während eine Person freiwillig und nüchtern fremden Menschen von ihren persönlichen Problemen und dem regelmäßigen Alkoholkonsum erzählt, hat sie die Wahl-Kontrolle über diese Informationen. Aber sobald die fremden Menschen über die persönlichen Informationen verfügen, können die Fremden die Informationen weiterverbreiten und die erzählende Person verliert die Kontrolle darüber, was mit ihren Informationen in Zukunft passiert. Der Gedanke findet sich auch bei Menges: „(...) exercising full control by telling strangers about personal information can and often does threaten our future privacy with regard to the information.“⁶⁶¹ Wenn die erzählende Person den Fremden Zugang zu Informationen über ihre persönlichen Probleme gewährt, stimmt sie dadurch nicht automatisch zu, dass die Fremden ihre Informationen benutzen dürfen, indem diese sie zum Beispiel weiterverbreiten. Nach dem Gewähren des Zugangs zu Informationen ist es jedoch möglich, dass die Informationen benutzt werden – dessen sollte man sich beim Teilen der Informationen bewusst sein.

Verletzung der Privatsphäre

Die Privatsphäre einer Person wird verletzt, wenn sie nicht mehr wählen kann, wem sie Zugang zu welchen Informationen gewährt oder verweigert, oder wenn sie nicht mehr wählen kann, zu wel-

660 Altman 1976:13f.; Dienlin 2014:107

661 Menges 2022:703

chem Zweck ihre Informationen benutzt werden. Ich stimme Mainz und Uhrenfeldt zu und argumentiere, dass für diese eingeschränkte oder fehlende Wahl-Kontrolle immer Außenstehende verantwortlich sein müssen, da man seine Privatsphäre nicht selbst verletzen kann.⁶⁶² Eine Person kann Drogen konsumieren und dadurch ihre Möglichkeit zur Wahl-Kontrolle selber einschränken – denn man kann womöglich im berauschten Zustand nicht mehr so wählen, wie man das im nüchternen Zustand tun würde und könnte sich im Nachhinein für das bereitwillige Gewähren von Zugang zu den eigenen Informationen schämen. Solange sich die Person aber freiwillig für das Konsumieren der Drogen entschieden hat und sich der Konsequenzen bewusst war, hat sie im Vorhinein ihre Kontrolle über ihren eigenen Bewusstseinszustand ausgeübt.

Ob die Privatsphäre des Individuums verletzt wird, hängt dementsprechend vom Verhalten der Außenstehenden ab. Außenstehende können die Privatsphäre eines Individuums verletzen, indem sie entweder *bewusst* versuchen auf persönliche Informationen des Individuums zuzugreifen oder diese zu benutzen, ohne dass das Individuum darüber die Wahl-Kontrolle hat, oder Außenstehende greifen tatsächlich, womöglich auch *aus Versehen*, auf persönliche Informationen des Individuums zu oder benutzen diese, ohne dass das Individuum darüber die Wahl-Kontrolle hat.

Ein tatsächlicher, aber unbeabsichtigter Zugriff ohne die Kontrolle des Individuums lässt sich durch folgendes Beispiel beschreiben: Ein Kind benutzt eine öffentliche Toilette und schließt die Tür nicht ab, weil es Sorge hat, das Schloss alleine nicht wieder öffnen zu können. Eine weitere Toilettennutzerin öffnet die Tür, in der Annahme, dass die Toilette nicht besetzt ist. Die Toilettennutzerin sieht das Kind, entschuldigt sich und schließt die Tür schnell wieder. Sie verletzt in dem Fall die Privatsphäre des Kindes, weil sie aus Versehen auf persönliche Informationen des Kindes zugreift. Das Kind ist dieses Risiko eingegangen, als es die Tür nicht abgeschlossen hat. Es hat also bewusst etwas von seiner Wahl-Kontrolle über den Zugang zu und die Benutzung von persönlichen Informationen aufgegeben, weil es das Abschließen vermeiden wollte. So kann es manchmal bei einer Abwägung von möglichen Risiken dazu kommen, dass der Schutz der Privatsphäre nicht die oberste Priorität hat. Das Indivi-

662 Mainz, Uhrenfeldt 2021:298

duum kann sich jederzeit dafür entscheiden, etwas Kontrolle über den Zugang zu und die Benutzung von persönlichen Informationen abzugeben und zu riskieren, dass Außenstehende dann tatsächlich auf persönliche Informationen des Individuums zugreifen. So ein tatsächlicher, aber unbeabsichtigter Zugriff auf persönliche Informationen sollte im Datenökosystem nicht möglich sein, weil die Daten so gespeichert sein sollten, dass niemand zufällig darauf stoßen kann.

Eine tatsächliche Benutzung persönlicher Informationen ohne die Kontrolle des Individuums passiert zum Beispiel dann, wenn Menschen, denen man sich anvertraut, das Anvertraute weitergeben. Das Weitergeben der Informationen verletzt die Privatsphäre, weil die ursprüngliche Quelle der Informationen dann keine Wahl-Kontrolle über Zugang zu und Benutzung von ihren persönlichen Informationen mehr hat. Das heißt, solange man nicht gebeten wurde, persönliche Informationen von anderen weiterzugeben, stellt das eine Verletzung der Privatsphäre dieser anderen Personen dar. Hier lässt sich eine klare Parallele zu der Zweckentfremdung von personenbezogenen Daten erkennen. Die Wahl-Kontrolle des betroffenen Individuums ist nur intakt, wenn die Daten ausschließlich für vereinbarte Zwecke verwendet werden.

Der Versuch des Zugriffs auf oder der Benutzung von persönlichen Informationen lässt sich durch das Abhörbeispiel illustrieren: Wenn jemand das Telefon eines anderen abhört, aber keine Informationen bekommt, beeinträchtigt er trotzdem allein durch seinen Versuch die Privatsphäre des anderen.⁶⁶³ Übertragen auf das Datenökosystem bedeutet dies, dass allein der Versuch, auf Daten zuzugreifen, ohne dass das betroffene Individuum darüber die Kontrolle hat, die Privatsphäre des Individuums verletzt.

Fahrlässigkeit und Beihilfe

Wie unter 6.2.1 dargestellt, verletzen laut Lundgren Außenstehende die Privatsphäre eines Individuums außerdem dann, wenn sie das Individuum einem substanziell größeren Risiko aussetzen, dass eine andere außenstehende Person auf seine persönlichen Informationen zugreift.⁶⁶⁴ Wenn zum Beispiel ein Arzt während der Behandlung die

663 Mainz, Uhrenfeldt 2021:299

664 Lundgren 2021b:387

Tür des Behandlungszimmers offenstehen lässt, ist das Risiko substantiell größer, dass eine andere außenstehende Person vorbeiläuft, hineinschaut und (womöglich auch aus Versehen) auf persönliche Informationen der Patient:innen zugreift. Der Arzt könnte die Tür des Behandlungszimmers absichtlich offenstehen lassen, um das Risiko zu erhöhen, dass jemand Unbefugtes hineinschaut. Allerdings würde ich ein solches Fehlverhalten keinem Arzt unterstellen wollen. Trotzdem kann die Situation entstehen durch fahrlässiges Handeln, weil die Tür zum Beispiel aus Eile nicht vollständig geschlossen wurde. Eine solche fahrlässige Handlung bezeichne ich als Beihilfe zur Privatsphärenverletzung und stimme Lundgren damit zu, dass der Anspruch auf Privatsphäre auch einen Schutz vor bestimmten Risiken für die Privatsphäre umfasst.⁶⁶⁵ Das heißt im Kontext von Datenökosystemen, dass Datengenerierende aus ethischer Sicht nicht fahrlässig mit den Daten der Datenquellen umgehen sollten.

Lundgren hat diese Spezifikation der Privatsphärenverletzung zwar aus Sicht des Zugangs-Ansatzes aufgestellt, aber ich argumentiere, dass sie sich auf die Sicht des Kontroll-Ansatzes übertragen lässt. Denn auch aus Sicht des Kontroll-Ansatzes kann der tatsächliche Zugang zu persönlichen Informationen problematisch sein – das läge dann allerdings nicht an dem Zugang selbst, sondern an der fehlenden Kontrolle über den Zugang. Ein Individuum einem substantiell größeren Risiko aussetzen, dass eine andere außenstehende Person auf seine persönlichen Informationen zugreift bedeutet also für den Kontroll-Ansatz nicht nur, dass der Zugang für Außenstehende erleichtert wird, sondern auch, dass die Kontrolle des Individuums beschränkt wird oder die schon beschränkte Kontrolle nicht berücksichtigt wird.

Laut Lundgren verletzen Außenstehende die Privatsphäre eines Individuums außerdem dann, wenn sie dafür sorgen, dass das Individuum glaubt, dass oder unsicher ist, ob seine privaten Angelegenheiten dem Risiko des Zugriffs durch eine andere außenstehende Person ausgesetzt sind.⁶⁶⁶ Wenn Außenstehende einen solchen Glauben oder Unsicherheit bei den betroffenen Individuen auslösen kann das zwar normativ verurteilt werden, aber es stellt allein noch keine Verletzung der Privatsphäre dar. Ich denke, eine intakte Privatsphäre

⁶⁶⁵ Lundgren 2021b:387

⁶⁶⁶ Ebd.:389

umfasst nicht das Wissen darüber, ob die persönlichen Informationen dem Risiko des Zugriffs durch eine außenstehende Person ausgesetzt sind. Denn die Verletzung der Privatsphäre geschieht nicht, wenn das Individuum das Gefühl hat, die Kontrolle zu verlieren, sondern wenn die Außenstehenden tatsächlich zugreifen oder versuchen zuzugreifen.

Zusammenfassung

In der Literatur wird nicht klar unterschieden zwischen der Perspektive des Individuums und der Perspektive von Außenstehenden – ich denke das ist ein Fehler. Denn hierdurch wird deutlich, dass nur Außenstehende die Privatsphäre des Individuums verletzen können – dies geschieht durch eine Handlung, die nicht zwingend eine schlechte Intention haben muss. Dank Tabelle 2 wird deutlich, wann die Privatsphäre von Individuen intakt und wann sie verletzt ist, und was Außenstehende vermeiden sollten, um die Privatsphäre der Individuen nicht zu verletzen.

Tabelle 2 Teile der Privatsphäre als Wahl-Kontrolle⁶⁶⁷

Wahl-Kontroll-Ansatz	Individuum	Außenstehende
Privatsphäre intakt	Das Individuum hat Wahl-Kontrolle über den Zugang zu und die Benutzung von persönlichen Informationen.	Außenstehende versuchen nicht auf persönliche Informationen des Individuums zuzugreifen, ohne dass das Individuum darüber die Wahl-Kontrolle hat, und sie greifen auch nicht tatsächlich, nicht einmal aus Versehen, darauf zu.
Privatsphäre verletzt	Das Individuum hat eine eingeschränkte oder fehlende Wahl-Kontrolle über den Zugang zu und die Benutzung von persönlichen Informationen.	Außenstehende versuchen <i>bewusst</i> auf persönliche Informationen des Individuums zuzugreifen, ohne dass das Individuum darüber die Wahl-Kontrolle hat. ODER Außenstehende greifen tatsächlich, womöglich auch <i>aus Versehen</i> , auf persönliche Informationen des Individuums zu und benutzen diese, ohne dass das Individuum darüber die Wahl-Kontrolle hat.

667 Eigene Darstellung

Abschließend lässt sich sagen, dass es die Definition der Privatsphäre als Wahl-Kontrolle ermöglicht zu bestimmen, wann Privatsphäre intakt und wann sie verletzt ist.

Privatsphäre ist intakt, wenn das Individuum die Wahl-Kontrolle hat über Zugang zu und Benutzung von seinen persönlichen⁶⁶⁸ Informationen. Das heißt, das Individuum hat die Kontrolle darüber, mit wem es welche Informationen zu welchem Zweck teilt.

Privatsphäre wird verletzt, wenn das Individuum die Kontrolle über Zugang zu und die Benutzung von persönlichen Informationen verliert. Außenstehende können diesen Kontrollverlust verursachen, indem sie bewusst versuchen auf persönliche Informationen des Individuums zuzugreifen und diese zu benutzen oder tatsächlich zugreifen, womöglich auch aus Versehen, ohne dass das Individuum darüber die Kontrolle hat. Außerdem können Außenstehende durch fahrlässiges Handeln Beihilfe zur Privatsphärenverletzung leisten, indem sie das Individuum einem substanziell größeren Risiko aussetzen, dass eine andere außenstehende Person auf seine persönlichen Informationen zugreift.

Außerdem lässt die Definition von Privatsphäre als Wahl-Kontrolle Raum für individuelle Intuitionen, da die Individuen nach eigenem Ermessen Zugang gewähren und verweigern können, und erfüllt damit all meine Kriterien. Ob alle Individuen ein Recht auf Privatsphäre im Sinne ihrer Wahl-Kontrolle haben, soll im folgenden Kapitel erörtert werden.

6.3 Moralische Pflicht zum Schutz der Privatsphäre und resultierendes Recht auf Privatsphäre

Eine Pflicht zum Schutz der Privatsphäre sowie ein daraus abgeleitetes Recht auf Privatsphäre würden vor Handlungen schützen, die das Risiko einer erheblichen Beeinträchtigung der Privatsphäre mit sich bringen.⁶⁶⁹ Vor welchen Handlungen eine solche moralische Pflicht und das daraus resultierende Recht auf Privatsphäre genau

668 Das *Persönliche* bezieht sich hier darauf, dass die Informationen das Individuum betreffen und es deshalb entscheiden kann, mit wem es welche Informationen zu welchem Zweck teilt.

669 Lundgren 2021a:672

schützt, hängt je nach Autor:innen von der jeweiligen Definition der Privatsphäre ab. In dieser Arbeit soll die moralische Pflicht zum Schutz der Privatsphäre die Datenquellen davor bewahren die Wahl-Kontrolle über ihre Daten zu verlieren. Das Ziel dieses Kapitels ist es, eine moralische Pflicht zum Schutz der Privatsphäre der Datenquellen zu begründen und zu verstehen, wie daraus ein Recht auf Privatsphäre resultieren kann.

Eine solche moralische Pflicht zum Schutz der Privatsphäre lässt sich aus Kants erster Formulierung des Kategorischen Imperativs ableiten.⁶⁷⁰ Denn wenn eine Handlungsmaxime weder gedacht noch gewollt werden kann, ist es eine vollkommene Pflicht, diese Handlung zu vermeiden. Eine Handlungsmaxime, die zwar denkbar ist, aber nicht widerspruchsfrei gewollt werden kann, etabliert eine unvollkommene Pflicht.⁶⁷¹ Es ist zwar denkbar, dass die Privatsphäre von Datenquellen verletzt wird, um andere Ziele zu verwirklichen, aber es kann nicht gewollt werden – das etabliert eine unvollkommene Pflicht zum Unterlassen der Verletzung der Privatsphäre. Diese Pflicht sowie eine damit einhergehende Pflicht zum Schutz der Privatsphäre lassen sich begründen, indem zum einen erklärt wird, warum die Verletzung der Privatsphäre von Individuen vermieden werden sollte, und zum anderen aufgezeigt wird, warum eine intakte Privatsphäre erstrebenswert ist.

Die Vermeidung von Privatsphärenverletzungen ist ein guter Grund, warum die Privatsphäre schützenswert ist. Der Gedanke findet sich auch bei O'Neill: „Securing privacy matters because it can protect individuals from interference (...)”.⁶⁷² Der Schutz vor solchen Eingriffen ist deshalb notwendig, weil Verletzungen der Privatsphäre die Möglichkeit zur Erpressung schaffen können.⁶⁷³ Denn wenn Unbefugte an sensible Gesundheitsdaten gelangen, könnten sie zum Beispiel Menschen mit einer psychischen Diagnose erpressen. Der Schutz der Privatsphäre erlaubt es Personen, ihre psychische Diagnose nur mit denjenigen Personen zu teilen, denen sie vertrauen.

670 Kant 2008:53 [421]

671 Ebd.:55–58 [422–424]

672 O'Neill 2021:79

673 Ebd.:79

Laut O'Neill ist es möglich, dass durch die Verbreitung von persönlichen Informationen Schaden angerichtet wird: „(...) in connected societies where information trading is both efficient and nearly without cost, disclosure of personal information opens individuals up to certain risks—such as being controlled by entities with their own agendas.“⁶⁷⁴ Wenn Informationen über eine Person für die Öffentlichkeit zugänglich gemacht werden, dann wird diese Person schlechter gestellt im Sinn eines erhöhten Risikos für zum Beispiel staatliche Kontrolle oder kommerzielle Ausbeutung.⁶⁷⁵

Persönliche Informationen können auch von Regierungen zur Unterdrückung der Staatsbürger:innen und zur Erweiterung der eigenen Macht benutzt werden.⁶⁷⁶ Zum Beispiel gibt es in China über jeden Menschen eine Akte namens „Dangan“, die ab der Grundschule geführt wird und alle möglichen persönlichen Informationen enthält. Insbesondere Einträge zur politischen Einstellung können die beruflichen Möglichkeiten und die Reisefreiheit der Menschen beeinflussen.⁶⁷⁷ Gleichermäßen können Wirtschaftsunternehmen persönliche Informationen dazu benutzen, Kunden mit einer Flut an Werbung zu überfordern oder auch ihre Angestellten zu kontrollieren.⁶⁷⁸ Insbesondere, wenn diese Informationen digital gespeichert werden, erhöht sich das Risiko, weil Daten im digitalen Raum dauerhaft zugreifbar bleiben.⁶⁷⁹ Deshalb werden den Menschen laut Moore durch die Digitalisierung, die Gefahr der Manipulation und die Möglichkeit der Verbreitung von persönlichen Informationen als Risiken auferlegt, welche ungerechtfertigt Schaden anrichten können.⁶⁸⁰

Der Schutz der Privatsphäre verhindert also, dass Menschen diskriminiert werden beispielsweise wegen einer bestimmten politischen Einstellung, und dadurch wiederum erlaubt sie es den Menschen, ihre Rechte wahrzunehmen, zum Beispiel zu demonstrieren. Wenn eine Regierung wüsste, welche politische Einstellung die Staatsbürger:innen haben und wo sie sich aufhalten, dann könnten

674 O'Neill 2021:88

675 Ebd.:86, 91

676 Moore 2010:88

677 Moore 2010:89

678 Ebd.:89f.

679 Ebd.:90f.

680 Ebd.:98

sie das Versammeln von Gruppen zu Demonstrationen verhindern. Die Privatsphäre schützt vor solchen Eingriffen und untermauert damit grundlegende Menschenrechte.⁶⁸¹ Außerdem verhindert der Schutz der Privatsphäre, dass sich die betreffenden Personen für die offenbarten Informationen schämen, sich verfolgt fühlen oder andere mentale Beeinträchtigungen erleiden.⁶⁸²

Zudem ermöglicht eine intakte Privatsphäre auch mehr Autonomie, da die Menschen in privaten Räumen nicht von anderen bewertet werden und dementsprechend unabhängiger entscheiden können.⁶⁸³ Rössler behauptet, dass „(...) Autonomie nicht, oder jedenfalls nicht in all ihren und nicht in ihren relevantesten Aspekten, lebbar ist ohne den Schutz von Privatheit, ohne die Unterscheidung zwischen privaten und öffentlichen Dimensionen oder Bereichen des Lebens.“⁶⁸⁴ Einerseits beschützt die Privatsphäre also das, was der Philosoph Isaiah Berlin negative Freiheit nennt – die Abwesenheit von Eingriffen.⁶⁸⁵ Andererseits unterstützt die Privatsphäre aber auch die von O'Neill sogenannten „capacities to act“⁶⁸⁶, ermöglicht dadurch also die positive Freiheit.⁶⁸⁷ Der Schutz der Privatsphäre schließt also auch andere Werte ein.⁶⁸⁸

Laut Moore ist Privatsphäre für das menschliche Wohlbefinden unerlässlich, da die Fähigkeit, sich zurückzuziehen, für Menschen eine Lebensnotwendigkeit und gleichzeitig die Gesellschaft anderer Menschen ein menschliches Grundbedürfnis ist.⁶⁸⁹ Um beidem gerecht zu werden, öffnen sie ihre Privatsphäre selektiv: „Somewhere on the continuum between one's innermost thoughts that are never shared and what one offers up for anyone's consideration we switch from the private to the public.“⁶⁹⁰ Daraus schlussfolgert Moore, dass die Fähigkeit, den Zugang zu und die Nutzung von persönlichen Informationen zu regeln, für das menschliche Wohlbefin-

681 Bernal 2016:252

682 Price, Cohen 2019:41

683 Masur et al. 2018:6; Westin 1967, S. 35–43

684 Rössler 2003:30

685 Berlin 1997:195

686 O'Neill 2021:79

687 Berlin 1997:196, 202f.

688 Barocas, Nissenbaum 2014:49

689 Ebd.:48f.; 86f.

690 Moore 2010:87

den unerlässlich ist.⁶⁹¹ In ähnlicher Weise argumentiert Fried, dass der Entzug der Privatsphäre die Möglichkeit, Intimität zu gewähren, zerstört und dadurch die wesentliche Dimension von Liebe und Freundschaft unmöglich macht, sowie die Fähigkeit des Subjekts, Vertrauensbeziehungen einzugehen, untergräbt. Da aber intime Beziehungen der Liebe und der Freundschaft dem menschlichen Leben einen großen Teil des positiven Wertes verleihen und die Privatsphäre dafür den Rahmen bildet, ist ihr Schutz notwendig.⁶⁹²

Moore betont weiter, dass Privatsphäre nicht nur schützenswert, sondern auch wertvoll sei, da sie für das Überleben und die geistige Gesundheit notwendig ist.⁶⁹³ Daraus ergibt sich ein Anspruch auf Kontrolle über persönliche Informationen – zumindest solange dadurch niemand geschädigt wird. Da Informationen von mehreren Personen gleichzeitig besessen, konsumiert oder betrachtet werden können, ohne einander zu schaden⁶⁹⁴, entstehen moralische Nutzungsansprüche an die eigenen Informationen, sofern niemand dadurch schlechter gestellt wird.⁶⁹⁵

Die Verletzung der Privatsphäre stellt also insbesondere deshalb ein unerwünschtes Ereignis dar, weil sie mit einer Risikoauferlegung gleichzusetzen ist – es entsteht das Risiko ungewollter Eingriffe und Diskriminierung sowie das Risiko fehlender Autonomie und Intimität. Ich stimme also Moore zu, dass den betroffenen Individuen durch die Verletzung der Privatsphäre ein unzulässiges Risiko auferlegt wird.⁶⁹⁶ Für Moore ist zwar die Schlussfolgerung aus dieser Argumentation, dass es ein Recht auf Privatsphäre geben sollte, aber die Argumente für eine intakte Privatsphäre und gegen die Verletzung der Privatsphäre können ebenfalls zu der Schlussfolgerung führen, dass es eine Pflicht zum Schutz der Privatsphäre geben sollte. Da in dieser Arbeit davon ausgegangen wird, dass ein Recht auf Privatsphäre nur aus einer Pflicht zum Schutz der Privatsphäre resultieren kann⁶⁹⁷, ist hier die Schlussfolgerung, dass es eine Pflicht zum Schutz der Privatsphäre geben sollte. Die moralische Pflicht

691 Moore 2010:21; 56

692 Fried 1968:216

693 Moore 2010:43f., 86f.

694 Ebd.:82, 98

695 Ebd.:84f.

696 Ebd.:97

697 Mohr 2010:77

der Datengenerierenden zum Schutz der individuellen Privatsphäre begründet sich dabei sowohl durch die negativen Konsequenzen, die eine Verletzung der Privatsphäre verursachen kann – es entstehen Risiken, die für das Wohlbefinden der betroffenen Person moralisch relevant sind⁶⁹⁸ – als auch durch die positiven Konsequenzen, für die eine intakte Privatsphäre sorgen kann.⁶⁹⁹

Dabei sind aus deontologischer Sicht genau die Handlungsfolgen relevant, welche die moralischen Grundsätze verbieten oder herbeiführen wollen. Somit ist laut Hare aus deontologischer Sicht das Verletzen der Privatsphäre von Datenquellen unter anderem deshalb falsch, weil es Erpressung, staatliche Kontrolle oder kommerzielle Ausbeutung zur Folge haben kann. Der Grundsatz des Kategorischen Imperativs verbietet die Handlungsfolgen der Erpressung, staatlicher Kontrolle oder kommerzieller Ausbeutung, weil die zugrundeliegende Handlungsmaxime nicht gewollt werden kann und somit eine unvollkommene Pflicht entsteht, diese Handlung zu vermeiden. Entsprechend dieses Grundsatzes ist es moralisch relevant, wenn die Folge einer Handlung entweder Erpressung, staatliche Kontrolle oder kommerzielle Ausbeutung ist.⁷⁰⁰ Im Prinzip ist es denkbar, dass sich die Menschen gegenseitig erpressen, kontrollieren und ausbeuten. Aber niemand kann es wollen erpresst, staatlich kontrolliert oder kommerziell ausgebeutet zu werden.

Außerdem ist laut Hare das Verletzen der Privatsphäre von Datenquellen deshalb falsch, weil sich Datenquellen ohne intakte Privatsphäre nicht autonom entfalten können und zum Beispiel keine intimen Beziehungen der Liebe und der Freundschaft eingehen können – das schadet ihrem Wohlbefinden und dadurch können sie ihrem Selbstzweck nicht gerecht werden.⁷⁰¹ In dem die Privatsphäre der Datenquellen verletzt wird, also ihre Daten ohne ihre Kontrolle und ihre Zustimmung verwendet werden, werden die Datenquellen als bloßes Mittel gebraucht. Die dritte Formel des Kategorischen Imperativs verbietet aber, dass Datennutzende in dieser Weise als bloßes Mittel gebraucht werden. Diese Konsequenz, Datenquellen die Möglichkeit zu verwehren sich autonom zu entfalten für ihr Wohl-

698 Moore 2010:97 Rössler 2003:3

699 Masur et al. 2018:6; Vgl. Westin 1967, S. 35–43; Fried 1968:216

700 Hare 1993:15

701 Rössler 2003:30; Moore 2010: 21; 56, 87; Fried 1968:216

befinden (und sie dadurch bloß als Mittel zu gebrauchen), ist das, was das Verletzen der Privatsphäre falsch mache.⁷⁰² So lässt sich aus den negativen Konsequenzen, die eine Verletzung der Privatsphäre verursachen kann mit der deontologischen Perspektive von Hare eine vollkommene Pflicht zum Schutz der Privatsphäre begründen – denn es ist nicht denkbar, dass die Menschen den Kategorischen Imperativ ignorieren und sich als bloße Mittel gebrauchen.

Aus dieser vollkommenen moralischen Pflicht zum Schutz der Privatsphäre auf Seiten der Datengenerierenden kann ein Primärrecht auf Privatsphäre für Datenquellen resultieren.⁷⁰³ Der praktische Philosoph Ingmar Persson und der Medizin- und Technikethiker Julian Savulescu argumentieren jedoch, es sei unmöglich, dass es ein Recht auf Privatsphäre geben kann. Allerdings legen sie ihrem Argument eine definitorische Voraussetzung zu Grunde, die ich hier widerlegen möchte. Die beiden Autoren definieren ein Recht auf Privatsphäre folgendermaßen: „A right to privacy is conceived as a right that others do not acquire information about us that we reserve for ourselves and selected others.”⁷⁰⁴ Dabei machen sie – ohne dies begrifflich zu kennzeichnen – eine Unterscheidung zwischen dem passiven Erlangen (acquire) der Informationen und den Mitteln, die zum aktiven Beschaffen (acquire) der Informationen verwendet werden. Ihre These ist, dass wir das Recht gegenüber anderen haben können, dass sie sich von bestimmten Mitteln der Informationsbeschaffung fernhalten, aber nicht von der Informationsbeschaffung an sich.

Aus Perssons und Savulescus Sicht ist das Erlangen von Informationen keine Handlung, sondern ein innerer Zustand, der herbeigeführt wird.⁷⁰⁵ Im Verlaufe des Artikels wird klar, dass mit dem Erlangen (acquire) von Informationen das passive Wahrnehmen von Informationen gemeint ist – nicht das aktive Beschaffen. Denn Persson und Savulescu vergleichen das Erlangen von Informationen mit dem Empfinden von Emotionen: „(...) the state of acquiring information is in itself evaluatively neutral.”⁷⁰⁶ Es geht ihnen also darum, dass es kein Recht zum Schutz gegen das zufällige und unabsichtliche Wahrnehmen von privaten Informationen geben kann.

702 Hare 1993:15

703 Mohr 2010:77; Mieth, Bambauer 2016:3

704 Persson, Savulescu 2022:1

705 Ebd.

706 Ebd.:3

Diese These beruht aber auf einem Missverständnis: Das Recht auf Privatsphäre soll kein Recht sein auf den Schutz vor Sinneswahrnehmungen von Mitmenschen, sondern vor deren absichtlicher Informationsbeschaffung. Denn die informationelle Privatsphäre wird nicht mehr vorrangig im direkten Kontakt durch Sinneseindrücke verletzt, sondern online. Im digitalen Raum lassen sich die Mittel nicht mehr so leicht von der Informationsbeschaffung trennen, da man kaum unabsichtlich private Informationen wahrnehmen kann, die nicht geteilt werden sollten. Das Gegenüber könnte im Zoom Meeting aus Versehen die Kamera angeschaltet haben, sodass eine private Situation wahrzunehmen ist. Aber ansonsten hängt die Beschaffung von Informationen meist mit einem bewusst ausgewählten Mittel zusammen.

An dieser Stelle lohnt es sich, die Argumentationen für ein (moralisches) Recht auf Privatsphäre zu betrachten, da hieraus weitere Gründe für eine Pflicht zum Schutz der Privatsphäre ersichtlich werden. Laut Moore gibt es grob zwei Perspektiven auf das Recht zur Privatsphäre: Es gibt in der philosophischen Debatte die Reduktionist:innen, die argumentieren, dass die Privatsphäre von anderen Rechten, wie dem Recht auf Leben, Freiheit und Eigentum, abgeleitet ist und es gibt die der Nicht-Reduktionist:innen, welche die Privatsphäre als mit anderen Rechten oder moralischen Konzepten verwandt betrachten, diese aber als eine eigene Art von Rechten anerkennen.⁷⁰⁷

Reduktionismus

Die bereits erwähnte Moralphilosophin und Metaphysikerin Judith Jarvis Thomson ist der Meinung, dass das Recht auf Privatsphäre ein abgeleitetes Recht ist. Das werde dadurch deutlich, dass man jede Verletzung der Privatsphäre erklären könne, ohne das Recht auf Privatsphäre zu erwähnen. Wenn zum Beispiel jemand beobachtet oder belauscht wird, erscheint das wie eine Verletzung der Privatsphäre. Thomson meint dazu, Menschen hätten das Recht, nicht beobachtet und belauscht zu werden, aber nicht, weil sie ein Recht auf Privatsphäre haben, sondern weil sie Rechte an ihrer Person haben. Wenn jemand gefoltert wird, um ihm persönliche Informationen zu entlo-

707 Moore 2010:14ff.

cken, wird seine Privatsphäre verletzt. Aber laut Thomson muss das nicht mit Hilfe seines Rechtes auf Privatsphäre erklärt werden, sondern mit seinem Recht, nicht verletzt oder geschädigt zu werden. Und wenn sich jemand den Inhalt eines fremden Safes anschaut, ist das laut Thomson falsch, weil jeder das Recht hat, dass sein Eigentum nicht angesehen wird – nicht, weil man ein Recht auf Privatsphäre hat.⁷⁰⁸ Laut Thomson lässt sich die Verletzung der Privatsphäre vollständig mit Verstößen gegen andere Individualrechte erklären.⁷⁰⁹

Auch Macnish meint, dass durch den Verlust der Kontrolle über die eigenen Informationen zwar nicht die Privatsphäre verletzt wird, aber ein Risiko für anderweitigen Schaden entsteht. Sobald die Fremde im Café die Kontrolle über die Informationen im Tagebuch übernimmt, entscheidet jemand anderes als die Person selbst, was mit dem Tagebuch und den darin enthaltenen Informationen geschieht. Die Fremde aus dem Café, die über die Informationen im Tagebuch verfügt, kann nun sowohl auf die Informationen zugreifen (d. h. die Privatsphäre der Person verletzen) als auch, unter sonst gleichen Bedingungen, die Informationen wahrscheinlich zu ihrem Vorteil nutzen. Es gibt Anreize für die Fremde aus dem Café, so zu handeln, dass sie davon profitiert und die Tagebuchbesitzerin die Kosten dafür trägt. Es sei rational, unter der Annahme zu handeln, dass sie dies bereits getan hat. Auch wenn die Fremde aus dem Café – die neue Kontrolleurin der Informationen – nicht tatsächlich auf die Informationen zugegriffen hat, sind die Folgen so, als hätte sie es getan. Es handelt sich also um eine Verletzung der Rechte und Interessen, die wir durch Geheimhaltung bestimmter Informationen schützen wollen⁷¹⁰: „(...) a loss of control may involve harms to the rights that privacy protects.“⁷¹¹ Die Verletzung dieser Rechte und Interessen könne sich wie eine Verletzung der eigenen Privatsphäre anfühlen, auch wenn sie es nicht sei. Denn durch den Verlust der Kontrolle sei man denjenigen ausgeliefert, die nun Kontrolle haben über die eigenen Informationen: „(...) it is the increased risk of losing privacy that is one of the considerations that renders a loss of control over information (or space) problematic.“⁷¹² Denn

708 Thomson 1975:313

709 Ebd.:308

710 Macnish 2018:426ff.

711 Ebd.:429

712 Ebd.:423

durch den Kontrollverlust fühlt man sich nicht nur verletztlich, man ist auch verletztlich.⁷¹³

Auch wenn in dieser Arbeit, mit Bezug auf Mohr, davon ausgegangen wird, dass sich das Recht auf Privatsphäre nur aus der Pflicht zum Schutz der Privatsphäre ableiten lässt⁷¹⁴, wird trotzdem kein reduktionistischer Ansatz vertreten. Denn das aus der Pflicht zum Schutz der Privatsphäre resultierende Recht auf Privatsphäre kann dennoch als eine eigene Art von Recht anerkannt werden.

Nicht-Reduktionismus

Parent argumentiert, es wäre vernünftiger und verständlicher, von einem Grundrecht auf Privatsphäre zu sprechen, das unter bestimmten Umständen Personen Schutz bieten kann, die nicht gesehen oder gehört werden wollen, oder die nicht wollen, dass ihr Eigentum beobachtet wird: „Privacy is a fundamental human value in societies like ours. It makes perfectly good sense for us, then, to acknowledge a fundamental right to privacy.“⁷¹⁵ Auf diese Weise müssten Privatsphärenverletzungen nicht mehr mit Hilfe der Verletzung anderer Rechte erklärt werden.

Der Behauptung, dass das Recht auf Privatsphäre ein eigenständiges Recht sein soll, würden Manson und O'Neill zustimmen. Sie begründen das Recht auf Privatsphäre damit, dass die Menschen ein Interesse an ihrer Privatsphäre haben.⁷¹⁶ Sie gehen sogar einen Schritt weiter und postulieren, dass alle Menschen ein Interesse am Schutz der Privatsphäre haben sollten: „It seems uncontentious enough that each of us may have reason to keep certain information from becoming known by others, or by certain others, without our consent.“⁷¹⁷ Aber Moore bemerkt die Schwäche dieses Argumentes – seine Subjektivität. Denn wenn die Interessen der privaten Menschen relevant sind, dann wären auch die Interessen der Privatsphäre-Verletzenden ausschlaggebend: „(...) preferences can be arbitrary

713 Macnish 2018:419, 430

714 Mohr 2010:77

715 Parent 1983b:350

716 Manson, O'Neill 2007:98

717 Ebd.:98f.

(...).“⁷¹⁸ Um diesem Widerspruch aus dem Weg zu gehen, argumentiert Moore, dass ein eigenständiges Recht auf Privatsphäre wertvoll ist, weil es für das menschliche Wohlbefinden unerlässlich ist und außerdem durch den Anspruch auf Nutzung und Kontrolle der eigenen Informationen keinen Schaden für jemand anderen entsteht.⁷¹⁹

Laut Moore darf eine Person nicht beobachtet oder belauscht werden, weil dadurch Risiken entstehen, die für das Wohlbefinden der beobachteten oder belauschten Person moralisch relevant sind. Das Beobachten oder Belauschen selbst mag die Situation der betroffenen Person nicht direkt verschlechtern, aber eine solche Praxis des gegenseitigen Beobachtens und Belauschens würde die betroffenen Personen schlechter stellen. Laut Moore haben Individuen das Recht auf Privatsphäre, nicht weil ihr materielles Wohlergehen dadurch geschädigt wird oder weil sie den allgemeinen Wunsch haben, nicht beobachtet zu werden – dann wäre der Wunsch zu beobachten auch moralisch relevant. Sondern Individuen haben ein Recht auf Privatsphäre, weil ihnen durch die Verletzung der Privatsphäre ein unzulässiges Risiko auferlegt würde.⁷²⁰ Da in dieser Arbeit davon ausgegangen wird, dass ein Recht auf Privatsphäre nur aus einer Pflicht zum Schutz der Privatsphäre resultieren kann⁷²¹, haben zuerst einmal Datengenerierende eine Pflicht zum Schutz der Privatsphäre von Datenquellen, weil Erstere den Letztgenannten durch die Verletzung der Privatsphäre ein unzulässiges Risiko auferlegen würden. Daraus kann dann ein Recht der Datenquellen auf ihre intakte Privatsphäre abgeleitet werden.

Es gibt aber auch Einwände gegen die Pflicht zum Schutz der Privatsphäre: So ließe sich argumentieren, dass die Risiken, die durch das Missachten der Privatsphäre entstehen können, ausgeglichen werden durch mehr Möglichkeiten und mehr Sicherheit.⁷²² Denn durch die Überwachung aller Menschen können die Böswilligen unter ihnen identifiziert und davon abgehalten werden, Schaden anzurichten. Aber die bei der Überwachung zusammengetragenen Informationen können auch für andere Zwecke als die Identifikati-

718 Moore 2010:34

719 Ebd.

720 Moore 2010:97

721 Mohr 2010:77

722 Ebd.:91

on von Terroristen genutzt werden. Diese Zweckentfremdung der Daten nennt sich *data shifting*. So könnten mit Hilfe der Terrorismus-Überwachungsdaten auch politische Einstellungen beobachtet und bewertet werden. Dies kann, genau wie beim chinesischen „Dangan“, zu unterschiedlicher Behandlung von Menschen je nach politischer Einstellung führen. Dieses *data shifting* ist besonders deshalb gefährlich, weil sich die Risiken der multiplen Datennutzung erhöhen können. Wenn zum Beispiel die Regierung wechselt und sich als autokratisch erweist, entstehen neue Risiken, die zu Beginn nicht vorausgesehen wurden. Daraus lässt sich ein starkes Argument gegen diesen Einwand ableiten. O'Neill dreht das Argument sogar um: „Privacy is necessary for a degree of security (...)“.⁷²³ Man kann eine Einschränkung der Privatsphäre nicht mit einem Gewinn an Sicherheit rechtfertigen, weil der Schutz der Privatsphäre selbst wichtig ist, um Sicherheit zu ermöglichen. Denn beim Verletzen der Privatsphäre entstehen Risiken, welche die Sicherheit der Betroffenen gefährden.

Ein zweiter Einwand gegen die Pflicht zum Schutz der Privatsphäre ist, dass Individuen durch ihr Verhalten und das Teilen von Informationen in der Öffentlichkeit der Kontrolle über ihre Informationen durch andere zustimmen. Allerdings bedeutet das Verhalten in der Öffentlichkeit nicht, dass man einer zweckentfremdeten Nutzung oder einer Sammlung dieser Informationen zustimmt. Für viele Menschen ist es eine Notwendigkeit, in der Gesellschaft zu erscheinen – das ist nicht gleichzusetzen mit dem Einverständnis zur Überwachung ihres Verhaltens.⁷²⁴ Hier ist wieder Moores Unterschied zwischen Zugang und Benutzung relevant: Nur weil eine Person den Zugang zu ihren Informationen gewährt, heißt das nicht, dass sie auch mit jeglicher Benutzung ihrer Informationen einverstanden ist.⁷²⁵

Die moralische Pflicht zum Schutz der Privatsphäre führt laut Mohr zu Legitimitäts-Forderungen an die Rechtsordnung: „Die Menschheit hat die moralische Pflicht, ein System von Rechten zu etablieren, welches sicherstellt, dass die Adressaten von Pflichten rechtlich zur Erfüllung ihrer Pflichten gezwungen werden können. Dazu sind moralische Rechte nicht imstande, nur [mit] juristischen

723 O'Neill 2021:80

724 Moore 2010:92

725 Ebd.:28

Rechten korrelieren Rechtspflichten, und nur diese sichern die Erfüllung von berechtigten Ansprüchen.“⁷²⁶ Ein Recht bleibt aber etwas Institutionelles, das aus einer moralischen Pflicht zum Schutz motiviert sein kann. Das ist in der Geschichte schon oft geschehen. Im Jahr 1890 zum Beispiel forderten die Juristen Samuel D. Warren und Louis D. Brandeis die Entwicklung von Gesetzen parallel zu der Neuerungen, dass Fotografien von Privatpersonen in Zeitungen verbreitet wurden. Neue mechanische Geräte ermöglichten es plötzlich, Privates zu veröffentlichen: „For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers (...).“⁷²⁷ Heute, 133 Jahre später, gibt es eine europäische Rechtsprechung, die den Schutz unserer Privatsphäre im Angesicht der neuen technischen Entwicklungen gewähren soll. Die rechtliche Entwicklung macht deutlich, dass Datengenerierende eine Pflicht zum Schutz der Privatsphäre haben, zu der sie mit Hilfe der Rechtsprechung zur Verantwortung gezogen werden können.

6.3.1 Aktueller rechtlicher Rahmen im Vergleich zu ethischen Anforderungen

In der Europäischen Union ist Datenschutz rechtlich verankert in der Datenschutzgrundverordnung (DSGVO): „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.“⁷²⁸ Für die Verarbeitung von personenbezogenen Daten wurden folgende Grundsätze erstellt: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht.⁷²⁹ Die Verarbeitung personenbezogener Daten ist nach der DSGVO dann rechtmäßig, wenn die betroffene Person ihre Einwilligung für einen oder mehrere bestimm-

726 Mohr 2010:77

727 Warren, Brandeis 1890:195

728 Artikel 1, Absatz 1 DSGVO

729 Artikel 5 DSGVO

te Zwecke gibt.⁷³⁰ Die Erklärung zur Einwilligung muss „(...) in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (...)“⁷³¹ formuliert sein und die Einwilligung der betroffenen Person muss nachweisbar und jederzeit leicht widerrufbar sein.⁷³² Außerdem soll die Einwilligung freiwillig auf der Basis von Informationen über die Verarbeitung und ihre Zwecke erfolgen.⁷³³ Dabei soll die Zustimmung *aktiv* erfolgen und nicht auf Grund einer vorausgewählten Einwilligung. Zudem kann ein Vertrag, eine rechtliche Verpflichtung zum Schutz lebenswichtiger Interessen von natürlichen Personen sein, und öffentliches Interesse und die Wahrung berechtigter Interessen von natürlichen Personen kann ein rechtmäßiger Grund für die Verarbeitung personenbezogener Daten sein.⁷³⁴ Die Personen, deren Daten verarbeitet wurden, haben unter anderem ein Recht auf Auskunft, Berichtigung unrichtiger Daten und Löschung von falschen oder nicht mehr benötigten Daten.⁷³⁵ „Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.“⁷³⁶ Dabei muss es immer eine verantwortliche Person für die Datenverarbeitung geben⁷³⁷, und personenbezogene Daten dürfen nicht beliebig weitergegeben werden⁷³⁸.

Auch das deutsche Grundgesetz schützt die Kontrolle von Individuen über ihre Informationen. Das Bundesverfassungsgericht hat im Jahr 1983 geurteilt, dass sich aus der Menschenwürde (GG Artikel 1, Absatz 1) und dem allgemeinen Persönlichkeitsrecht (GG Artikel 2, Absatz 1) ein Recht auf informationelle Selbstbestimmung ableiten lässt: „Das Grundrecht gewährleistet insoweit die Befugnis des

730 Art. 6, Absatz 1 a) DSGVO

731 Art. 7 DSGVO

732 Ebd.

733 Erwägungsgrund 32 DSGVO

734 Art 6, Absatz 1 b)-f) DSGVO

735 Artikel 15–17 DSGVO

736 Artikel 22, Absatz 1 DSGVO

737 Artikel 24–43 DSGVO

738 Artikel 44–50 DSGVO

Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“⁷³⁹

Bedrohungen der Privatsphäre entstehen dem Juristen Daniel Solove zufolge durch zum Beispiel Überwachung, Datensammlung, persönliche Identifizierung und Zweckentfremdung, sodass die Verletzung der Vertraulichkeit und persönliche Bloßstellung, sowie der Ausschluss von Individuen, Einflussnahme auf Entscheidungen oder Erpressung möglich werden.⁷⁴⁰ Die Ingenieurwissenschaftlerin Marie Caroline Oetzel und die Wirtschaftsinformatikerin Sarah Spiekermann haben im Jahr 2014 den damaligen Entwurf der DSGVO mit den möglichen Bedrohungen der Privatsphäre abgeglichen und kamen zu dem Schluss, dass die Datenschutzvorschriften die Eindämmung aller potenziellen Gefahren für die Privatsphäre unterstützen.⁷⁴¹

Ich argumentiere jedoch, dass im Recht ausschließlich ein ethischer Mindeststandard festgehalten ist, der im Gegensatz zur Ethik auch Ausnahmen vorsieht. Laut Artikel sechs der Datenschutzgrundverordnung ist die Datenverarbeitung auch dann rechtmäßig, wenn die betroffene Person der Verarbeitung nicht zugestimmt hat. Denn weitere Bedingungen für die Rechtmäßigkeit der Datenverarbeitung sind die Erfüllung eines Vertrages (b), die Erfüllung einer rechtlichen Verpflichtung (c), der Schutz von lebenswichtigen Interessen von Personen (d), die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (e), oder die Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (f).⁷⁴² Dies gilt auch für das Übermitteln personenbezogener Daten an ein Drittland oder an eine internationale Organisation. So können auch hier Verträge (b und c), öffentliches Interesse (d), Rechtsansprüche (e) oder lebenswichtige Interessen (f) ausschlaggebend sein.⁷⁴³

Eigentlich sollten die betroffenen Personen ihre Einwilligung zu jedem konkreten Verarbeitungszweck ihrer Daten geben können⁷⁴⁴,

739 BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83

740 Solove 2006; Oetzel, Spiekermann 2014:130

741 Oetzel, Spiekermann 2014:130

742 Artikel 6 (1) DSGVO

743 Artikel 49 (1) DSGVO

744 Erwägungsgrund 32 DSGVO

aber auch hier gibt es Ausnahmen. Denn insbesondere im Kontext von wissenschaftlicher Forschung ist es schwierig, jeden einzelnen Verarbeitungszweck schon während der Datenerhebung anzugeben. Deshalb ist es laut Erwägungsgrund 33 der DSGVO möglich, nur eine breite Zustimmung für bestimmte Bereiche wissenschaftlicher Forschung einzuholen.⁷⁴⁵ Ähnlich urteilte das Bundesverfassungsgericht, dass es auch bei der Datenerhebung für Statistiken nicht möglich sei, die Einwilligung für jeden konkreten Zweck einzuholen.⁷⁴⁶ Zudem gilt laut DSGVO der Datenschutz nur für Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das heißt, anonymisierte Informationen sind nicht durch die DSGVO geschützt, da die Kosten und der Zeitaufwand zur Identifizierung von natürlichen Personen unverhältnismäßig hoch wären.⁷⁴⁷

Die Ethik hingegen sieht keine Ausnahmen vor. Prinzipiell sollten Datenquellen immer die Kontrolle darüber haben, mit wem sie welche Informationen zu welchem Zweck teilen. Durch breite Zustimmung zu verschiedenen potenziellen Verarbeitungszwecken verlieren Menschen jedoch die Kontrolle über die Verwendung ihrer Daten. Wenn die Daten für unbekannte Zwecke verwendet werden, können die Datenquellen nicht mehr kontrollieren, mit wem sie welche Informationen zu welchem Zweck teilen. Laut DSGVO soll die Anonymisierung von Informationen ein wirksames Mittel zum Schutz der Privatsphäre sein.⁷⁴⁸ Aus der ethischen Perspektive unterstützt das Anonymisieren von Daten den Schutz von Individuen allerdings nicht ausreichend, da nur die vermeintlich personenbezogenen Informationen gelöscht (oder bei Pseudonymisierung separat gespeichert)⁷⁴⁹ werden. Jedoch müssen Informationen nicht personenbezogen sein, um durch ihre Verarbeitung eine Gefahr für ein Individuum darzustellen.⁷⁵⁰ Denn es ist möglich, dass aus nicht-persönlichen Informationen, dann doch persönliche Informationen über geschützte Merkmale abgeleitet werden.⁷⁵¹ Ein hoher Kosten-

745 Erwägungsgrund 33 DSGVO

746 BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83

747 Erwägungsgrund 26 DSGVO

748 Ebd.

749 Wimmer 2019

750 Martani, Hummel 2022:37

751 Ebd.:34; Manson, O'Neill 2007:104; Wachter, Mittelstadt 2019:564

und Zeitaufwand hält die Ethik nicht davon ab, diese Möglichkeit zu problematisieren.

Die DSGVO als aktueller rechtlicher Rahmen bildet die Mindestanforderungen der Ethik weitestgehend gut ab. Denn auch die ethische Erörterung der Privatsphäre in Bezug auf Datenverarbeitung ergibt, dass die Datenquellen geschützt werden sollten. Die DSGVO setzt das um, indem das Verhalten der Datengenerierenden reguliert wird. Die ethische Analyse sieht vor, dass Außenstehende bei Individuen keinen Kontrollverlust verursachen dürfen, indem sie bewusst versuchen, auf persönliche Informationen des Individuums zuzugreifen und diese zu benutzen oder tatsächlich zugreifen, auch aus Versehen, ohne dass das Individuum darüber die Kontrolle hat. Außerdem sollten Außenstehende nicht durch fahrlässiges Handeln Beihilfe zur Privatsphärenverletzung leisten, indem sie das Individuum dem substanziell größeren Risiko aussetzen, dass eine andere außenstehende Person auf seine persönlichen Informationen zugreift. Denn Datengenerierende haben eine moralische Pflicht zum Schutz der individuellen Privatsphäre. Deshalb ist es wichtig, dass die Handlungen und die Kommunikation, die zur Beschaffung von persönlichen Informationen, sowie für die Verwendungen von solchen Informationen genutzt werden, moralisch zulässig sind.⁷⁵² In der DSGVO geht es nicht vorrangig um die moralische Zulässigkeit der mit Datenverarbeitung verbundenen Handlungen und Kommunikation – es geht um die rechtliche Zulässigkeit. In Bereichen wie der Zweckgebundenheit der Verarbeitung oder dem Schutz von anonymisierten Daten wäre die Ethik strenger als das geltende Recht. Trotzdem bietet die DSGVO eine gute Grundlage für die ethische Regulierung von Datenverarbeitung. Denn durch diese Verordnung wurde die moralische Pflicht zum Schutz der Privatsphäre in juristisches Recht gegossen.

752 Manson, O'Neill 2007:110

6.4 Aus der Pflicht zum Schutz der Privatsphäre abgeleitete Anforderungen

In diesem Kapitel ist klar geworden, dass Datengenerierende zum Schutz der Privatsphäre der Datenquellen moralisch verpflichtet sind, und dass die Privatsphäre der Datenquellen aber auf Grund des geplanten oder tatsächlichen Zugriffs auf ihre Daten ohne ihre Wahl-Kontrolle verletzt werden kann. Die Verletzung der Privatsphäre kann auf Grund ihrer unerwünschten Folgen von ungewollten Eingriffen und fehlender Autonomie als Risikoauferlegung bezeichnet werden. Mit Hilfe der deontologischen Risikoethik lässt sich deshalb argumentieren, dass diese Risikoauferlegung nur im Rahmen eines gerechten sozialen Systems der Risikobereitschaft geschehen darf, welche allen Beteiligten zum Vorteil gereicht.⁷⁵³ Das bedeutet, durch die Regel der dritten Formel des Kategorischen Imperativs von Kant, dass niemand als bloßes Mittel gebraucht werden darf.⁷⁵⁴ Das heißt in der Praxis, die individuelle Kontrolle der Datenquellen über das Risiko sollte so groß wie möglich sein. Dafür sollten die Risikoexponierten ohne Täuschung über das Risiko informiert werden und ohne Zwang die Wahl haben, ob sie das Risiko tragen wollen. Auf diese Weise kann die Privatsphäre sowohl geschützt als auch gefördert werden.

Aus der Definition von Privatsphäre als Wahl-Kontrolle des Individuums über Zugang zu und Benutzung von seinen persönlichen Informationen lassen sich Anforderungen an den Umgang mit Daten und insbesondere mit den Datenquellen im Datenökosystem ableiten. Wie in Tabelle 3 zu sehen ist, drückt die Definition zwei Ziele aus: Ein Individuum sollte die Wahl-Kontrolle sowohl über den Zugang zu als auch die Benutzung von seinen persönlichen Informationen haben. Da Wahl-Kontrolle bedeutet, dass man entscheiden kann, mit wem man welche Informationen zu welchem Zweck teilt, sollten die betroffenen Personen also einerseits entscheiden können, wer Zugriff auf welche Informationen bekommt. Andererseits sollten die betroffenen Individuen entscheiden können, zu welchem Zweck ihre Informationen gesammelt oder verarbeitet werden. Administrativ bedeutet das, dass einerseits das Einverständnis der Individuen

753 Hansson 2003:305

754 Kant 2008: 65 [429]

eingeholt werden sollte, und die Individuen andererseits über jeden Verwendungszweck der Daten informiert sowie die Daten vor Zweckentfremdung geschützt werden sollten.

Tabelle 3 Administrative Anforderungen für die Umsetzung von Privatsphäre⁷⁵⁵

Privatsphäre Definition	Privatsphäre Ziele	Umsetzung des Ziels	Administrative Anforderungen
Privatsphäre = Wahl-Kontrolle des Individuums über Zugang zu und Benutzung von seinen persönlichen Informationen	Das Individuum hat die Wahl-Kontrolle über den <i>Zugang</i> zu seinen persönlichen Informationen	Das Individuum kann entscheiden, wer <i>Zugriff</i> auf welche Informationen bekommt	<i>Einverständnis</i> der Individuen wird eingeholt
			Gewährleistung von <i>Freiwilligkeit</i> der Einwilligung
	Das Individuum hat die Wahl-Kontrolle über die <i>Benutzung</i> von seinen persönlichen Informationen	Das Individuum kann entscheiden, zu welchem <i>Zweck</i> seine Informationen gesammelt oder verarbeitet werden	Individuen werden über alle Verwendungszwecke <i>informiert</i>
			Gewährleistung von <i>Zweckentsprechung</i> der Informationen

Diese administrativen Anforderungen sorgen dafür, dass die Datenquellen in Bezug auf den Umgang mit ihren Daten im Datenökosystem selbstbestimmt handeln können und sie somit nicht als bloßes Mittel gebraucht werden. Da die Auferlegung eines Risikos nur dann zulässig ist, wenn niemand als bloßes Mittel gebraucht wird, ist die Erfüllung der administrativen Anforderungen eine notwendige Bedingung für die Zulässigkeit der Risikoauferlegung.

Aus dem Prinzip der Privatsphäre lässt sich also die Anforderung ableiten, dass Individuen sowohl nach ihrem Einverständnis gefragt werden, bevor ihre Informationen gesammelt und gespeichert werden als auch, dass Individuen vorher darüber informiert werden, zu welchem Zweck ihre Informationen gesammelt, gespeichert und verarbeitet werden. Die in der DSGVO verankerte Anforderung der informierten Einwilligung lässt sich also direkt aus der Definition von Privatsphäre als Wahl-Kontrolle über Zugang zu und Benutzung

755 Eigene Darstellung

von persönlichen Informationen ableiten. Während aber gemäß der DSGVO auch Verträge, öffentliches Interesse oder lebenswichtige Interessen rechtmäßige Gründe zur Datenverarbeitung sein können, handelt es sich aus ethischer Sicht immer dann um eine Verletzung der Privatsphäre, wenn Außenstehende auf persönliche Informationen des Individuums zugreifen, ohne dass das Individuum darüber die Wahl-Kontrolle hat.

In einem Datenökosystem sind Datenquellen dem Risiko ausgesetzt, dass ihre Privatsphäre verletzt wird, weil ihnen oft die Kontrolle über den Zugang zu und die Benutzung ihrer persönlichen Informationen fehlt. Diese Situation wird durch epistemische Asymmetrie erzeugt, da die Datenquellen in der Realität oft nicht wissen, wer zu welchen Zwecken ihre Informationen sammelt und auswertet. Wenn zum Beispiel ein Supermarkt das Kaufverhalten seiner Kundinnen beobachtet, um herauszufinden, welche von ihnen schwanger ist, ohne die Kundinnen zu informieren und um ihr Einverständnis zu bitten, dann fehlt den Kundinnen das Wissen darüber, dass ihre Privatsphäre verletzt wird. Aber, selbst wenn die Kundinnen informiert sind, können die Informationen über ihr Kaufverhalten trotzdem ohne ihr Wissen zweckentfremdet werden. Durch dieses fehlende Wissen über den Umgang von Außenstehenden mit den eigenen Daten ist es wahrscheinlicher, dass die Privatsphäre von Datenquellen tatsächlich verletzt wird. Denn die Privatsphäre als Wahl-Kontrolle über Zugang zu und Benutzung von persönlichen Informationen wird verletzt, wenn die Datenquellen gar nicht wissen, dass Zugang zu und Benutzung von ihren Informationen stattfindet.

Das fehlende Wissen und die dadurch mögliche Verletzung der Privatsphäre werden durch die Struktur eines Datenökosystems begünstigt. Denn Datengenerierende sind zu einem gewissen Grad dazu in der Lage, die für Datenquellen verfügbaren Beweise in Bezug darauf, was mit den Daten passiert, zu kontrollieren – das ermöglicht epistemische Dominanz.⁷⁵⁶ Epistemische Dominanz kann bössartig sein, wenn der dominierte Akteur absichtlich daran gehindert wird, epistemisch wertvolle Zustände zu erreichen. Aber wenn die dominierenden Akteure wohlmeinend und gut informiert sind, kann

756 Harris 2022:134, 137

das den dominierten Akteuren epistemisch zugutekommen.⁷⁵⁷ Aus der Pflicht zum Schutz der Privatsphäre entsteht auch eine Pflicht des dominierenden Akteurs, wohlmeinend zu sein. Wenn die Privatsphäre nicht geschützt wird oder sogar durch bössartige epistemische Dominanz verletzt wird, besteht das Risiko, dass die betroffenen Individuen neben dem Kontrollverlust noch weitere Schäden erleiden durch zum Beispiel Diskriminierung oder eine Einschränkung ihrer Autonomie. Angenommen, wir wollen in einer Welt leben, in der sich die Menschen nicht gegenseitig Schaden zufügen, so sollte epistemische Dominanz nicht bössartig ausgenutzt werden, um möglichst die Verletzung von Privatsphäre zu vermeiden.

Mainz und Uhrenfeldt sind der Meinung, dass die Verletzung der Privatsphäre aus gewichtigeren Gründen, die nichts mit der Privatsphäre zu tun haben, gerechtfertigt sein kann.⁷⁵⁸ Da die Datenquellen bei der Verletzung ihrer Privatsphäre jedoch Risiken ausgesetzt werden, ist eine solche Verletzung nur unter den Bedingungen der deontologischen Risikoethik zulässig – unabhängig davon, wie gewichtig die Gründe sind. Solange die administrativen Anforderungen eingehalten werden, kann die Risikoexposition der Datenquellen im Datenökosystem, in Form von der Verletzung ihrer Privatsphäre, Teil eines gerechten sozialen Systems der Risikobereitschaft sein. Als nächstes ist es wichtig, auch das Risiko zu betrachten, dem die Datennutzenden im Datenökosystem ausgesetzt sind.

757 Harris 2022:136f., 139

758 Mainz, Uhrenfeldt 2021:295, Fußnote 18

