11 Fazit für die ethische Gestaltung im Umgang mit digitalen Daten

In dieser Arbeit wurde gezeigt, wie der Umgang mit digitalen Daten in Datenökosystemen ethisch gestaltet werden kann. Begonnen wurde mit der Erkenntnis, dass Datenökosysteme als ein System von Akteuren, zwischen denen mit Hilfe von technologischen Mitteln Daten fließen, verstanden werden kann. Allein auf Grund der Struktur, den Beziehungen zwischen den Akteuren, werden ihnen unterschiedlich viel Wissen und Kontrolle über den Datenfluss im Datenökosystem ermöglicht. *Datenquellen* stellen ihre Daten zur Verfügung, *Datengenerierende* sammeln und speichern die Daten, *Datenverarbeitende* kombinieren und analysieren die Daten, um sie dann aufbereitet als Ergebnisse zur Verfügung stellen zu können, und *Datennutzende* arbeiten mit den aufbereiteten Daten, bzw. sie sind auf diese Daten angewiesen. Datengenerierende und Datenverarbeitende sind dabei die Akteure mit mehr Wissen und Kontrolle, da sie wissen und bestimmen können, was mit den Daten passiert. Dadurch wurde klar, dass der Umgang mit digitalen Daten im Datenökosystem eine Risikoauferlegung für Datenquellen und Datennutzende beinhaltet. Denn Datenquellen können nicht kontrollieren, was mit ihren Daten geschieht, sodass ihnen bei der Datensammlung das Risiko der Verletzung ihrer Privatsphäre und somit ein Verlust von Autonomie auferlegt wird. Datennutzende können hingegen nicht nachvollziehen, wie die Ergebnisse der Datenverarbeitung zustande gekommen sind, sodass ihnen bei der intransparenten Bereitstellung der Ergebnisse das Risiko auferlegt wird, auf dieser Grundlage zu falschen Überzeugungen zu gelangen und somit nicht für ihre Interessen einstehen zu können.

Da diese Risikoauferlegung, sobald sie entgegen der Wünsche der Risikoexponierten geschieht, deren Autonomie beschränken kann, entsteht ein ethisches Problem. Um den Umgang mit Daten im Datenökosystem trotzdem ethisch gestalten zu können, wurde in dieser Arbeit erörtert, wann es zulässig ist, anderen ein Risiko auf-

zuerlegen – nämlich nur dann, wenn die Risikoauferlegung Teil eines gerechten sozialen Systems der Risikobereitschaft ist, von dem alle profitieren und in dem niemand als bloßes Mittel gebraucht wird. Der Kategorische Imperativ von Kant verbietet aber nicht nur den Gebrauch anderer als bloßes Mittel, sondern auch bestimmte Handlungsfolgen, die durch den Umgang mit Daten in einem Datenökosystem riskiert werden: die Verletzung der Privatsphäre und das Fehlen von Transparenz.

Es ließ sich in dieser Arbeit argumentativ nachweisen, dass die Privatsphäre der Datenquellen durch den Zugriff auf ihre Daten ohne ihre Wahl-Kontrolle verletzt werden kann. Diese Verletzung der Privatsphäre würde bedeuten, dass die Datenquellen der Gefahr von Erpressung, staatlicher Kontrolle oder kommerzieller Ausbeutung sowie Autonomieverlust ausgesetzt wären. Das wäre ein unerwünschtes Ereignis, da dies zu ungewollten Übergriffen oder Diskriminierung führen kann und weil eine intakte Privatsphäre eine unbedingte Voraussetzung für ein autonomes Leben ist. Da dieses unerwünschte Ereignis der Privatsphärenverletzung nur mit einer gewissen Wahrscheinlichkeit eintritt, kann sie als Risiko bezeichnet werden.

Außerdem konnte argumentativ nachgewiesen werden, dass Datennutzenden auf Grund der epistemischen Asymmetrie in Datenökosystemen Transparenz verwehrt werden kann, indem die Information, wie die Ergebnisse der Datenverarbeitung zustande gekommen sind, verwehrt wird. Die Unmöglichkeit, die Ergebnisse zu überprüfen, ist aus einer epistemischen Perspektive problematisch, weil verzerrte Ergebnisse zu falschen Überzeugungen führen können. Dies sollte aus ethischer Sicht vermieden werden, da es für das menschliche Wohlergehen wichtig ist, sich von richtigen und nicht von falschen Überzeugungen leiten zu lassen und das Wissen darüber notwendig ist, um seine eigenen Interessen vertreten zu können. Da es bei fehlender Transparenz jedoch möglich ist, dass Datennutzende vorsätzlich falsch informiert oder durch verzerrte Ergebnisse unabsichtlich unfairen Entscheidungen ausgesetzt werden, handelt es sich hier ebenfalls um unerwünschte Ereignisse, die mit einer gewissen Wahrscheinlichkeit eintreten können, und damit um ein Risiko.

Das heißt, die Privatsphäre der Datenquellen und die Transparenz für die Datennutzenden können durch die Datenverarbeitung im

Datenökosystem gefährdet werden – das sollten sie aber nicht. Es kann nicht gewollt werden, dass Datenquellen und Datennutzenden diese Risiken auferlegt werden, deshalb entsteht eine moralische Pflicht für Datengenerierende und Datenverarbeitende, dies zu vermeiden. Da aber eine Auferlegung von Risiken nicht immer vermeidbar ist, kann mit Hilfe der in dieser Arbeit entwickelten deontologischen Risikoethik erörtert werden, unter welchen Bedingungen sie trotzdem ethisch zulässig sein kann. So stellt sich heraus, dass durch die Einhaltung einiger administrativer Anforderungen die Privatsphäre der Datenquellen und die Transparenz für die Datennutzenden im Datenökosystem geschützt und gefördert werden können:

Administrative Anforderungen für die Umsetzung von Privatsphäre:

- *Einverständnis* der Individuen wird eingeholt
- Gewährleistung von *Freiwilligkeit* der Einwilligung
- Individuen werden über alle Verwendungszwecke *informiert*
- Gewährleistung von *Zweckentsprechung* der Informationen

Administrative Anforderungen für die Umsetzung von Transparenz:

- *Entstehung* des Ergebnisses verstehen: Welcher Input führt zu welchem Output und welche Trainingsdaten wurden verwendet?
- Algorithmische Ergebnisse im zum Verständnis notwendigen *Kontext* darstellen.

Da die Auferlegung eines Risikos nur dann zulässig ist, wenn niemand als bloßes Mittel gebraucht wird und die administrativen Anforderungen dafür sorgen, dass die Selbstbestimmung der Akteure ermöglicht wird und sie somit nicht als bloßes Mittel gebraucht werden, ist die Erfüllung der administrativen Anforderungen eine notwendige Bedingung für die Zulässigkeit der Risikoauferlegung.

Als nächstes wurde gezeigt, dass aus einer Position der erhöhten Kontrolle über die Datenverarbeitung innerhalb eines Datenökosystems Verantwortung erwächst für die Minimierung der Risiken und das Erzeugen von positiven Ergebnissen. Denn es ließ sich argumentativ nachweisen, dass Datengenerierende und Datenverarbeitende auf Grund ihrer erhöhten Kontrolle innerhalb des Datenökosystems Verantwortung tragen für den Schutz und die Förderung der Privatsphäre der Datenquellen und der Transparenz für die Datennut-

zenden. Somit ist offensichtlich, wer für die ethische Gestaltung von Datenökosystemen zuständig ist. Wie diese Gestaltung aussehen soll, wurde anhand der aus der Arbeit abgeleiteten Kriterien für die ethische Gestaltung erwogen. Nur die Ethischen Leitlinien und die ethische Risikoanalyse von Hansson erfüllen alle Kriterien für die ethische Gestaltung einer Technologie:

i) Die Umsetzungsmethode sollte konkrete praktische Anleitung bieten.
ii) Die Umsetzungsmethode sollte den Einfluss der Technologie auf alle Betroffenen berücksichtigen.
iii) Im Rahmen der Umsetzungsmethode sollte die Verantwortung für die Umsetzung der ethischen Überlegungen bestimmten menschlichen Akteuren zugeordnet werden.

Erst wenn diese vier Kriterien alle erfüllt sind, kann in Betracht gezogen werden, dass der jeweilige Ansatz zur Ausrichtung technischer Entwicklungen an ethischen Maßstäben auch für die ethische Gestaltung eines Datenökosystems geeignet ist. Allerdings erfüllen die beiden Ansätze, die sich zur Gestaltung einer Technologie eignen würden, nicht alle Kriterien für die ethische Gestaltung eines Datenökosystems:

I. Die Umsetzungsmethode sollte es ermöglichen, die Auferlegung von Risiken zu regulieren.
II. Die Umsetzungsmethode sollte es ermöglichen, die administrativen Anforderungen zur Umsetzung von Privatsphäre für die Datenquellen zu erfüllen.
III. Die Umsetzungsmethode sollte es ermöglichen, die administrativen Anforderungen zur Umsetzung von Transparenz für die Datennutzenden zu erfüllen.

Denn die Umsetzungsmethode der Ethischen Leitlinien ermöglicht es nicht, die Risikoauferlegung zu problematisieren und dementsprechend die Auferlegung von Risiken in der Praxis regulieren (I). Die ethische Risikoanalyse ermöglicht es zwar die Risikoauferlegung zu problematisieren, aber sie beantwortet die Frage, unter welchen Umständen das Risiko zulässig ist, nur mit einem Risikotausch, der für alle Beteiligten von Vorteil ist. Da es für eine zulässige Risikoauferlegung nicht reicht, wenn ein Risiko durch einen eigenen Vorteil kompensiert wird, reicht diese Antwort auch nicht, um die Auferlegung

von Risiken regulieren zu können (I). Deshalb habe ich aus den Erkenntnissen der bisherigen Arbeit und auf Grundlage der ethischen Risikoanalyse von Hansson einen eigenen ethischen Verfahrensmaßstab entwickelt, der die Frage beantwortet, wie Datenökosysteme gestaltet werden sollen. Durch die Anwendung der folgenden vier Schritte ist es den Argumenten in dieser Arbeit zufolge möglich, ein Datenökosystem ethisch zu gestalten:

Schritt 1: Positionierung zu Verantwortung, Nutzen und Risiken
Schritt 2: Risikoverteilung bewerten mit Hanssons ethischer Risikoanalyse
Schritt 3: Überprüfung der Zulässigkeit von Risikoauferlegung
Schritt 4: Fehlervorsorge durch Minimierung der Risiken

Aus der ethischen Erkenntnis, dass Risiken nur dann auferlegt werden dürfen, wenn dadurch niemand als bloßes Mittel gebraucht wird, und aus den Konzepten der Privatsphäre und der Transparenz abgeleiteten administrativen Anforderungen wurde eine Umsetzungsmethode entwickelt, die es ermöglicht, bei der Gestaltung eines Datenökosystems und seiner technischen Einzelelemente die ethischen Anforderungen einzubinden.

Die beiden Forschungsfragen aus der Einleitung wurden in dieser Arbeit beantwortet:

1. Wie lassen sich Datenökosysteme ethisch bewerten?
2. Wie sollten Datenökosysteme dementsprechend gestaltet werden?

Zur Beantwortung der ersten Forschungsfrage wurde argumentiert, dass sich Datenökosysteme am besten mit Hilfe der deontologischen Risikoethik ethisch bewerten lassen. Dies war möglich, weil anhand der Struktur von Datenökosystemen erkennbar wurde, dass die Akteure unterschiedlich viel Wissen und Kontrolle haben und zudem das Sammeln und Verarbeiten von Daten im Datenökosystem als Risikoauferlegung verstanden werden muss. Von den drei dargestellten klassischen Moraltheorien hat es nur die kantianische Deontologie ermöglicht:

a. das asymmetrische Wissen sowie die ungleiche Kontrolle der Akteure im Datenökosystem zu betrachten und
b. das Auferlegen der Risiken zu bewerten.

Im Datenökosystem ist es also dann zulässig, Datenquellen und Datennutzenden Risiken aufzuerlegen, wenn sie dabei nicht als bloßes Mittel gebraucht werden. Das heißt, solange die individuelle Kontrolle so groß wie möglich ist, weil die Risikoexponierten ohne Täuschung über das Risiko informiert werden und ohne Zwang die Wahl haben, ob sie das Risiko tragen wollen, lassen sich Datenökosysteme ethisch als zulässig einstufen.

Die zweite Forschungsfrage wurde mit der Entwicklung des ethischen Verfahrensmaßstabs beantwortet. Datenökosysteme sollten entsprechend meines ethischen Verfahrensmaßstabs gestaltet werden, da dieser Vorschlag zur Umsetzung digitaler Ethik in die Praxis gut geeignet ist, um ethische Probleme im Zusammenhang mit der Datenverarbeitung in Datenökosystemen zu adressieren. Denn durch meinen ethischen Verfahrensmaßstab können einerseits die Risiken des Datenökosystems minimiert werden, andererseits kann dadurch die aktive Gestaltung von Datenökosystemen an der deontologischen Risikoethik orientiert werden, um die Ungleichheit des Wissens und der Kontrolle über Risiken möglichst auszugleichen.

Meine Arbeit leistet in dreierlei Hinsicht einen neuen Beitrag zur Forschung im Bereich der digitalen Ethik:

- mit der Entwicklung der deontologischen Risikoethik,
- mit dem Erarbeiten der administrativen Anforderungen und
- mit dem daraus abgeleiteten ethischen Verfahrensmaßstab.

Mit Kants dritter Formel des Kategorischen Imperativs habe ich eine Antwort gefunden auf die Frage, wann es zulässig ist, anderen ein Risiko aufzuerlegen. Das Prinzip von Hansson war dabei eine wichtige Grundlage. Ich baue darauf auf, dass jede Risikoauferlegung nur zulässig ist als Teil eines gerechten sozialen Systems der Risikobereitschaft, das auch den Risikoexponierten zum Vorteil gereicht.[1451] Dieses System soll laut Hansson Regeln enthalten, die bestimmte Arten von risikobehafteten Aktivitäten zulassen – er stellt jedoch nur die Regel auf, dass die Risikoauferlegung für alle Beteiligten von Vorteil muss. Da ich aber der Ansicht bin, dass es für eine zulässige Risikoauferlegung nicht reicht, wenn ein Risiko durch einen eigenen Vorteil kompensiert wird, habe ich die dritte Formel des Kategori-

1451 Hansson 2003:305

schen Imperativs von Kant als eine weitere Regel vorgeschlagen. Dadurch ist es nun möglich, eine klare Antwort auf die Frage zu geben, unter welchen Bedingungen es zulässig ist, andere einem Risiko auszusetzen. Hierdurch lassen sich auch konkrete administrative Anforderungen zum Schutz vor bestimmten Risiken ableiten.

Die administrativen Anforderungen zur Umsetzung von Privatsphäre und Transparenz wurden in dieser Arbeit aus den ausführlichen Definitionen dieser Konzepte und dem normativen Anspruch an ihren Schutz abgeleitet. Durch die Begriffsdefinitionen wurde klar, unter welchen Umständen Privatsphäre intakt bzw. verletzt ist und wie Transparenz überhaupt ermöglicht werden kann bei der Bereitstellung von algorithmischen Ergebnissen. Dank der Begründung einer Pflicht zum Schutz der Privatsphäre und der Bereitstellung von transparenten Ergebnissen konnte geschlussfolgert werden, dass sowohl der Schutz der Privatsphäre als auch die Bereitstellung von transparenten Ergebnissen in der Praxis gewährleistet werden sollten. Die administrativen Anforderungen liefern also eine Antwort auf die Frage, unter welchen Bedingungen die Privatsphäre intakt und die Transparenz gesichert ist. Somit sind die Anforderungen an eine ethische Gestaltung gut begründet.

Unter anderem dadurch wurde auch der Umsetzungsvorschlag für die Praxis in dieser Arbeit ausführlich theoretisch hergeleitet. Denn die Kriterien für die ethische Gestaltung eines Datenökosystems wurden aus der deontologischen Risikoethik und den administrativen Anforderungen abgeleitet. Zuvor sollten aber noch die allgemeineren Kriterien für die ethische Gestaltung von Technologien erfüllt sein. Auch diese stammen aus gut begründeten theoretischen Überlegungen zur Ausrichtung technischer Entwicklungen an ethischen Maßstäben. Denn diese ist nur möglich, wenn konkrete praktische Anleitung gegeben ist, es spezifische und gut begründete ethische Anforderungen an die Gestaltung gibt, der Vorteil für alle von der Technologie betroffenen Personen das Ziel ist und die Verantwortung für die ethische Gestaltung des Datenökosystems einem bestimmten menschlichen Akteur zugeordnet ist. Dadurch konnte ein ethischer Verfahrensmaßstab auf Grundlage der ethischen Risikoanalyse von Hansson aufgestellt werden, der konkrete praktische Anleitung bietet, dabei den Einfluss der Technologie auf alle Betroffenen berücksichtigt und für dessen Anwendung das zu diesem Zweck aufzustellende Ethikteam verantwortlich ist. Dank diesem

ethischen Verfahrensmaßstabs ist es auch möglich, die Auferlegung von Risiken zu regulieren und die administrativen Anforderungen zur Umsetzung von Privatsphäre für die Datenquellen und zur Umsetzung von Transparenz für die Datennutzenden zu erfüllen. Somit wurde in dieser Arbeit nicht nur ein theoretischer Beitrag geleistet, sondern es wurde mit dem ethischen Verfahrensmaßstab auch eine Möglichkeit zur praktischen Umsetzung dieser theoretischen Überlegungen geschaffen.

In dieser Arbeit habe ich mich der besten Eigenschaften der von Bolte und van Wynsberghe sogenannten zweiten und dritten Welle der KI-Ethik bedient. Einerseits beschäftige ich mich, wie die zweite Welle, mit den konkreten Risiken, die aktuell durch den Umgang mit Daten entstehen. Andererseits nutze ich, wie die dritte Welle, zur Analyse dieser Risiken einen strukturellen Ansatz. Denn es ging in dieser Arbeit nicht um einzelne Technologien, sondern um die Struktur von Datenökosystemen, in denen sie angewendet werden. Dabei verfolge ich, ebenfalls wie die dritte Welle, einen systemisch orientierten Ansatz, der ethische Fragestellungen auf struktureller Ebene sichtbar macht. So wurde deutlich, dass der Umgang mit Daten im Datenökosystem als Risikoauferlegung verstanden werden kann und sich dementsprechend die Frage stellt, wann eine solche Risikoauferlegung ethisch zulässig ist. Um diese ethischen Überlegungen zu realisieren, setze ich, wie die zweite Welle, auf einen durchdachten Gestaltungsprozess, um sozio-technische Strukturen zu verändern. Dabei gehe ich nicht davon aus, dass sich ethische und strukturelle Probleme allein durch Verbesserungen einzelner Anwendungen lösen lassen und distanziere mich somit von dem Techno-Solutionismus der zweiten Welle – vielmehr lassen sich die Probleme durch Kommunikation über die Zwecke der Datenverarbeitung und die Aussagekraft der Ergebnisse lösen. Ebenso vertrete ich auch nicht die Auffassung der dritten Welle, dass erst umfassende strukturelle Veränderungen notwendig sind, bevor Technologie ethischer gestaltet werden kann – es ist schon jetzt möglich, Datenquellen und Datennutzende nicht im Ungewissen über Pläne und Vorgehensweisen zu lassen.

Das OZG und die laufende Digitalisierung der Verwaltungsdienstleistungen in Deutschland bieten in dieser Arbeit hilfreiche Beispiele zur Veranschaulichung der theoretischen Überlegungen. Das bedeu-

tet jedoch nicht, dass die erarbeitete Theorie sowie der ethische Verfahrensmaßstab ausschließlich zur Anwendung im Verwaltungskontext geeignet sind. Der ethische Verfahrensmaßstab kann für die Gestaltung jeglicher Datenökosysteme angewandt werden. Dabei ist jedoch zu beachten, dass die Gruppenprivatsphäre womöglich neue administrative Anforderungen an die Gestaltung verlangt. Denn sobald Datenverarbeitende Gruppenprofile erstellen, um Werbung oder die Bepreisung von Produkten personalisieren zu können, reicht die Berücksichtigung der individuellen Privatsphäre nicht mehr zum Schutz vor Ungleichbehandlung. Das heißt, je nach Kontext des Datenökosystems, sollte die Gruppenprivatsphäre beim Minimieren des Risikos in Schritt 4 des ethischen Verfahrensmaßstabs Beachtung finden.

In unterschiedlichen Kontexten mag es unterschiedliche Probleme bei der Umsetzung von Bedingungen für ein gerechtes soziales System der Risikobereitschaft geben. Zum Beispiel ist im Kontext medizinischer Forschung die von mir geforderte individuelle Einwilligung oft nur schwer umsetzbar. Während im Verwaltungskontext jeder Antrag einzeln bearbeitet werden muss und es somit möglich ist, jede antragstellende Person nach der Einwilligung zur Nutzung ihrer Daten zu fragen, ist es in der medizinischen Forschung wichtig, so viele Daten wie möglich zu sammeln, damit ihre Analyse aussagekräftig ist. Das heißt, die administrativen Anforderungen zum Schutz der Privatsphäre sind im Kontext der Verwaltung umsetzbar, können jedoch in anderen Kontexten Anpassungen erfordern. In jedem Fall gilt das Prinzip der Maximierung der individuellen Kontrolle – seine Umsetzung kann aber in verschiedenen Kontexten unterschiedlich ausgestaltet werden. Das heißt, bei der Anwendung meines ethischen Verfahrensmaßstabs in anderen Kontexten, wie zum Beispiel medizinischer Forschung, können im Rahmen der Kontrollmaximierung durch Informationen und Kompensation Lösungen gefunden werden.

In Bezug auf die Transparenz wurde in dieser Arbeit zwar davon ausgegangen, dass der Einsatz von Black Box KI-Algorithmen (KI-Systeme) für die Datennutzenden ein besonders großes Risiko erzeugt, aber auch wenn die bereitgestellten Ergebnisse für die Datenverarbeitenden nachvollziehbar sind, gelten die gleichen administrativen Anforderungen an die Umsetzung der Transparenz. Insbesondere wenn sich die Ergebnisse auf Personen beziehen, ist ihre

Nachvollziehbarkeit ethisch geboten, damit Einspruch erhoben und die eigenen Interessen vertreten werden können. Aus epistemischer Sicht ist aber auch unabhängig von Personen die Transparenz essentiell für jeglichen Erkenntnisgewinn. Das heißt, die Anforderungen an die Transparenz können auch hilfreich sein für Datenökosysteme, die sich nicht auf Personen beziehen.

Auch die in dieser Arbeit entwickelte deontologische Risikoethik lässt sich über den Verwaltungskontext und Datenökosysteme hinaus auf jegliche Risikoauferlegung anwenden. Immer wenn sich die Frage stellt, unter welchen Bedingungen es zulässig ist, andere einem Risiko auszusetzen, bietet die deontologische Risikoethik eine Antwort. Denn aus meiner Sicht ist ein System der Risikobereitschaft nur dann gerecht und sozial und gereicht allen zum Vorteil, wenn die Regel gilt, dass niemand als bloßes Mittel gebraucht wird. Deshalb kann dieser Ansatz in jeglichem Kontext hilfreich sein, wenn es darum geht, die ethische Zulässigkeit von Risikoauferlegung einzuschätzen.

Diese Arbeit bietet eine Grundlage, um bewusst zu reflektieren, welche Ziele bei der Gestaltung von Datenökosystemen gefördert werden sollten. Sie liefert damit einen normativen Orientierungsrahmen für die ethische Gestaltung von Datenökosystemen – jenseits technischer Einzellösungen und unter Berücksichtigung struktureller Bedingungen. Somit trägt diese Arbeit mit Hilfe von vertieften theoretischen Erörterungen dazu bei, technische Entwicklungen in der Praxis an ethischen Maßstäben auszurichten. Es lässt sich aus den Ergebnissen schließen, dass es unter bestimmten Bedingungen möglich ist, Datenökosysteme ethisch zu gestalten und wie diese Bedingungen hergestellt werden können. Die Umsetzung dieser Bedingungen ermöglicht es zum Beispiel, dass wir online einen neuen Ausweis beantragen oder unseren Wohnsitz ummelden können, und uns die dabei entstehenden Risiken nur unter zulässigen Bedingungen auferlegt und unsere Privatsphäre sowie die Transparenz der Ergebnisse geschützt und gefördert werden.