Recht der Informationsgesellschaft 44

Benjamin Manthey

Das datenschutzrechtliche Transparenzgebot

Die Grenzen des individuellen Datenschutzes anhand verdeckter Datenverarbeitungen im Internet

Nomos

Recht der Informationsgesellschaft

herausgegeben von

Prof. Dr. Jörg Fritzsche, Universität Regensburg, Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht
Prof. Dr. Jürgen Kühling, LL.M., Universität Regensburg, Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht
Prof. Dr. Gerrit Manssen, Universität Regensburg, Lehrstuhl für Öffentliches Recht, insbesondere deutsches und europäisches Verwaltungsrecht
Prof. Dr. Robert Uerpmann-Wittzack, Maître en droit, Universität Regensburg, Lehrstuhl für Öffentliches Recht und Völkerrecht

Band 44

Benjamin Manthey

Das datenschutzrechtliche Transparenzgebot

Die Grenzen des individuellen Datenschutzes anhand verdeckter Datenverarbeitungen im Internet

Nomos

Onlineversion
Nomos eLibrary

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Regensburg, Univ., Diss., 2019

ISBN 978-3-8487-6712-0 (Print)
ISBN 978-3-7489-0833-3 (ePDF)

Die Bände 1 bis 33 sind im Lit-Verlag erschienen.

1. Auflage 2020

Inhaltsverzeichnis

Erster Teil:
Das Transparenzgebot – Zukunftsweisende Grundlage oder obsoletes Relikt des Datenschutzrechts?

Zweiter Teil:
Grundlagen

Dritter Teil:
Rechtliche Bewertung der Transparenz der Datenverarbeitung

Vierter Teil:
Grenzen und Potenzial des Transparenzgebots

Diese Arbeit wurde im Wintersemester 2019/2020 von der Fakultät für Rechtswissenschaften der Universität Regensburg als Dissertation angenommen. Rechtsprechung und Schrifttum konnten bis Juni 2019 berücksichtigt werden.

Besonderer Dank gebührt meinem Doktorvater, Herrn Professor Dr. Robert Uerpmann-Wittzack, für die Betreuung und Förderung der Arbeit in allen Stadien. Fragen konnten über die Dauer der Bearbeitung immer zeitnah geklärt werden und der nötige Freiraum für die Bearbeitung war stets persönlich wie fachlich gegeben. Ebenso gebührt besonderer Dank Herrn Professor Dr. Kühling für die Bereitschaft das Zweitgutachten zu verfassen und für dessen zügige Erstellung.

Dank gebührt Frau Professorin Dr. Andrea Edenharter, meiner nicht nur für die unzähligen kritischen Gespräche sehr geschätzten Kollegin am Lehrstuhl. Unzählige Gespräche zu unzähligen Gelegenheiten haben der Arbeit an den richtigen und wichtigen Stellen Feinschliff verliehen. Danken möchte ich auch den geschätzten Kolleg*innen Frau Rechtsanwältin Anna Rickert, Frau Rechtsanwältin Katharina Frösner und Herrn Rechtsanwalt Thomas Stadler für die kritische Begleitung am Anfang der Themenfindung. John and Joanna Doe möchten aus Datenschutzgründen nicht namentlich dafür den verdienten Dank erhalten, dass sie ein neutrales Auge auf die technischen Fragen der Arbeit geworfen haben. All der kritische Input zur richtigen Zeit hat erheblich dazu beigetragen, dass die Arbeit nicht auf Abwege geraten ist.

Danken will ich auch meinen Kolleginnen am Lehrstuhl, insbesondere Frau Margit Berndl, die durch Ihre wertvolle Unterstützung bei allen organisatorischen und planerischen Lehrstuhlaufgaben erheblich dazu beigetragen hat, dass die Zeit für die Erstellung dieser Arbeit neben der Lehrstuhltätigkeit nicht zu knapp wurde.

Meiner Frau Danke ich von Herzen - und in Anerkenntnis des Umstandes, dass Worte den angemessenen Dank kaum zu fassen vermögen - für die bedingungslose Unterstützung auf dem Weg zu dieser Arbeit, bei ihrer Anfertigung und Fertigstellung.

Erster Teil:

Das Transparenzgebot – Zukunftsweisende Grundlage oder obsoletes Relikt des Datenschutzrechts?

§ 1: Einleitung und Problemstellung

Die Diskrepanz zwischen den Visionen der Internetpioniere der ersten Stunde und der heutigen Realität könnte größer kaum ausfallen. Die ursprünglichen Visionen zur herstellbaren Freiheit stehen in krassem Missverhältnis zum verlorenen Vertrauen.

I. Unabhängiges Internet

John Perry Barlow schrieb 1996 über das Internet in seiner „*Declaration of the Independence of Cyberspace*“:[1]

> [...] I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. [...] You do not know us, nor do you know our world. [...]

Die Realität hat dieses Statement überholt und das Internet unterliegt staatlichen Regularien und wird zudem überwiegend von privaten Entitäten beherrscht, die die Infrastruktur betreiben und den Rahmen für die Inhalteausgestaltung und -verwendung vorgeben.

Hierbei hat er also einen der wesentlichen Faktoren, weswegen dieses Netzwerk für wirtschaftliche Akteure nunmehr so interessant geworden ist, auf den Punkt gebracht:

> hctsaufsicht zum Beispiel: Lernen Sie da nicht dieses Problem oder diese Abgrenzung! Versuchen Sie zu verstehen, wieso es diese beiden Konzepte gibt und (generell!) wie man zwei (stellenweise konkurierende und kollidierende) Konzepte voneinander abgrenzt. Ganz viel lässt sich über den Telos erschließen. Der steht im Groben im Gesetz. Wenn Sie sich diesen Zugriff erschließen, sind Sie auch in Klausuren gut, in denen Sie die Details nicht kennen. Wichtig ist die Frage 'wie', nicht 'was'. Der Opt [...] Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. [...]

In einem Interview 20 Jahre nach der Unabhängigkeitserklärung räumte Barlow diese Irrtümer selbst ein.[2]

---

1 Barlow, Declaration of the Independence of Cyberspace.

2 https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/.

II. Abhängiges Internet

Noch häufiger als diese Problematik sind Betroffene, die unvermittelt eine E-Mail von einem Werbeunternehmen wie Facebook bekommen, weil ein Dritter einen Account angelegt hat und dabei dessen Adressbuch ausgewertet wurde.[3] Sie stehen in diesen Momenten regelmäßig vor der Frage, woher das Unternehmen ihre Daten hat und ob es diese verwenden darf.

Schon lange vor Entstehung dieser Problematik hat die alltägliche Benutzung von Informationstechnologie nicht mehr nur dem Nutzer die von ihm gewünschten Informationen verschafft. Mit der Benutzung von inzwischen oft vernetzten Geräten wie Computer, Smartphone und Tablet wird der Nutzer selbst gleichsam zu einer wertvollen Informationsquelle. Zu denjenigen, die davon profitieren, gehören auch die prominentesten Akteure im IT-Software- und IT-Dienstleistungsbereich, wie Google, Microsoft und Apple.[4]

Die Informationsquelle „Nutzer" wird zunehmend intensiver angezapft. Dies gilt sowohl für die Datenerfassung selbst, als auch für den anschließende Datenverarbeitung.[5] Daten werden heute oft ein kleiner Teil von „Big Data".[6] Insbesondere für die Art und Weise der Datenerfassung finden sich mit dem technischen Fortschritt immer neue Wege, die mit dem bestehenden Datenschutzrecht nur unzureichend geregelt werden können.[7] Die Datenerhebungssituationen sind für den durchschnittlichen Benutzer kaum alle erfassbar, ebenso wie der weiter steigende Datenerhebungsumfang schwer überblickt werden kann. Zur Verwirklichung eines effektiven Datenschutzes, sind Lücken im Rechtsregime des Datenschutzes zu vermieden. Dies ist ein ein chronisches Problem der schnellen technischen Entwicklung[8] und eine vorausschauende Rechtsetzung zu Einzelfragen ist kaum möglich.

---

3 Zum Friend-Finder und dessen spezifischen Transparenzproblemen mehr bei Meyer, DSRITB 2011, 529 (537 f.).

4 Dazu auch Kurz, Wachsender Datenreichtum, S. 58.

5 Zur Datenerfassung durch Software auf Endgeräten beispielsweise Hoffmann-Riem, JZ 2008, 1009 (1011).

6 Eine umfassende, im Wesentlichen zutreffende und dennoch leicht zugängliche Erläuterung dieses Modebegriffs und der zugrundeliegenden Technologie findet sich bei Hofstetter, 87 ff. nicht aktuell, aber dafür die Grundlagen darstellend Hader, 15 ff. kritisch zum Begriff auch Bull, S. 34–46.

7 So beispielsweise bei der Richtlinie 2009/136/EG, in der das Nutzertracking durch Cookies eingedämmt werden sollte, obwohl schon es damals nicht nur via Cookie stattfand.

8 Dazu schon Schneider, NJW 1984, 390 (390 ff.); ebenfalls auf technische Weiterentwicklungen bezogene Probleme bei Simitis, NJW 1998, 2473 (2473 ff.).

Es befinden sich ständig neue Datensammelmaschinen in der Entwicklung, bei der sich mitunter neue Fragen zum Datenschutz(recht) stellen. Beispielsweise wird das Auto zu einer umfassenden Datensammelmaschine ausgebaut.[9] Diese Entwicklung wird im Kontext von dem, was euphemistisch als „*Internet der Dinge*" bezeichnet wird, tatsächlich aber nur die Vernetzung von allem ist, aktuell am deutlichsten und ist ebenso problematisch.[10] Dieser Einwand greift aber zu kurz, denn genauso, wie die Datenverarbeitungsformen am Anfang ihrer Entwicklung stehen,[11] steht auch das Datenschutzrecht eher am Anfang seiner Entwicklung. Das Rechtsgebiet hat sich erst in der zweiten Hälfte des 20. Jahrhunderts in Form eigenständiger, geschlossener Regelungswerke manifestiert.

Daher liegt es nahe, den Versuch zu unternehmen, sich zunächst auf die Bearbeitung beziehungsweise Kodifizierung von wenigen, aber universell anwendbaren, Grundprinzipien zu konzentrieren. Mit solchen Grundprinzipien könnte die effektive Gewährleistung der Privatsphäre selbst angesichts des schnellen technischen Fortschritts Bestand haben. Ein solches Grundprinzip ist das Transparenzgebot. Demnach ist „eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß[, verfassungswidrig]."[12]

Transparenz wird einerseits in Datenschutzdebatten als Allheilmittel dargestellt, weil sie den Menschen Reaktionen auf Risiken ermögliche.[13] Trotz der Tatsache, dass Privatsphäre seit Längerem ein Objekt kritischer wissenschaftlicher Betrachtung ist,[14] wird die Frage selten untersucht, inwieweit und welche tatsächlichen Effekte diese Transparenz hat. Diese drängt sich aber auf wegen der in Bezug auf das Alltagsverhalten der Betroffenen weit-

9 Roßnagel, SVR 2014, 281; im Kontext von Big Data dazu auch Boehme-Neßler, DuD 2016, 419 (422); zum meist unmittelbaren Zusammenhang mit Fragen der Daten- und Systemsicherheit Szoldra, The truth about car hacking; zur Sicherheit auch Krauß/Waidner, DuD 2015, 383 (385 ff.).

10 Internet of Shit, The Internet of Things has a dirty little secret, Wobei das Problempotenzial nicht beim Datenschutz aufhört, dazu.

11 Hill, DÖV 2014, 213.

12 BVerfG, Urteil v. 15. Dez. 1983 (1 BvR 209, 269, 362, 420, 440, 484/83), BVerfGE 65, 1 (43).

13 Albrecht, S. 59.

14 Warren/Brandeis, Harvard Law Review 1890, 193 (194).

gehend folgenlos gebliebenen Enthüllungen von Edward Snowden,[15] welche vorsätzlichen und systematischen Rechtsbruch durch diverse Geheimdienste offenbarten.

Dieses Prinzip hat das Potenzial, technikneutral umgesetzt zu werden und bietet sich als Mindestbedingung für einen effektiven (individualrechtlichen) Datenschutz an. Das Transparenzgebot ist hierfür besonders geeignet, weil es unabhängig von den anderen etablierten Datenschutzgrundsätze funktionieren kann. Auch ist es unabhängig von der dogmatischen Einordnung von Daten in der Rechtsordnung.[16] Damit bietet es eine solide Grundlage gegenüber technischen und denkbaren rechtlichen Entwicklungsschritten.

Kritisch ist zu betrachten, inwieweit Transparenz in Konflikt mit Technikgestaltung geraten kann. Die aktuellen Entwicklungen lassen zunehmend vermuten, dass Transparenz nur mit teils massiven Eingriffen in übliche Nutzungsprozesse erreicht werden kann. Daten sind sowohl Gegenleistung als auch der Grund für die kostenlosen oder unverhältnismäßig billigen Angebote im Internet und damit für dessen aktuelle Gestalt.[17] Konkret sieht man dies beispielsweise an der Vielzahl von Berichten über verstecktes Datensammeln von diversen Softwareanwendungen[18].[19]

---

15 So zu geringen Klickzahlen bei Artikeln über die Vorratsdatenspeicherung in der Süddeutschen Zeitung Schmidt, Warum ich keine Artikel zur Vorratsdatenspeicherung lese.

16 Hoeren, MMR 2013, 486 (So wird versucht, Daten mit dem Rechtskonzept des Eigentums zu fassen, konkret § 903 BGB); Dorner, CR 2014, 617 (den Ansatz generell ablehnend); grundsätzlich kritisch Härting, CR 2011, 169 (173); umfassender Härting/Schneider, CR 2015, 819 (826 f.); Vorgeschlagen wird auch Daten über § 823 BGB zu schützen Spindler, JZ 2016, 805 (813 f.); die Rechtsprechung scheint diese Grenzziehung nicht zu sehen, so BGH in etwas anderem Kontext Götting, JZ 2016, 908 (911 f.); Überblick zum Themenkomplex Specht, CR 2016, 288 (289 ff.); Daten als Gegenleistung und die Folgeprobleme für die Einwilligung werden ebenfalls diskutiert Specht, JZ 2016, 763 (770); zuletzt kritisch zur neurlichen Debatte Kühling/Sackmann, NVwZ 2018, 681 (684-686).

17 Albrecht, S. 89.

18 So die Verwendung von Red Shell - ohne Information oder Opt-Out Möglichkeit für (minderjährige) Betroffene (ein Trackingtool),https://www.reddit.com/r/Steam/comments/8pud8b/psa_red_shell_spyware_holy_potatoes_were_in_space/ oder die Weitergabe von Kundendaten an Dritte, ohne Information oder Opt-Out, https://www.golem.de/news/datenschutz-british-airways-soll-unerlaubt-persoenliche-daten-weitergeben-1807-135603.html.

19 Zum Thema der Trackingfragen in der realen Welt durch Ortung von Smartphones siehe einführend Maier/Ossoinig, VuR 2015, 330.

§ 2: Eingrenzung des Themas

Zur weiteren Eingrenzung der Frage, ob das Transparenzgebot als zukunftsweisende Grundlage oder als obsoletes Relikt des Datenschutzrechts anzusehen ist, bietet sich die Unterscheidung von Datenverarbeitungen an, die mit dem Transparenzgebot offensichtlich in Einklang stehen, und solchen, die es (möglicherweise) nicht tun.

Jede Form der Datenverarbeitung kann offen, mit Kenntnis der Betroffenen, stattfinden[20] oder völlig verdeckt stattfinden.[21] Auch die Grenzziehung zwischen offener und verdeckter Datenverarbeitungen ist interessant und nur scheinbar einfach.[22] Die verdeckte Datenverarbeitung stellt ein datenschutzrechtliches Problem dar, zu dessen Lösung eine entsprechende Umsetzung des Transparenzgebots beitragen könnte.[23]

I. Offene Datenverarbeitung

Offene Datenverarbeitungen finden häufig statt, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ohnehin vertragliche Beziehungen bestehen. Im Regelfall liegt hier eine informierte Einwilligung des Betroffenen vor und es besteht insbesondere infolge der Informiertheit kein Konflikt mit dem Transparenzgebot. Soweit beispielsweise Facebook seine AGB ohne Zustimmung der Nutzer ändert, handelt es ich um eine Ausweitung der Datenverarbeitungsbefugnisse unter Missachtung datenschutzrechtlicher (und vertragsrechtlicher) Vorgaben. Eine offene Datenverarbeitung erfolgt im obigen Sinne beispielsweise beim „*Cloud Computing*“, bei dem Anwendungsdaten und auszuführende Anwendungen für unterschiedliche Zwecke auf Computer von Dritten ausgelagert werden, also in einen Bereich, in dem die physische Kontrolle der Betroffenen über Datenverarbeitungsanlagen vollständig fehlt.

Ob eine offene Datenverarbeitung rechtmäßig ist, ist im Kern keine Frage des Transparenzgebots mehr und für die vorliegende Arbeit daher irrelevant.

---

20 Dazu S. 25.
21 Dazu S. 26.
22 Dazu S. 28.
23 Dazu S. 30, sowie S. 31 und S. 31.

II. Verdeckte Datenverarbeitung

Neben dieser Form der offenen Datenverarbeitung werden Daten zunehmend auch erhoben, ohne dass die Betroffenen über die Datenerhebung informiert werden.

Hierbei werden unterschiedliche, meist monetäre, Zwecke verfolgt. Der typische (Internet-)Nutzer ist dabei weder in Kenntnis davon, dass Daten erhoben werden, noch von wem oder wofür. An dieser Stelle wird deutlich, dass das Konzept des geltenden Datenschutzrechts leer zu laufen droht. Denn alle individualrechtlichen Ansprüche aus dem Datenschutzrecht setzen mindestens die Kenntnis des Betroffenen von der Datenerhebung und der verantwortlichen Stelle voraus.

Eine solche verdeckte Datenerhebung findet bei gewissen Formen von eingebundenen Inhalten in Internet-Seiten statt. Wenn beispielsweise eine Webseite eine von Google Fonts zur Verfügung gestellte Schriftart verwendet, wird bei einem Aufruf dieser Webseite auch eine Verbindung zu einem Google-Server hergestellt. Hierbei offenbart der Betroffene unter anderem seine IP-Adresse[24] und den Zeitpunkt des Aufrufs der Schriftart gegenüber Google. Dies ist technisch notwendig, um die entsprechende Schriftart anzu-

24 Abkürzung für *Internet Protocol Adresse*. Es ist zwischen IP Version 4 und IP Version 6 zu unterscheiden. Erstere bildet Adressen nach dem Muster a.b.c.d für die gilt

$$a, b, c, d \in \{0...255\}$$

Dies geht zurück auf RFC 791, abrufbar unter https://tools.ietf.org/html/rfc791, abgerufen am 16.12.2017. Die Nachfolgeversion 6 arbeitet nicht mehr mit 32-bit Adressen, sondern mit 128 bits. Die Beschreibung des Protokolls in der derzeitigen Fassung ist abrufbar im RFC 8200, unter https://tools.ietf.org/html/rfc8200, abgerufen am 16.12.2017. Dies gewährt einen größeren Adressraum, der nach dem Muster a:b:c:d:e:f:g:h für die eine hexadezimale Schreibweise, in der 0-f die Zahlen von 0-15 repräsentieren, üblich ist und für die gilt

$$a, b, c, d, e, f, g, h \in \{0...ffff\}$$

Diese technischen Details und die Implikationen von IP Version 6 für die Privatsphäre sind aber kein Fokus dieser Arbeit.

zeigen. Bei einem Konzern wie Google liegen Hintergedanken nahe,[25] gerade im Hinblick auf den primären Unternehmenszweck Werbung zu verkaufen.[26]

Hier bleibt dem Betroffenen bei üblicher Benutzung der im Hintergrund ablaufende Vorgang verborgen. Dieser lässt sich zwar im Quelltext der Seite nachvollziehen. Die Information fehlt aber in der Seitendarstellung des verwendeten Browsers. Auch bei einem normalen Vorgang, wie der Einbindung eines Videos von der Plattform YouTube, ist Hintergrundwissen erforderlich, um den Datenverarbeitungsvorgang als solchen erkennen und qualitativ einordnen zu können. Die Nutzer werden in beiden Fällen selten vom Seitenbetreiber darüber informiert, dass Daten an Dritte fließen.

Ebenso verborgen bleiben dem Internetnutzer auch die meisten Techniken zur Nutzerverfolgung, die auf Webseiten eingesetzt werden. Ein zeitgemäßes Beispiel hierfür ist das sogenannte „Fingerprinting". Wie der Name nahe legt, wird hierbei einem Browser oder einem Endgerät ein eindeutiger Fingerabdruck zugewiesen, um bei erneuten Seitenaufrufen eine Identifikation zu ermöglichen.

Die durch teils bewusst herbeigeführte Intransparenz an unterschiedlichen Stellen im Verarbeitungsprozess ist insbesondere im Kontext von Nutzerverfolgung allgegenwärtig.[27]

Eine der wenigen Methoden, von welcher die Betroffenen prominent und wiederholt Kenntnis erlangen, sind Cookies. Diese werden in Datenschutzerklärungen regelmäßig als „*Textdateien*" beschrieben, die es Seitenbetreibern ermöglichen, diverse Funktionen „*komfortabel*" umzusetzen, wie die Speicherung von Darstellungsinformationen für zukünftige Seitenbesuche oder Logins und Single-Sign-Ons. Zudem erlauben sie die Identifikation der Nutzer. Für deren Verwendung gab es bereits vor Inkrafttreten der DSGVO zumindest stellenweise und nach dem 25.05.2018 zunehmend Benachrichtigungen, um die Einwilligung der Nutzer einzuholen. Diese Information der Nutzer ging zunächst auf die Richtlinie 2009/136/EG zurück.[28]

---

25 Siehe nur http://www.wired.com/2013/09/gmail-wiretap-ruling/ (15.12.2014) und Joffe v. Google, Inc., United States Court of Appeals for the Ninth Circuit. Das Urteil beschäftigt sich mit der Frage, ob Google mit seinen StreetView-Fahrzeugen auch Daten über die auf der Straße empfangbaren W-Lan-Stationen sammeln darf.

26 Dies wird auch beiläufig artikuliert von Bull, in: Zukunft der informationellen Selbstbestimmung, 13–22 (21); ähnlich im Tenor auch Schaar, in: Zukunft der informationellen Selbstbestimmung, 93–102 (102).

27 Albrecht, S. 59, 85, 92.

28 ABl. L 337/11, dort heißt es in Art. 2 Nr. 5, dass „... die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder

III. Grenzfälle zwischen verdeckter und offener Datenverarbeitung

Ein Grenzfall hin zur offenen Datenverarbeitung entsteht, wenn die Verantwortliche mit den erhaltenen Daten ihren Umsatz generiert, ohne dass der Betroffene hiervon Kenntnis hat, was in gewisser Weise in Konflikt mit § 4 Abs. 4 Satz 3 BDSG.Soweit also der Betroffene nicht weiß, zu welchem Zweck die Daten erhoben werden, kann es sich ebenfalls de facto um eine verdeckte Datenerhebung handeln.

Dieses Problem ergibt sich bei den oben aufgeführten eingebundenen Inhalten nur, wenn der Seitenbetreiber und die Verantwortliche unterschiedliche Entitäten sind. Aus Sicht des Betreibers dient die Datenverarbeitung der Inhaltedarstellung. Aus Perspektive des Drittanbieters liegt hingegen das Problem potenziell vor, wenn dieser mit den Daten weitere Verarbeitungen vornimmt, die über das bloße Bereitstellen der Inhalte hinausgehen.

Ein weiteres Beispiel für diese Grenzfälle ist Facebook. Eine Information, dass Facebook mit den Nutzerdaten seinen Umsatz generiert, fehlt in den allgemeinen Geschäftsbedingungen.[29] Auch in den Erläuterungen zum Datenschutz findet sich hierzu keine explizite Äußerung.[30] Der Nutzer bleibt hierüber formal im Unklaren, denn in diesem Fall ist ihm zwar bekannt, dass die Daten erhoben werden. Informationen über die Zielsetzung werden aber vorenthalten.[31]

Dieser Fall ist für diese Arbeit weniger interessant, da zwei entscheidende Argumente eine hinreichend offene Datenverarbeitung nahe legen. Es ist zum einen allgemein bekannt, dass Facebook die Daten aus eigenen wirtschaftlichen Interessen heraus verarbeitet. Zum anderen ist in den Datenschutzbestimmungen relativ detailliert aufgeschlüsselt wozu die Daten konkret verwendet werden. Hier wird der Betroffene also lediglich über einen der Zwecke der Datenverarbeitung im Unklaren gelassen, der sich auch bei oberflächlicher Betrachtung des Sachverhalts offenbart.

Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u.a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat."

29 Facebook Inc., Nutzungsbedingungen.

30 Dies., Datenrichtlinie.

31 Im Anschluss hieran stellt sich die Frage, ob nicht der Nutzer grundsätzlich eigenverantwortlich entscheiden können muss, ob er seine Gegenleistung für eine vertragliche Dienstleistung in Form von Daten oder in Form von Geld erbringen will.

Einen interessanten Grenzfall zur verdeckten Datenverarbeitung bildet dagegen die Datenerhebung durch (Nutz-)Software auf den Endgeräten.[32] Zu nennen sind hier insbesondere auch Betriebssysteme selbst, wie beispielsweise MacOS[33], iOS[34], Android[35], ChromeOS[36], Ubuntu[37] und Windows 10[38]. Dies stellt im Hinblick auf die Implikationen für die Nutzer und deren informationelle Selbstbestimmung ein schwerwiegendes Problem dar. Hier lässt sich die Bedeutung der Beeinträchtigung kaum durch den Verweis auf die Einwilligung der Nutzer schmälern. Denn rechtliche Selbstbestimmung ist nur unter der Voraussetzung möglich, dass entsprechende Informationen beim Entscheidungsträger zur Zeit der Entscheidung tatsächlich vorhanden sind. Nur auf deren Grundlage kann er überhaupt zu der Erkenntnis gelangen, dass er gerade eine (grund-)rechtserhebliche Entscheidung trifft. An dieser Information fehlt es aber jedenfalls, wenn der Betroffene weder erfährt, dass seine Daten gerade gezielt gesammelt werden, noch um welche Daten es sich dabei handelt.

Solche Funktionen sind, wenn überhaupt, irgendwo in seitenlangen Klauselwerken erwähnt. Daher stellt sich die Frage, ob dies einen Verstoß gegen das datenschutzrechtliche Transparenzgebot darstellt und mit welchen Konsequenzen diesem begegnet werden müsste . An dieser Stelle wirkt das Transparenzgebot mit der informierten Einwilligung zusammen.

Dieser Fall unterscheidet sich in zwei Punkten signifikant von dem obigen.[39] Zunächst findet die Datenerfassung in einer atypischen Situation statt. Zwar sind sich die Nutzer mehr und mehr dessen bewusst, dass ihr „online"-Verhalten unter Beobachtung steht. Dieses Bewusstsein ist in Bezug auf die Endgeräte und das „offline"-Verhalten aber kaum vorhanden – noch weniger,

---

32 Ein aktuelles Beispiel http://www.heise.de/security/meldung/Shazam-meldet-Standort-heimlich-an-Werbenetzwerke-2111850.html (15.12.2014).

33 https://www.washingtonpost.com/news/the-switch/wp/2014/10/20/apples-mac-computers-can-automatically-collect-your-location-information/ (29.08.2015).

34 http://www.igeeksblog.com/top-10-ios-8-privacy-settings/ (29.08.2015).

35 http://digiday.com/platforms/google-tracking/ und http://www.engadget.com/2013/11/06/google-profile-photos-android-calls/ (je 15.12.2014).

36 http://arstechnica.com/information-technology/2013/09/why-the-nsa-loves-google s-chromebook/ (15.12.2014) und https://nakedsecurity.sophos.com/2015/06/24/not-ok-google-privacy-advocates-take-on-the-chromium-team-and-win/ (29.08.2015).

37 https://fixubuntu.com/ (29.08.2015).

38 http://www.zeit.de/digital/datenschutz/2015-08/privatsphaere-windows-10-einstellungen-deaktivieren und http://www.heise.de/newsticker/meldung/Windows-10-Datensammelwut-beherrschen-2774941.html (je 29.08.2015).

39 Siehe S. 28.

wenn es um stationäre Endgeräte geht. Dies mag auch daran liegen, dass dies ein eher neues Phänomen ist. Zudem befinden sich Funktionen ohne Abschaltfunktion potenziell jenseits der informierten Einwilligung. Es bleibt dabei unklar, welche Funktionen dies sind.[40]

IV. Verdeckte Datenverarbeitung im Lichte des Transparenzgebots

Gerade bei der verdeckten Datenverarbeitung wird deutlich, dass sie weit unter der Wahrnehmungsschwelle der überwiegenden Mehrzahl der Betroffenen stattfindet.[41] Abseits von technischen oder rechtlichen Fachdiskussionen ist dieses Thema weithin unentdeckt, so dass jenseits ohnehin interessierter Kreise kaum Informationen darüber verbreitet werden. Das Datenschutzrecht deckt insoweit in seiner aktuellen Form dieses Problem möglicherweise unzureichend ab.[42]

Im Datenschutzrecht gilt bei der Datenverarbeitung der Grundsatz der Transparenz.[43] Bereits im Volkszählungsurteil hat das Bundesverfassungsgericht die Kenntnis des Betroffenen von der Datenverarbeitung als Voraussetzung informationeller Selbstbestimmung postuliert.[44] Damit ist das Transparenzgebot ein zwingender Aspekt in Fragen des Datenschutzrechts, welches als Zweck die Wahrung der informationellen Selbstbestimmung verfolgt.

Die Ausgestaltung von datenschutzrechtlichen Ansprüchen setzt beim Betroffenen ebenso zwingend Kenntnis über die Datenverarbeitung selbst und die entsprechende verantwortliche Stelle voraus. Fehlt eines von beidem, laufen alle bestehenden individualrechtlichen Schutzmechanismen des Datenschutzrechts leer. Denn Auskunfts-, Berichtigungs- oder Löschungsansprüche können nur geltend gemacht werden, wenn der Anspruchsgegner

40 https://www.microsoft.com/en-us/Useterms/OEM/Windows/10/UseTerms_OEM_Windows_10_German.htm (31.08.2015), wo es unter 3. heißt „Viele dieser Features können über die Benutzeroberfläche deaktiviert werden, oder Sie können sich entscheiden, sie nicht zu verwenden." Es ist also nicht nur ein Opt-out, sondern die Datenerfassung ist hier in Teilen zwangsweise integriert.

41 Dazu S. 26.

42 Zu Unzulänglichkeiten des Datenschutzrechts im Allgemeinen Masing, NJW 2012, 2305.

43 Kühling/Seidel/Sivridis, S. 111; auch unter der DSGVO gilt dieser fort Kühling/Klar/Sackmann, S. 146.

44 BVerfG, Urteil v. 15. Dez. 1983 (1 BvR 209, 269, 362, 420, 440, 484/83), BVerfGE 65, 1 (43).

und der Datenverarbeitungsvorgang als solcher bekannt sind. Deswegen stellt sich die Frage, ob dieser Grundsatz oder dessen bisherige Umsetzung an den aktuellen Stand der Technik und ihre Verwendung angepasst werden kann. Darüber hinaus ist offen, ob auf Grundlage bisheriger Entwicklungen eine technologieneutrale oder technologieadäquate[45] Form eines datenschutzrechtlichen Transparenzgebots entwickelt werden kann.

V. Transparenz als Lösung für verdeckte Datenverarbeitung

Offen ist damit, ob die derzeitigen Mittel der Verantwortlichen einen ausreichenden Ausgleich für die umfassenden, verdeckten Datenverarbeitungen darstellen. Diese Verarbeitungen begleiten Betroffene im Internet im Besonderen, aber auch in der Informationstechnologie im Allgemeinen zunehmend. Das Mittel zur Erfüllung von Transparenzpflichten in Form der einfachgesetzlichen Informationspflichten aus dem Datenschutzrecht war und ist die Datenschutzerklärung, welche in der vorliegenden Arbeit anhand ausgewählter Beispiele vertieft wird. Dies geschieht mit Fokus Potenziale und Grenzen dieses Mittels anhand der aktuellen Entwicklung in der Praxis. Verdeckte Datenverarbeitungen können demgegenüber kaum durch Auskunftsansprüche erfasst werden, da diese bereits die Kenntnis einer Datenverarbeitung voraussetzen.

VI. Grenzen des Transparenzgebots

Gerade bei den Informationspflichten ist allerdings auch zu beleuchten, ob diese Anforderungen (technisch) umfassend umsetzbar sind. Zudem stellt sich die Frage, ob und gegebenenfalls wo eine Grenze zu ziehen ist. Bei konsequenter Umsetzung müssten beispielsweise auch DNS-Server und andere Teile der Infrastruktur diesem Gebot genügen. Diese erfassen betriebsbedingt, wer wann mit wem Daten austauschen will. Die Bedeutung dieser Daten, die oftmals verharmlosend als „*Metadaten*“ bezeichnet werden, war schon vor dem Whistleblowing von Edward Snowden im Jahr 2013 bekannt. Es wurde unter anderem enthüllt, dass private Akteure, wie Google, Microsoft und Apple, umfangreich mit Geheimdiensten zur Datensammlung

45 Dazu ausführlich am Beispiel der DSGVO Sydow/Kring, ZD 2014, 271.

kooperieren.[46] Bereits weit vorher entstand ein ganzer Industriezweig der mit diesen Informationen (und daraus gebildeten Persönlichkeitsprofilen) seinen Umsatz erwirtschaftet. Die Relevanz des Problems wird auch durch die zunehmende Unschärfe der Grenze zwischen privaten und öffentlichen Akteuren im Internet deutlich.[47] In ihrem Einfluss auf die Gesellschaft entsprechen große Suchmaschinen viel eher einem staatlichen Akteur als einem privaten, obwohl sie rechtlich eindeutig ein privater Akteur sind. Zudem haben staatliche Stellen ebenfalls regelmäßig großes Interesse an privaten Datensammlungen.[48]

Es erscheint aber, gerade aus technischer Perspektive, fragwürdig technisch sinnvolle Vermittlungsdienste, wie das DNS, im Ergebnis so strengen Regeln zu unterwerfen. Denn ein DNS-Server ist anders betrachtet eben „nur" Teil der Infrastruktur, die allerdings zuweilen von obigen Akteuren betrieben wird.[49] In der Google privacy policy heißt es passend: „We may combine personal information from one service with information, including personal information, from other Google services [...]."[50]

Das Transparenzgebot bewegt sich damit jedenfalls in einem Spannungsfeld zur technischen Ausgestaltung von Kommunikationsvorgängen, dessen Grenzen unklar sind. Aus rechtlicher Perspektive drängt sich zudem die Frage auf, welchen Mehrwert Transparenz in Fällen einer erlaubten Datenverarbeitung ohne Einwilligung hat.

---

46 Vergleiche zu den Enthüllungen u.a. https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill, https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript, http://news.softpedia.com/news/snowden-used-free-software-because-he-was-afraid-of-backdoors-in-microsoft-apps-502039.shtml, https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining, speziell zur Kooperation mit Privaten Akteuren http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html und https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data abgerufen am 12.01.2016.

47 Dazu Hijmans/Kranenborg, in: Data Protection Anno 2014: How to Restore Trust?, 3–17 (S. 4).

48 Kurz, in: Persönlichkeit im Netz - Sicherheit - Kontrolle - Transparenz, 1 (11); ebenso Bull, in: Zukunft der informationellen Selbstbestimmung, 13–22 (16-18).

49 So beispielsweise die DNS-Server von Google, erreichbar unter 8.8.8.8 oder 8.8.4.4. Vergleiche auch https://developers.google.com/speed/public-dns/?hl=en (30.08.2015).

50 https://www.google.com/policies/privacy/ (30.08.2015).

§ 3: Forschungsstand

Eine der Vorfragen im Rahmen dieser Arbeit ist, ob IP-Adressen grundsätzlich Personenbezug aufweisen. Diese wurde in der Arbeit von *Schmidt-Holtmann*[51] umfassend untersucht. Hierauf kann aufgebaut werden und eine ergänzende Bearbeitung vorgenommen werden. Zudem hat der EuGH hierzu eine Entscheidung gefällt,[52] die genauerer Untersuchung bedarf.

Diese Vorfrage ist insbesondere auch für die Nutzerverfolgung wichtig, da bei dieser regelmäßig mit IP-Adressen gearbeitet wird. Das Beispiel selbst wurde bereits mehrfach bearbeitet, so in der Arbeit von *Fröhle*[53] und auch in der Arbeit von *Himmels*.[54] Die erste Arbeit ist schon infolge der zwischenzeitlichen Rechtsentwicklung teilweise obsolet. Die zweite Arbeit widmet sich der Thematik aus einer lauterkeitsrechtlichen Perspektive. In Bezug auf die technischen Grundlagen bleiben beide Arbeiten themenbedingt bei relativ oberflächlichen Erkenntnissen und Zusammenhängen. Das datenschutzrechtliche Gesamtbild und sich aufdrängende Folgefragen für dieses bleiben unbearbeitet. An genau diesen Stellen versucht die vorliegende Arbeit, in Bezug auf die Nutzerverfolgung, jenseits der Beispielbetrachtung auch zu prüfen, ob und wie dies zum Gefüge des Datenschutzes passt.

Eingebundene Inhalte sind, soweit ersichtlich, aus datenschutzrechtlicher Perspektive unbearbeitet. Es gibt im Bereich der Betriebssysteme unzählige Diskussionen über die Zulässigkeit von Datenverarbeitung auf Grund von Klauseln in Lizenzverträgen, sogenannten EULAs (End User License Agreements).Diese Diskussionen sollen allerdings hier mit dem Fokus auf das datenschutzrechtliche Transparenzgebot betrachtet werden.

Obwohl seit Längerem – beispielsweise in Rechtsgebieten wie dem Verbraucherschutzrecht[55] oder Informationsfreiheitsrecht[56] – das Stichwort Transparenz häufig fällt, erfährt das Transparenzgebot des Datenschutzrechts relativ wenig Beachtung in der Fachliteratur. Aktuell hat sich eine Arbeit mit

51 „Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht“, 2014.
52 EuGH, Urteil v. 19. Okt. 2016 (C-582/14).
53 Fröhle.
54 Himmels.
55 Vergleiche nur v. Westphalen, NJW 2013, 961 (961 ff.); Ufer, MMR 2015, 226 (226 ff.).
56 Vergleiche nur Koppensteiner, EuR 2014, 594 (594 ff.); Caspar, DÖV 2013, 371 (371 ff.).

der ausufernden Transparenz beschäftigt, die Erwägungen aber spezifisch auf die DSGVO stützt.[57]

Es gibt eine kurze Auseinandersetzung mit dem Transparenzgebot, die sich auf die Beziehung zwischen Bürger und Staat beschränkt.[58] Allerdings gibt es keine Arbeit, die sich konkret mit Notwendigkeit und Potenzial des datenschutzrechtlichen Transparenzgebots und den Vorgaben aus Menschen- und Grundrechten auseinandersetzt. Ebenso fehlt eine Arbeit, die vertieft auf technische Gegebenheiten bei der Verwirklichung des Datenschutzes im Bereich der Informationstechnologie eingeht.

Auch die Frage, was genau der datenschutzrechtliche Grundsatz der Transparenz beinhaltet, ist keinesfalls abschließend geklärt. So beschränkt sich beispielsweise eine Umschreibung des Grundsatzes darauf, dass die Datenverarbeitung „möglichst nachvollziehbar“ sein muss.[59] Auch die Frage, welchen Umfang dieser Grundsatz konkret hat, wird zwar beantwortet, allerdings ohne substantielle Begründung und mit Widersprüchen.[60]

57 Robrecht, S. 11–20.
58 Albers, S. 120 ff.
59 In: Wolff /and, Syst.A Rn. 43.
60 Ebd., Syst.A Rn. 45.

§ 4: Gang der weiteren Untersuchung

Um das Transparenzgebot zu untersuchen, müssen zunächst seine rechtlichen Grundlagen und Rahmenbedingungen sowie seine Bedeutung und Umsetzung im Datenschutzrecht unter Berücksichtigung unionsrechtlicher Grundlagen dargestellt werden. Im Anschluss werden neuere Formen von Datenerhebungen auf ihre Übereinstimmung mit den erarbeiteten Grundsätzen des Transparenzgebots. Hieraus lässt sich schließen, ob dem Transparenzgebot hinreichend Rechnung getragen wird und welcher Korrekturen es bedarf,[61] um dies zukünftig möglichst technikneutral zu erreichen.[62]

I. Grundlagen

Die Arbeit untersucht zuerst das Datenschutzrecht auf Vorgaben und die bisherige Umsetzung für ein Transparenzgebot. Dabei werden internationale Normen, schwerpunktmäßig Art. 8 der Europäischen Menschenrechtskonvention (EMRK) sowie die Datenschutzkonvention des Europarats berücksichtigt. Hinzu tritt das Unionsrecht aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) und der Charta der Grundrechte der Europäischen Union (GrCh) sowie das Sekundärrecht, einschließlich der DSGVO. Das nationale Recht mit dem Grundrecht auf informationelle Selbstbestimmung und den entsprechenden Datenschutzgesetzen wird ebenfalls erfasst. Methodisch ist bei dieser Untersuchung die Genese und die Entwicklung der Rechtsnormen entscheidend. So werden die Kontexte klarer, in denen die normative Entscheidung getroffen worden ist. Diese geben zusammen mit der Rechtsprechung Aufschluss über das Problembewusstsein und die Perspektive des Normgebers.

Aus der Zusammenschau kann die Essenz eines Transparenzgebots herausgearbeitet werden. Auf Grund der Inhaltsbestimmung des Transparenzgebots kann die Rechtslage auf konzeptionelle Umsetzungslücken hin untersucht werden. Hier wird der in der Vorarbeit erarbeitete datenschutzrechtliche Soll-Zustand mit dem kodifizierten Ist-Zustand verglichen, um Diskrepanzen zu

61 Zu diesem grundsätzlichen Problem im Datenschutzrecht allgemein Bull, S. 134.

62 Wobei es Stimmen gibt, die davon ausgehen, dass dies unmöglich ist Robrecht, in: Zukunft der informationellen Selbstbestimmung, 83–92 (87).

entdecken. Aus diesen können Schlussfolgerungen für gegebenenfalls nötige Veränderungen in der Umsetzung des Transparenzgebots gezogen werden. In einem zweiten Schritt werden dann als Grundlage für Teil 3 die technischen Vorgänge der Datenverarbeitung anhand von ausgewählten Beispielen erläutert.

II. Datenschutzrechtliche Beurteilung

Im praktisch orientierten dritten Teil erfolgt die Beurteilung der Transparenz in den Beispielsachverhalten, anhand der Erkenntnisse aus Teil 2 in Bezug auf das Transparenzgebot. Methodisch ist hierbei auf die Subsumtion der Beispielsfälle unter die entsprechenden Transparenzanforderungen zurückzugreifen. Ergeben sich Unzulänglichkeiten der Umsetzung des Transparenzgebots bei den praktischen Beispielsfällen, werden hieraus Schlussfolgerungen für den Anpassungsbedarfs des Datenschutzrechts gezogen. Die Erkenntnisse liegen damit auch in einer praktischen, sachverhaltsbezogenen Form vor. Die Erwägungen sind durch aktuelle, alltägliche Sachverhalte und eine im Wirkungsbereich des Datenschutzrechts alltäglich bestehende Beeinträchtigung der Privatsphäre untermauert. Die Schlussfolgerungen profitieren dementsprechend von diesem Praxisbezug und fallen deutlich konkreter aus, als noch im ersten Teil. Gleichzeitig können sie von den dortigen Ausführungen profitieren.

III. Potenzial und Grenzen des Transparenzgebots

Aus den kombinierten Erkenntnissen aus Teil 2 und Teil 3 lassen sich die Anforderungen an das datenschutzrechtliche Transparenzgebot weiter konkretisieren. Auf der rechtlichen Seite wird das Potenzial des Transparenzgebots zur Verwirklichung informationeller Selbstbestimmung fassbarer. Ebenso wird erkennbar, wie eine möglichst technikneutrale Umsetzung dieses Potenzials gelingen kann. Jenseits dessen wird aber auch klarer werden, welchen tatsächlichen Grenzen dieser Ansatz unterliegt. Sowohl in Bezug auf die Technik, als auch auf deren Benutzung durch die Betroffenen, wird durch die Beispiele deutlicher, welchen tatsächlichen Beitrag Transparenz für die informationelle Selbstbestimmung haben kann. Aus diesen Konkretisierungen lassen sich wiederum praxistaugliche Schlussfolgerungen für eine sinnvolle Weiterentwicklung des Transparenzgebots und seiner Umsetzung ableiten.

Zweiter Teil:

Grundlagen

§ 5: Begriffsbestimmungen und Vorfragen

Zur Erleichterung der Lektüre werden einige Konzepte und insbesondere Begriffe im folgenden Teil der Arbeit erläutert. Soweit erforderlich werden Begriffe auch definiert und abgegrenzt. Wenn in der Arbeit Begriffe des Art. 4 DSGVO verwendet werden und nichts anderes bestimmt ist, so kommt ihnen die dort definierte Bedeutung zu.

I. Eingrenzung des zu untersuchenden Rechts

Die folgende Analyse beschäftigt sich auf der Seite der verantwortlichen Stelle nur mit privaten Akteuren. Auch bereichsspezifischer Datenschutz bleibt im Rahmen dieser Arbeit unberücksichtigt, da dieser für die allgemeine Frage nach der Bedeutung des Transparenzgebots zu spezielle Antworten bereit hält. Eine Ableitung allgemeiner Erkenntnisse aus diesen Spezialregelungen fällt zudem regelmäßig schwer und setzt sich leicht systematischen Bedenken aus. Schließlich würde der Umfang der Arbeit noch weiter erhöht, ohne absehbar adäquaten Mehrwert.

II. Schutzziel(e) des Datenschutzrechts

Bevor datenschutzrechtliche Fragen im Detail strukturiert beantwortet werden können, stellt sich dem Grunde nach die Frage nach dem durch das Recht verfolgten Zweck. Auch mit der DSGVO ist die Frage nach der Schutzkonzeption des Datenschutzrechts noch nicht beantwortet.[1] Bereits vor dieser Normierung war das Datenschutzrecht insoweit alles andere als leicht zu handhaben.[2] Zudem verschärft sich die Problematik durch die zahlreich zu fällenden Abwägungsentscheidungen mit der DSGVO erheblich, da die Ergebnisse der Abwägungsentscheidungen nicht zuletzt maßgeblich von den konkret gewählten Schutzzielen abhängen. Zur Verbesserung der Untersuchungsergebnisse geht die Arbeit daher davon aus, dass maßgebliches Schutzziel des Datenschutzrechts im Allgemeinen und des Transparenzge-

1 Dazu zusammenfassend und kritisch Veil, NVwZ 2018, 686 (691 f.).
2 Ebd., 686 (690 f.).

bots im Besonderen die Gewährleistung informationeller Selbstbestimmung beziehungsweise (gerade aus Perspektive des EGMR) ungestörter Persönlichkeitsentwicklung ist.

III. Transparenz

1. Wortbedeutung

Als zentraler Begriff der Arbeit muss zunächst Transparenz erfasst werden. Im Duden wird Transparenz umschrieben mit „*Durchscheinen, Durchsichtigkeit, [Licht]durchlässigkeit, Durchschaubarkeit, Nachvollziehbarkeit*“. Im Etymologischen Wörterbuch der deutschen Sprache findet sich unter dem Adjektiv „*transparent*“ die Rückführung auf das identisch geschriebene französische Wort „*transparent*“. Dieses Wort wiederum setzt sich zusammen aus „*parere*“ (*sichtbar sein, erscheinen*)[3] und „*trans-*“ (*hinüber, jenseits, extrem*[4] und *durch*[5]). Demnach findet sich das Wort seit dem 18. Jahrhundert in Fachsprachen wieder und zählt zum erweiterten Standardwortsatz.[6]

Ob der diversen Verwendung des Begriffs läuft die Arbeit Gefahr, sich eben der grundsätzlichen Kritik auszusetzen, der auch das Wort Transparenz in seiner allgemeinen Verwendung unterliegt. So äußert beispielsweise *Byung-Chul Han* Bedenken gegenüber allgegenwärtigen undifferenzierten Forderungen nach Transparenz.[7] Dieser Kritik kann durch eine entsprechend spezifische Definition und/oder durch eine Konzentration auf relevante Teilaspekte begegnet werden.

Damit wird das Erfordernis deutlich, eine Definition von „Transparenz“ bereits für den Einstieg in die Arbeit zu verwenden, die ohne die sprachlichen Grundlagen zu verkennen, die Besonderheiten der Anforderungen des Datenschutzrechts erfassen kann und damit gleichzeitig in der Lage ist, problematische Aspekte von Transparenz auszublenden, soweit sie nicht auch in Bezug auf das Datenschutzrecht relevant sind.

Gerade im Datenschutzrecht muss Transparenz nicht im Wortsinn (Durchsichtigkeit der Datenverarbeitung) verstanden werden. Es kann auch nur dahingehend interpretiert werden, dass spezifische Informationen über etwas

3 Kluge, vgl. transparent.
4 Ebd., vgl. trans-.
5 Ebd., vgl. durch.
6 Erläuterungen zu dieser Differenzierung ebd., S. XXII f.
7 Byung-Chul Han, Wir steuern auf eine Katastrophe zu.

zur Verfügung gestellt werden sollen.[8] Es ist nicht zwingend die Transparenz hier als vollständig zu verstehen.

Auch der rechtliche Rahmen schränkt die Wortbedeutung weiter ein. Nach bisherigen Ansätzen des Datenschutzrechts geht es im Kern um den Schutz der Persönlichkeitsentwicklung, welcher wiederum mit subjektiven Rechten verfolgt wird. So hatte bereits vor der DSGVO jeder Betroffene für sich das Recht von der verantwortlichen Stelle gewisse Informationen zu verlangen, siehe nur §§ 4a, 34 BDSG-alt. Hingegen hat nicht der Betroffene A das Recht Informationen zur Datenverarbeitung, die den B betrifft, von einer verantwortlichen Stelle zu fordern. Damit ist auch der Umfang des (bisherigen) Begriffsverständnisses weitgehend auf subjektive Rechte und ein entsprechendes Rechtsverständnis beschränkt und nicht umfassend, wie beispielsweise im Bereich des Informationsfreiheitsgesetzes.

2. Transparenz im datenschutzrechtlichen Kontext

Die allgemeine Wortbedeutung setzt sich dennoch im spezifischen Kontext des Datenschutzrechts fort.

a) Worum es nicht geht

Klarzustellen ist, dass es hier nicht um die Transparenz geht, die nicht nur im Aufgabenbereich der EU zunehmend Fuß fasst. Es geht nicht um Nachvollziehbarkeit und Kontrolle der Handlungen staatlicher Entitäten.[9] Auch nicht in Frage steht hier das schnell eröffnete Konfliktfeld von Meinungsäußerung und Datenschutz.[10] Nicht gemeint ist grundsätzlich die Transparenz im öffentlich-rechtlichen Sinne, wie sie Beispielsweise in Erwägungsgrund (EG) 72 der Richtlinie 95/46/EG (DSRL) oder in EG 154 der DSGVO zu finden ist.[11]

---

8 Ähnlich auch Schneider, S. 20.

9 Dazu beispielsweise ausführlich anhand eines Beispiels Wollenschläger, AöR 2010, 135. Jahrgang, 363 (364 ff.).

10 Bunge, ZD-Aktuell 2015, 04635 (Dazu zum Beispiel); Tinnefeld, ZD 2015, 22 (grundsätzlicher und eine Synthese in dem Feld bildend).

11 Weiterführend zu diesem Problemaspekt findet sich ein instruktives Beispiel für die dortige Problemlage bei Seeman, in: Zukunft der informationellen Selbstbestimmung, 127–135 (132-134).

b) Arbeitsdefiniton

Um strukturiert bis zu einer genaueren Klärung der Frage, was das Transparenzgebot konkret beinhaltet, arbeiten zu können, soll Transparenz im Sinne dieser Arbeit bedeuten,

dass der Betroffene weiß, wer wann welche Informationen in welchem Kontext über ihn verarbeitet und wozu diese Informationen verwendet werden.

Diese vorläufige Definition ist im Kern dem Volkszählungsurteil entnommen, wo es heißt:

> „eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung [ist verfassungswidrig], in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."[12]

Sie erhebt nicht den Anspruch umfassend oder abschließend zu sein.[13] Einziger Sinn dieser Definition besteht darin, der Arbeit an den erforderlichen Stellen einen nötigen Bezugspunkt zu geben, bis der Inhalt des Transparenzgebots genauer erarbeitet worden ist.

Es stellen sich im Detail einige Abgrenzungsfragen zu anderen Prinzipien und Mechanismen des Datenschutzrechts, insbesondere dem Zweckbindungsgrundsatz, den Auskunftsansprüchen sowie der Datensicherheit und dem Prinzip der Erforderlichkeit und Datensparsamkeit.

c) Bezug des Transparenzgebots zum Verarbeitungszweck

Regelmäßig wird der Zweckbindungsgrundsatz in Datenschutzregelungen explizit geregelt. Dies fängt in Art. 8 lit. a der Datenschutzkonvention des Europarats an und setzt sich bis in Art. 5 Abs. 1 lit. b DSGVO fort. In der Literatur wird dieser Grundsatz meist separat herausgestellt, ohne einen Bezug zum Transparenzgebot herzustellen.[14]

---

12 BVerfG, Urteil v. 15. Dez. 1983 (1 BvR 209, 269, 362, 420, 440, 484/83), BVerfGE 65, 1 (43).

13 So auch das Gericht selbst zu seinen Ausführungen in diesem Urteil ebd., 1 (44).

14 Kühling/Seidel/Sivridis, S. 28; Kühling/Klar/Sackmann, S. 146–147; Moos, S. 50 ff. am Beispiel von Art. 6 der Richtlinie 95/46 Klug, S. 150; Tinnefeld/Ehmann/Gerling, S. 63, 150 f. instruktiv auch zu Problemen bei der praktischen Umsetzung durch Legislative, Exekutive und Verantwortliche Bull, 105 f.

Bei genauer Betrachtung wird deutlich, dass beide Datenschutzgrundsätze eng miteinander verbunden sind. Denn Intransparenz entsteht auch, wenn die Zweckbindung durchbrochen wird.[15]

Wird beispielsweise der Zweck der Datenverarbeitung nach deren Erhebung verändert, wird damit nicht nur die Zweckbindung durchbrochen. Dieses Vorgehen kann ohne Weiteres auch dazu führen, dass der Betroffene nicht mehr weiß, wer was wann bei welcher Gelegenheit über ihn weiß.

Bereits in der Arbeitsdefinition[16] ist über den Kontext („*bei welcher Gelegenheit*“) eine gewisse Zweckbindung angedeutet. Sobald sich der Kontext verändert, wird der Verarbeitungsvorgang möglicherweise intransparent sofern der Betroffene hierüber keine Information erhält oder erhalten kann.

Werden beispielsweise die Nutzungsdaten (was hat der Benutzer wie lange angesehen etc.) einer Webseite wie Facebook erfasst, verändert sich der Kontext der Erfassung signifikant, wenn der Benutzer auf derselben Seite ein Casual Game spielt. Dabei werden zwar weiterhin die Nutzungsdaten von derselben Stelle zur gleichen Zeit erfasst. Die Gelegenheit allerdings verändert sich und mit ihr ganz deutlich auch die Qualität der Daten. Denn im ersten Fall nutzten die Betroffenen Seitenfunktionen und im anderen interagiert er in einem bestimmten vom Spiel gesetzten Rahmen mit dem Spieleanbieter vermittelt durch Facebook.

Noch klarer wird die Situation anhand von Like-Buttons. Auch hier ist Zeitpunkt und Verantwortlicher der Erhebung regelmäßig identisch. Der Unterschied entsteht aber, wenn im einen Fall ein Like auf der Seite selbst abgegeben wird und im anderen Fall der Like-Button auf einer Webseite Dritter verwendet wird. Wenn man davon ausgeht, dass auch unmittelbar auf Facebook über einen Besuch einer beliebigen Seite mit Like-Button geschrieben werden kann und somit dieses Datum bei Facebook hinterlassen wird, so ändert sich der Kontext im zweiten Fall erheblich, da hier zwar dieselbe Verarbeitung stattfindet, aber in einem anderen, unerwarteten Rahmen. Hier verändert sich also der Kontext der Datenverarbeitung erheblich.

Ein Transparenzgebot, das keinerlei Zweckbindung beinhaltet, stößt praktisch an seine Grenzen. Die Betroffenen werden in diesem Fall mit einer Informationsflut an Verarbeitungsvorgängen konfrontiert, weil die Daten mitunter von Dritten weiterverarbeitet werden (dürften) und die Betroffenen konsequenter Weise von allen diesen Vorgängen in Kenntnis gesetzt werden müssten. Die Zweckbindung hingegen hat hier den potenziell restriktiven

15 Am Beispiel der Versicherungswirtschaft Albrecht, S. 61.
16 Dazu S. 42.

Effekt, dass eine Datenverarbeitung nicht ohne Weiteres rechtmäßig ist, wenn die Daten für völlig andere als die zunächst intendierten Zwecke erhoben wurden.

Unabhängig von diesen Bezügen ist den üblichen Datenerfassungsvorgängen inhärent, dass sie in einem bestimmten Kontext erfolgen. Daten werden (jedenfalls aus Sicht der verantwortlichen Stelle) nie grundlos erhoben. Auch aus diesem Grund ist es naheliegend davon auszugehen, dass eine Datenverarbeitung immer zweckgebunden stattfinden muss.

Auch verfassungsrechtlich lässt sich dieser Grundsatz in Eingriffskonstellationen aus dem Grundsatz der Verhältnismäßigkeit eindeutig herleiten.[17] Wenn der Zweckbindungsgrundsatz allerdings aus all diesen Gründen erforderlich ist, stellt sich unmittelbar die Frage, wie dieser effektiv umgesetzt werden kann.

Eine effektive Umsetzung dieses Grundsatzes aus Sicht der Betroffenen ist jedenfalls dann ausgeschlossen, wenn die Datenverarbeitung intransparent erfolgt. In diesen Fällen haben Betroffene keine Möglichkeit zu prüfen, ob die Verarbeitung entsprechend dem bisherigen Verarbeitungszweck erfolgt Somit bedingt also einerseits die Zweckbindung eine funktionierende Transparenz, weil die Informationsflut bei Betroffenen schon im Vorfeld reduziert wird. Denn wenn Verarbeitungen nur im Rahmen spezifischer Zwecke stattfinden, muss auch nur in diesem Rahmen Transparenz hergestellt werden.

Gleichsam bedingt aber auch die Transparenz die Zweckbindung, insoweit nur dann überhaupt erst nachvollziehbar wird, welche Daten für welchen Zweck von wem verarbeitet werden und nur so die Grundlage für die effektive Rechtsdurchsetzung gegeben ist. Demnach ist eine Trennung der beiden Grundsätze im Rahmen dieser Arbeit nicht sinnvoll, sondern vielmehr das Anerkenntnis, dass beide Grundsätze jedenfalls in der praktischen Umsetzung eng aneinander operieren.

Der Zweckbindungsgrundsatz wird im Folgenden daher als relevanter Teilaspekt des Transparenzgebots behandelt werden, ohne dass hierbei verkannt werden soll, dass diesem Grundsatz auch eine darüber hinausgehende, eigenständige Bedeutung zukommt.[18]

---

17 Dazu Tinnefeld/Ehmann/Gerling, S. 149 ff.

18 Zu dessen eigenständiger Bedeutung beispielsweise v. Grafenstein, DSRITB 2016, 233 (238-241).

In der Literatur werden Inhalte der beiden Grundsätze in einem Punkt behandelt, ohne auf eine genaue Trennung zu achten.[19] Sobald der Zweckbindungsgrundsatz zu einem Trennungsgrundsatz oder Zusammenführungsverbot weiterentwickelt wird[20] - oder tatsächlich genau dazu führt - ist der Zusammenhang mit dem Transparenzgebot nicht mehr offensichtlich gegeben.

d) Erforderlichkeit Art. 7 lit. e) DSRL - Datensparsamkeit

Das Prinzip der Erforderlichkeit, eine Datenerhebung nur in dem zur Zweckerreichung notwendigen Umfang durchzuführen, setzt jedenfalls voraus, dass eine Zweckbestimmung stattgefunden hat. Nur mit ihr ist es möglich, zu bestimmen, welche Daten für dessen Erreichung erforderlich sind und welche nicht benötigt werden. Damit ist der Zweckbindungsgrundsatz conditio sine qua non für die Bestimmung der erforderlichen Daten. Die Erforderlichkeit der Datenerhebung beziehungsweise der Grundsatz der Datensparsamkeit resultieren aber nicht zwingend aus dem Transparenzgebot. Ob diese Prinzipien verwirklicht sind oder nicht, tangiert die Verwirklichung des Transparenzgebots nicht, denn auch ohne Erforderlichkeit und Datensparsamkeit ist es möglich die Datenverarbeitung für den Betroffenen transparent zu gestalten.

e) Verhältnis vom untersuchten Transparenzgebot und Auskunftsrechten

Anhand des Telos von Auskunftsansprüche aus den diversen Datenschutznormen wird deutlich, dass diese auch bezwecken, den Betroffenen mit informationeller Waffengleichheit zu versorgen und sicherzustellen, dass beim Betroffenen hinsichtlich seiner eigenen Daten kein Informationsdefizit im Vergleich zur verantwortlichen Stelle besteht. Auch die inhaltliche Ausrichtung von Auskunftsansprüche deckt sich mit Aspekten des Transparenzgebots. Die Ansprüche erfassen regelmäßig die Fragen, wer die Verantwortliche Stelle ist und über welche Daten sie in welchem Kontext wann und wozu verfügt.

Damit stellen Auskunftsansprüche einen verlängerten Arm des Transparenzgebots dar, der jenseits der üblichen Ausgangssituationen wie dem

19 So beispielsweise Roßnagel, der das berühmte Zitat des Bundesverfassungsgerichts sowohl bei der Zweckbindung als auch bei der Transparenz anführt; ebenso v. Zezschwitz, in: Roßnagel, 3.4 Rn. 71 und 50, 3.1 Rn. 4.

20 v. Zizschwitz, ebd., 3.1 Rn. 1.